(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0080121
(43) 공개일자 2011년07월12일

(51) Int. Cl.
G06F 12/14 (2006.01) *G06F 21/24* (2006.01)
(21) 출원번호 10-2010-0129896
(22) 출원일자 2010년12월17일
심사청구일자 없음
(30) 우선권주장
10305005.0 2010년01월04일
유럽특허청(EPO)(EP)

(71) 출원인
톰슨 라이센싱
프랑스 92130 이씨레뮬리노 루 잔다르크 1-5
(72) 발명자
코테이, 올리버
프랑스, 레네스 35000, 라우테 데 베진 68
(74) 대리인
문경진, 김학수

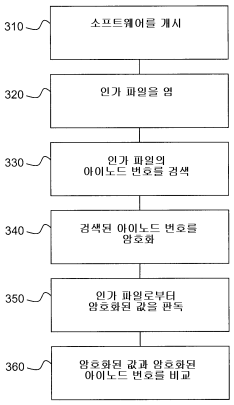
전체 청구항 수 : 총 12 항

(54) 컴퓨터 파일이 복사되었는지를 검출하는 방법 및 디바이스와, 이러한 검출을 가능하게 하는 방법 및 디바이스

(57) 요 약

본 발명은 컴퓨터 파일이 복사되었는지를 검출하는 방법에 관한 것이고, 이 컴퓨터 파일은 아이노드(inode) 번호를 갖는다. 컴퓨터 파일의 아이노드 번호는 검색된다(330). 컴퓨터 파일로부터, 저장된 아이노드 번호는 판독되고(350), 저장된 아이노드 번호는, 컴퓨터 파일이 복사되어선 안 되는 파일 시스템의 아이노드 번호이다. 검색된 아이노드 번호와 판독된 아이노드 번호는 비교되어(360), 만일 검색된 아이노드 번호가 판독된 아이노드 번호와 매칭하지 않으면, 컴퓨터 파일이 복사되었다는 것이 결정된다. 또한, 컴퓨터 파일의 복사에 대한 검출을 가능하게 하는 방법 및 디바이스들(420)과, 이러한 방법에 대응하는 소프트웨어 프로그램 제품들(430)이 제공된다.

대 표 도 - 도3



특허청구의 범위

청구항 1

컴퓨터 파일이 복사되었는지를 검출하는 방법에 있어서, 상기 컴퓨터 파일은 소프트웨어를 포함하고, 아이노드(inode) 번호를 가지며, 상기 소프트웨어 프로그램을 실행시키는 디바이스(410)에서 본 방법은,

- 상기 컴퓨터 파일의 아이노드 번호를 검색하는 단계(330),

- 저장된 아이노드 번호를 판독하는 단계(350)로서, 상기 저장된 아이노드 번호는 상기 컴퓨터 파일이 복사되어선 안 되는 파일 시스템의 아이노드 번호인, 판독 단계(350),

- 상기 검색된 아이노드 번호와 상기 판독된 아이노드 번호를 비교하는 단계(360),

- 만일 상기 검색된 아이노드 번호가 상기 판독된 아이노드 번호와 매칭하지 않는 경우, 상기 컴퓨터 파일이 복사되었다는 것을 결정하는 단계를

포함하는, 컴퓨터 파일이 복사되었는지를 검출하는 방법.

청구항 2

제 1항에 있어서, 상기 저장된 아이노드 번호는 상기 컴퓨터 파일로부터 판독되는, 컴퓨터 파일이 복사되었는지를 검출하는 방법.

청구항 3

제 1 단계에 있어서, 상기 판독된 아이노드 번호는 암호화 키를 사용하여 암호화되고, 상기 방법은 상기 암호화 키를 사용하여, 비교할 수 있도록, 상기 검색된 아이노드 번호를 암호화하는 단계(340)를 더 포함하는, 컴퓨터 파일이 복사되었는지를 검출하는 방법.

청구항 4

제 1 단계에 있어서, 상기 판독된 아이노드 번호는 암호화 키를 사용하여 암호화되고, 상기 방법은 대응하는 복호화 키를 사용하여, 비교할 수 있도록, 상기 검색된 아이노드 번호를 복호화하는 단계를 더 포함하는, 컴퓨터 파일이 복사되었는지를 검출하는 방법.

청구항 5

제 1항에 있어서, 상기 컴퓨터 파일은 소프트웨어 어플리케이션(application)을 위한 인가(license) 파일이고, 본 방법의 단계들은, 상기 디바이스에 의해 상기 소프트웨어 어플리케이션의 실행 동안 수행되며, 상기 방법은, 상기 인가 파일이 복사되었다는 것의 결정시, 상기 소프트웨어의 상기 실행을 정지하는 단계를 더 포함하는, 컴퓨터 파일이 복사되었는지를 검출하는 방법.

청구항 6

상기 컴퓨터 파일에 포함된 소프트웨어 프로그램에 의해 컴퓨터 파일의 복사에 대한 검출을 가능하게 하는 방법으로서, 본 방법은 디바이스(410)에서,

- 상기 컴퓨터 파일을 생성하는 단계(230)로서, 상기 컴퓨터 파일을 생성하는 단계(230)에 의해, 상기 컴퓨터 파일과 아이노드 번호를 관련시키는, 상기 컴퓨터 파일을 생성하는 단계(230),

- 상기 생성된 컴퓨터 파일의 상기 아이노드 번호를 검색하는 단계(240)와,

- 상기 검색된 아이노드 번호를 저장하는 단계(260)를

포함하는, 컴퓨터 파일에 대한 복사의 검출을 가능하게 하는 방법.

청구항 7

제 6항에 있어서, 상기 검색된 아이노드 번호는 상기 컴퓨터 파일에 저장되는, 컴퓨터 파일에 대한 복사의 검출

을 가능하게 하는 방법.

청구항 8

컴퓨터 파일이 복사되었는지를 검출하기 위한 디바이스(410)에 있어서, 상기 컴퓨터 파일은 소프트웨어 프로그램을 포함하고, 아이노드 번호를 가지며, 상기 디바이스(410)는 상기 소프트웨어 프로그램을 실행될 때,

- 상기 컴퓨터 파일의 상기 아이노드 번호를 검색하는 단계,

- 저장된 아이노드 번호를 판독하는 단계로서, 상기 저장된 아이노드 번호는 상기 컴퓨터 파일이 저장되어선 안되는 파일 시스템의 상기 아이노드 번호인, 판독하는 단계,

- 상기 검색된 아이노드 번호와 상기 판독된 아이노드 번호를 비교하는 단계와,

- 만일 상기 검색된 아이노드 번호가 상기 판독된 아이노드 번호와 매칭하지 않으면, 상기 컴퓨터 파일이 복사되었다고 결정하는 단계를

수행하기 위한 처리기(420)를 포함하는, 컴퓨터 파일이 복사되었는지를 검출하기 위한 디바이스.

청구항 9

제 8항에 있어서, 상기 처리기는 소프트웨어 어플리케이션을 더 실행하고, 상기 컴퓨터 파일이 복사되었다고 결정할 시, 상기 소프트웨어 어플리케이션의 실행을 더 정지하는, 컴퓨터 파일이 복사되었는지를 검출하기 위한 디바이스.

청구항 10

상기 컴퓨터 파일에 포함된 소프트웨어 프로그램에 의해 컴퓨터 파일의 복사에 대한 검출을 가능하게 하는 디바이스(410)에 있어서, 상기 디바이스(410)는,

- 상기 컴퓨터 파일을 생성하는 단계,

- 상기 생성된 컴퓨터 파일의 아이노드 번호를 검색하는 단계,

- 상기 저장된 아이노드 번호를 저장하는 단계를

수행하기 위한 처리기(420)를 포함하는, 컴퓨터 파일의 복사에 대한 검출을 가능하게 하는 디바이스.

청구항 11

지령들을 저장하는 소프트웨어 프로그램 제품(430)으로서, 처리기(420)에 의해 실행될 때, 제 1항 내지 제 5항 중 임의의 항의 방법을 수행하는, 소프트웨어 프로그램 제품.

청구항 12

지령들을 저장하는 소프트웨어 프로그램 제품(430)으로서, 처리기(420)에 의해 실행될 때, 제 6항 내지 제 7항 중 임의의 항의 방법을 수행하는, 소프트웨어 프로그램 제품.

명 세 서

기 술 분 야

[0001] 본 발명은 일반적으로 복사 방지에 관한 것이고, 더 구체적으로 소프트웨어 복사 방지에 관한 것이다.

배 경 기 술

[0002] 이 섹션은 아래에 서술되고 및/또는 청구되는 본 발명의 다양한 양상에 관련될 수 있는 기술의 다양한 양상들을 독자들에게 소개하려는 것이다. 본 논의는 독자들에게 본 발명의 다양한 양상에 대한 더 나은 이해를 돕기 위해 배경 정보를 제공하는데 도움이 된다고 믿어진다. 따라서, 이러한 설명은 종래 기술의 인정으로서가 아닌, 이러한 관점으로 읽혀야 한다.

[0003] 소프트웨어 배포자들은, 일부 사람들이 소프트웨어 어플리케이션(application)에 대한 비용을 지불하는 것 없이, 소프트웨어 어플리케이션들의 불법 복제물들을 사용하여 저작권 침해에 직면한다는 것은, 더 이상 놀랄

일이 아니다. 이는 특히, 컴퓨터 게임들의 영역에 해당된다. 따라서 게임 제공자 및 배포자들은 방지 메카니즘들을 사용하여, 이러한 저작권 침해를 방지하도록 시도한다. 이러한 방지 메카니즘들은,

[0004] - 시큐롬(SecuROM)

[0005] - 세이프미디어(SafeMedia)

[0006] - 주소 마크들(mark)과 다른 마크들 또는 플로피 디스크 상의 동기 필드들을 변경시키는 것.

[0007] - 데이터가 CD-R상에 기록될 수 없는 장소들에서 CD-ROM들 상에서의 데이터 사용.

[0008] - 소프트웨어가 완전히 작동되기 위하여, 구입에 대한 입증을 요구하도록 하는 것.

[0009] 등록 키들 및 일련 번호들 또한 이러한 방식으로 사용된다.

[0010] - 동글들(Dongle)

[0011] - 버스 암호화(encryption)

[0012] - 동일한 디렉토리에 소프트웨어 실행 파일로 저장되어야 하는 키파일(keyfile)

[0013] - 전화 또는 인터넷을 통한 제품 활성화를

[0014] 포함한다.

[0015] 이 소프트웨어는 종종 하드웨어 일련 번호 또는 MAC 주소와 같은 컴퓨터의 유일한 식별자를 통하여 특정 컴퓨터로 사용이 제한되지만, 이는, 단지 소수의 이러한 식별자들만이 손쉽게 이용가능하므로, 표준 PC 상에선 곤란하다. 더욱이, 만일 식별자가 (키파일과 같은) 파일에 설정되면, 후에 이 파일 자체는 다른 컴퓨터에 복사될 수 있고, MAC 주소는 최신의 이더넷 카드상에서 변경될 수 있으므로, 복사 방지를 극복하게 된다.

[0016] 이미 언급된 문제들에 덧붙여서, 해커들은 종종, 이러한 방지 메카니즘들을 적어도 부분적으로 무력화시키는 툴(tool)들을 개발함으로써 반격한다.

[0017] 바니카제미(Banikazemi) 등은 "저장소-기반의 파일 시스템 완전성 검사기(Storage-base File System Integrity Checker)"에서 침입 검출 시스템(IDS: intrusion detection system)을 소개했다. 이 시스템은 데이터의 수정을 검출할 수 있고, 또한 데이터의 수정되지 않은 버전(version)들로의 복구(roll-back)를 허용한다. 이 IDS는 집중된(centralised) 디스크들 상에 데이터를 저장하는 다수의 호스트들과, 별개의 저장 영역 네트워크 볼륨 제어기(Storage Area Networks Volume Controller)(SVC)를 포함한다. SVC는, 다른 것들 중에서, 이 파일들에 대한 슈퍼블록(superblock) 및 아이노드(inode) 테이블들과 같은 메타데이터를 판독함으로써, 검증 데이터를 생성한다. 그런 후에, 이 검증 데이터는, 이러한 호스트들이 검증데이터를 조작하지 않도록(temper) 확인하기 위하여, 호스트들에 의해 액세스 될 수 없는 위치에 저장된다. 그런 후에, SVC는, 침입에 의해 파일들이 수정되었는지를 검증하기 위하여 예를 들어, 아이노드 번호들을 사용한다. 이 시스템이 침입 검출에 대하여 잘 작동될 수 있는 반면에, 이 시스템은 파일들의 복사를 막지는 못한다.

발명의 내용

해결하려는 과제

[0018] 그러므로, 복사 검출 계획, 더 구체적으로 표준 PC 상에서 작동할 수 있는 복사 검출 계획에 대한 필요성이 존재한다고 판단된다.

과제의 해결 수단

[0019] 제 1 양상에서, 본 발명은 컴퓨터 파일이 복사되었는지를 검출하는 방법으로 유도되고, 이 컴퓨터 파일은 소프트웨어 프로그램을 포함하며, 아이노드 번호를 갖는다. 컴퓨터 파일의 아이노드 번호는 소프트웨어 프로그램을 실행하는 처리기에 의해 검색된다; 저장된 아이노드 번호는 판독되고, 저장된 아이노드 번호는 컴퓨터 파일이 복사되어선 안 되는 파일 시스템의 아이노드 번호이다; 검색된 아이노드 번호와 판독된 아이노드 번호가 비교된다; 그리고 검색된 아이노드 번호들이 이 판독 아이노드 번호와 매칭하지 않으면, 컴퓨터 파일이 복사되었다고 결정된다.

[0020] 바람직한 제 1 양상에서, 저장된 아이노드 번호는 컴퓨터 파일로부터 판독된다.

[0021] 바람직한 제 2 양상에서, 판독된 아이노드 번호는 암호화 키를 사용하여 암호화되고, 검색된 아이노드 번호는, 비교를 가능하게 하기 위하여, 암호화 키를 사용하여 암호화된다.

[0022] 바람직한 제 3 양상에서, 판독된 아이노드 번호는, 암호화 키를 사용하여 암호화되고, 검색된 아이노드 번호는, 비교를 가능하게 하기 위하여, 대응하는 복호화 키를 사용하여 복호화된다.

[0023] 바람직한 제 4 양상에서, 컴퓨터 파일은 소프트웨어 어플리케이션에 대한 인가(license) 파일이고, 본 방법은 디바이스에 의해 소프트웨어 어플리케이션의 실행 동안, 수행된다. 소프트웨어 어플리케이션의 실행은 인가 파일이 복사되었다고 결정될 시, 정지된다.

[0024] 제 2 양상에서, 본 발명은 컴퓨터 파일에 포함된 소프트웨어 프로그램에 의해 컴퓨터 파일의 복사에 대한 검출을 가능하게 하는 방법에 유도된다. 컴퓨터 파일이 생성되어, 검색되어 저장된 아이노드 번호와 이 컴퓨터 파일을 관련시킨다.

[0025] 바람직한 제 1 실시예에서, 아이노드 번호는 컴퓨터 파일에 저장된다.

[0026] 제 3 양상에서, 본 발명은, 소프트웨어 프로그램을 포함하고, 아이노드 번호를 갖는 컴퓨터 파일이 복사되었는지를 검출하기 위한 디바이스로 유도된다. 이 디바이스는, 소프트웨어 프로그램을 실행할 때, 컴퓨터 파일의 아이노드 번호의 검색; 컴퓨터 파일이 복사되어선 안 되는 파일 시스템의 아이노드 번호인, 저장된 아이노드 번호의 판독; 검색된 아이노드 번호와 판독된 아이노드 번호의 비교; 및 검색된 아이노드 번호가 판독된 아이노드 번호와 매칭되지 않는 경우, 컴퓨터 파일이 복사되었다는 것을 결정하기 위한, 처리기를 포함한다.

[0027] 바람직한 제 1 실시예에서, 처리기는 소프트웨어 어플리케이션을 더 실행하기 위함이고, 컴퓨터 파일이 복사되었다고 결정될 시, 소프트웨어 어플리케이션의 실행을 더 정지하기 위함이다.

[0028] 제 4 양상에서, 본 발명은 컴퓨터 파일에 포함된 소프트웨어 프로그램에 의해 컴퓨터 파일의 복사에 대한 검출을 가능하게 하는 디바이스로 유도된다. 이 디바이스는, 컴퓨터 파일의 생성; 생성된 컴퓨터 파일의 아이노드 번호를 검색; 검색된 아이노드 번호를 생성된 컴퓨터 파일에 저장하기 위한 처리기를 포함한다.

[0029] 제 5 양상에서, 본 발명은, 처리기에 의해 실행될 때, 본 발명의 제 1 양상을 수행하는 지령들을 저장하는 소프트웨어 프로그램 제품으로 유도된다.

[0030] 제 6 양상에서, 본 발명은, 처리기에 의해 실행될 때, 본 발명의 제 2 양상을 수행하는 지령들을 저장하는 소프트웨어 프로그램 제품으로 유도된다.

[0031] 본 발명의 바람직한 특징들은 첨부도면을 참조하여, 제한적이지 않은 방식으로, 이제부터 서술될 것이다.

발명의 효과

[0032] 본 발명은 파일이 불법 복사되었는지를 검출하는 방법 및 디바이스를 제공함으로써, 종래 기술에서의 상술 된 문제점을 개선하는데 효과가 있다.

도면의 간단한 설명

[0033] 도 1은 트리 구조를 사용하는 종래 기술의 파일 시스템을 도시하는 도면.

도 2는 본 발명의 바람직한 실시예에 따른 소프트웨어 설치 방법을 도시하는 도면.

도 3은 본 발명의 바람직한 실시예에 따른 복사 제어의 방법을 도시하는 도면.

도 4는 본 발명에 따른 방법의 구현에 적합한 시스템을 도시하는 도면.

발명을 실시하기 위한 구체적인 내용

[0034] 본 발명의 주 독창적인 아이디어는, 복사 제어를 구현하기 위한 파일 시스템의 양상을 이용하는데, 그 이유는 파일 시스템의 짧은 서술은 이해를 용이하게 돕기 때문이다.

[0035] 파일 시스템은 데이터의 구성 및 액세스를 용이하게 하는 시스템이라 말할 수 있다. 디스크 파일 시스템은 예를 들어, 디스크와 같은 저장 디바이스들 상에서 이용을 위한 파일 시스템이다. 소수의 예시들을 제외하고, FAT, NTFS, HFS, 및 UFS와 같은 다수의 디스크 파일 시스템들이 존재한다. 이러한 디스크 파일 시스템들 중, FAT 및 일부 정도의 NTFS는, 이들이 마이크로소프트 윈도우(Microsoft Windows)에 의해 사용되기에, 특히 널리 보급되

어 있다.

[0036] 대부분의 파일 시스템들의 공통 특징은 트리 구조를 사용한다는 것이고, 이에 대한 예시는 도 1에 도시된다. 파일 시스템(100)은 다수의 디렉토리들(110, 120, 130) 및 다수의 파일들(140, 141)을 포함한다. 루트(root) 디렉토리(110)는 이러한 트리 구조의 꼭대기에 있다. 이 루트 디렉토리(110)는 3개의 서브디렉토리들(120)(subdirectory)을 포함한다. 서브디렉토리들(120) 중, 서브 디렉토리(1)가 추가의 서브디렉토리(130)를 포함하는 반면에, 서브디렉토리(2) 및 서브디렉토리(3)는 다수의 파일들(140)을 포함한다. 게다가, 서브디렉토리 4인, 추가의 서브디렉토리(130)는 파일(141)을 포함한다. 당업자에게 있어서, 이 구조는 단지 예시일 뿐이고, 예를 들어, 디렉토리 레벨들의 개수에는 제한이 없다고 판단될 것이다.

[0037] 파일 시스템(100)에서 각 엔티티는 - 즉, 디렉토리, 서브디렉토리 및 파일 - (오직 하나의 파일(141)에 대해서만 도시된) 아이노드(142)라 불리는, 노드로 여겨질 수 있다. 각 아이노드는 소유권, 액세스 권한, 및 타입에 대한 정보와 같은 메타데이터와 관련되고, 이 아이노드는 파일시스템에서 유일한 아이노드 번호에 의해 식별되며, 아이노드의 수명 내내, 엔티티에 대한 아이노드로 남아있다. 즉, 아이노드 번호는 각 엔티티에 대해 일정하다.

[0038] 따라서, 본 발명의 주 독창적인 아이디어는, 복사 제어를 강제하기 위한 아이노드 번호를 사용하는 것이다.

[0039] 도 2는 본 발명의 바람직한 실시예에 따른 소프트웨어 설치의 방법을 도시한다. 사용자가 소프트웨어를 설치하기 위한 권한을 가지고 있고; 임의의 검증 검사가 본 발명의 범위를 벗어나는 것이라고 가정된다. 단계(210)에서 사용자는 소프트웨어에 대한, 설치 마법사(wizard)라 불리는 설치 어플리케이션을 개시(launch)한다. 설치 마법사는 소프트웨어 파일들을, 통상적으로 하드 디스크 상인 파일 시스템에 복사하고(220), 설치에 필요한 다른 종래 기술인 작업들을 수행한다(이러한 작업들(task)은 본 발명의 범위를 넘어섬).

[0040] 또한, 인가 파일이 인가파일의 위치가 소프트웨어 어플리케이션에 알려지는 동안 다른 경우로 생성될 수 있음에도 불구하고, 설치 마법사는 인가 파일이라 불리는 파일을 파일 시스템에, 바람직하게는 적어도 일부의 복사된(또는 설치된) 소프트웨어 파일로서 동일한 디렉토리에 생성한다(230). 그런 후에 설치 마법사는 생성된 인가 파일의 아이노드 번호를 검색하고(240), 또한 설치된 소프트웨어 프로그램에 의해 알려진 비밀 키를 사용하여 아이노드 번호를 암호화한다(250). 마지막으로 설치 마법사는 암호화된 아이노드 번호를 인가 파일에 저장한다(260). 그런 후에 소프트웨어는 설치된다.

[0041] 인가 파일이 오직 아이 노드 값을 갖는 것(및 저장할 수 있는 것)에 대해 전용일 필요는 없다는 것과, 또한, 인가 파일은 예를 들어, 컴퓨터 코드 및/또는 다른 데이터를 포함할 수 있다는 것이 주목되어야 한다.

[0042] 도 3은 본 발명의 바람직한 실시예에 따른 복사 제어의 방법을 도시한다. 단계(310)에서 소프트웨어는 개시된다. 그런 후에, 소프트웨어는 인가 파일을 열고(320), 인가파일의 아이노드 번호를 검색하며(330), 및 아이노드 번호를 비밀 키로 암호화한다(340). 그런 후에 소프트웨어는 인가 파일에 저장된 암호화된 값을 판독하고(350), 암호화된 아이노드 번호를 판독된 암호화된 값과 비교한다(360). 이러한 값들이 서로 다를 경우, 소프트웨어 실행은 중단된다; 반대로, 만일 값들이 서로 동일하다면, 소프트웨어 실행은 지속된다. 마찬가지로, 본 방법은, 파일 시스템에 나타나는 인가 파일이 존재하지 않는 경우, 단계(320)에서 미리 중단시킬 수 있다.

[0043] 당업자에게 있어서, 도 2 및 도 3에 도시된 본 방법들의 단계들이 본 방법의 작용들에 영향을 끼치는 것 없이도 어느 정도 변경될 수 있다고 판단된다. 예를 들어, 인가 파일은 소프트웨어 파일들이 디렉토리 X(단계(220))에 복사되기 이전에 생성될 수 있다(단계(230)); 게다가, 복사 단계(220)는 설치 마법사의 개시(단계(210)) 이후에, 실질적으로 임의의 순간에 수행될 수 있다. 더욱이, 도 3에서, 판독 단계(350)는 소프트웨어의 개시(310)와 값들의 비교(단계 (360)) 사이의 임의의 시점에서 수행될 수 있다.

[0044] 또한, 도 3의 복사 제어 방법이 적어도 하나의 대안적인 실시예를 갖는다고 판단된다. 대안적인 실시예는 암호화 대신에 복호화를 사용하지만, 일반적인 아이디어는 동일하다. 대안적인 실시예에서, 단계들(310 내지 330)은 단계(350), 즉 인가 파일로부터 암호화된 값의 판독에 의해 진행되는 바람직한 실시예로 수행된다. 하지만, 암호화된 값은 복호화되어, 후에, 인가 파일의 검색된 아이노드 번호와 비교되는 본래의 아이노드 번호를 초래한다. 자연히, 이러한 대안적인 실시예에서, 소프트웨어는 설치 마법사의 암호화 키에 대응하는 복호화 키에 액세스할 수 있다. 추가의 변형에서, 인가 파일의 암호화된 아이노드 번호는 인가 파일이 아닌 다른 위치, 예를 들어 추가의 파일에 저장된다.

[0045] 도 4는 본 발명에 따른, 방법의 구현에 적합한 시스템을 도시한다. 시스템(400)은 컴퓨터(410)와, 컴퓨터(410) 내부에 있을 수 있는 저장 디바이스(424)를 포함한다. 컴퓨터(410)는 처리기(420), 메모리(422), 네트워크 인터

페이스(428), 및 (설치되지 않은) 소프트웨어 어플리케이션 및 설치 마법사를 저장하는 DVD와 같은 데이터 지지체들(430)로부터 데이터를 판독하기 위한 판독기(426)를 포함한다.

[0046] 소프트웨어 설치, 즉, 도 3에 도시된 본 방법, 동안, 판독기(426)는 지지체(430)로부터 설치 마법사를 판독하고, 처리기(420)는 본 방법의 단계들을 실행하며, 필요하다면 다른 부품들(메모리(422), 저장소(424) 등)에게 특정 업무를 수행하도록 지시한다.

[0047] 복사 제어, 즉 도 4에 도시된 방법, 동안, 처리기(420)는 본 방법의 단계를 수행하고, 필요하다면 다른 부품들(특히 저장소(424))에게 특정 업무들을 수행하도록 지시한다.

[0048] 소프트웨어의 암호화 키(또는, 대안의 실시예에서, 복호화 키)가, 예를 들어 공격자가 암호화 키를 복구하는데 어려움을 느끼도록 의도되는, 코드 난독화(obfuscation)와 같은 임의의 적합한 종래기술인 소프트웨어 방지 기술들에 의해 바람직하게 방지된다고 판단된다. 하지만, 이러한 기술들은 본 발명의 범위를 벗어나는 것이다.

[0049] 특정 파일이 2가지 상이한 파일 시스템들에서 동일한 아이노드 번호에 관련되기 힘들다는 것과는 달리, 본 발명은 불법 복사들을 성공적으로 검출하는 높은 개연성을 갖는 복사 방지를 제공할 수 있다.

[0050] 본 발명의 방법이 오직 표준 작동들 - 읽기 및 쓰기- 을 사용하여 구현될 수 있고, 이는 공격자가 차단할 수 있는 특정 시스템 호출들이 존재하지 않는다는 것을 의미한다고 판단된다.

[0051] 따라서, 본 발명은 소프트웨어 어플리케이션에 대한 복사 방지를 위한 방법 및 디바이스를 제공할 수 있다고 판단된다.

[0052] 서술에서 개시된 특징부, 및 (적절하다면) 청구항, 및 도면들 각각은 개별적으로 또는 임의의 적절한 혼합으로 제공될 수 있다. 하드웨어에서 구현된 것으로 서술된 특징부들은 또한 소프트웨어로 구현될 수 있으며, 그 반대의 경우도 성립된다. 청구항들에 나타나는 참조 번호들은 설명의 목적이고, 청구항들의 범위에 제한적인 영향을 끼치지 않아야 한다.

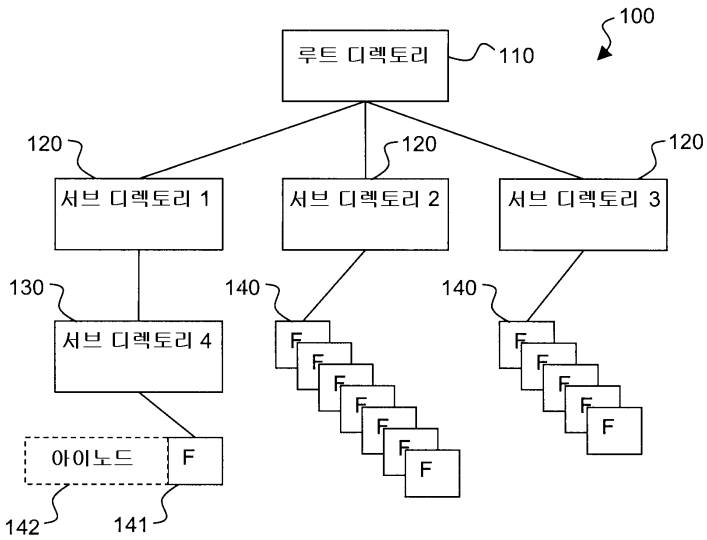
부호의 설명

[0053]

110 : 루트 디렉토리	120 : 서브 디렉토리
130 : 서브 디렉토리 4	140 : 파일
142 : 아이노드	410 : 컴퓨터
420 : 처리기	422 : 메모리
424 : 저장소	426 : 판독기
428 : 네트워크 인터페이스	430 : 데이터 지지체

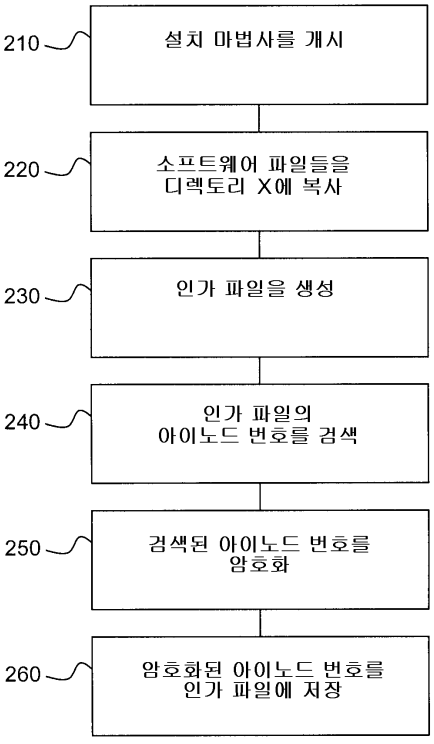
도면

도면1

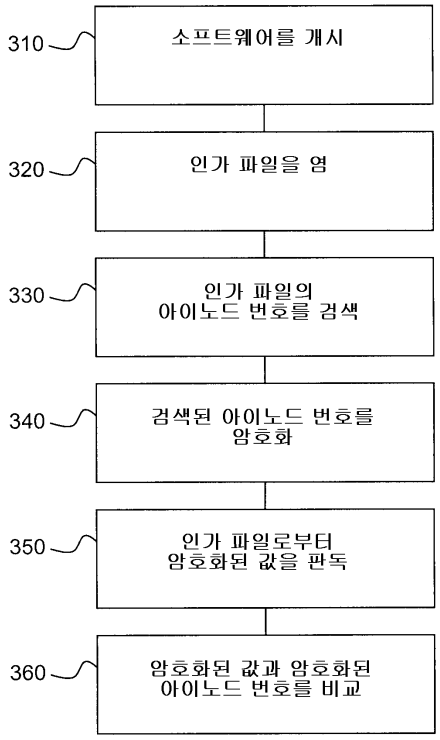


(종래 기술)

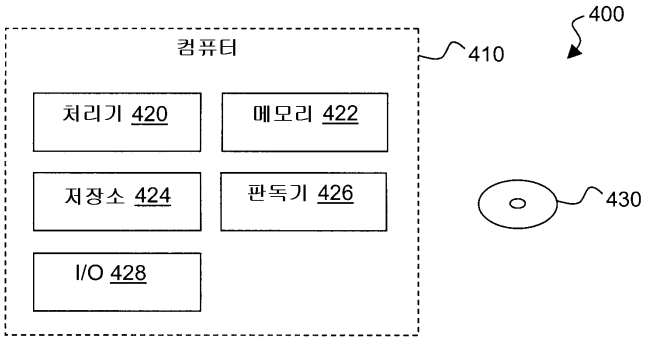
도면2



도면3


310
소프트웨어를 개시
320
인가 파일을 염
330
인가 파일의
아이노드 번호를 검색
340
검색된 아이노드 번호를
암호화
350
인가 파일로부터
암호화된 값을 판독
360
암호화된 값과 암호화된
아이노드 번호를 비교

도면4


400
컴퓨터
410
처리기 420
메모리 422
저장소 424
판독기 426
I/O 428
430