(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년03월03일
(11) 등록번호 10-1368827
(24) 등록일자 2014년02월24일

(51) 국제특허분류(Int. Cl.)
G06F 21/60 (2013.01) *G06Q 50/10* (2012.01)
(21) 출원번호 10-2012-0042439
(22) 출원일자 2012년04월24일
심사청구일자 2012년04월24일
(65) 공개번호 10-2013-0126803
(43) 공개일자 2013년11월21일
(56) 선행기술조사문헌
JP2006155279 A*
KR1020060049669 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 파수닷컴
서울특별시 마포구 월드컵북로 396, 비즈니스센타 17층 (상암동, 누리꿈스퀘어)
(72) 발명자
이형주
서울 은평구 갈현로1길 31, 104동 1002호 (신사동, 한신휴플러스아파트)
(74) 대리인
송경근

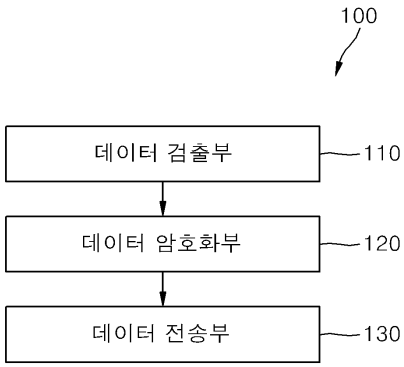
전체 청구항 수 : 총 10 항 심사관 : 박재용

(54) 발명의 명칭 **콘텐츠의 객체별 권한 설정 장치 및 방법, 그리고 객체별 권한에 따른 콘텐츠 제공 장치 및 방법**

(57) 요 약

콘텐츠의 객체별 권한 설정 장치 및 방법이 개시된다. 데이터 검출부는 복수의 객체를 포함하는 디지털 콘텐츠의 소스코드 중 복수의 객체 각각에 대응되는 부분인 데이터 영역을 복수의 객체별로 검출한다. 데이터 암호화부는 데이터 영역 중 보호 대상 객체에 대응하는 데이터 영역을 암호화한다. 데이터 전송부는 암호화된 데이터 영역을 포함하는 디지털 콘텐츠의 소스코드를 사용자 단말로 전송한다. 본 발명에 따르면, 콘텐츠에 포함된 객체별로 이용 권한을 부여하여 동일한 콘텐츠일지라도 사용자는 권한에 따라 선택된 객체를 제공받을 수 있다. 또한 DRM 프로그램이 깔려있지 않은 컴퓨터에서도 파일은 실행될 수 있으며, 실행되는 파일에서 암호화된 객체에만 접근할 수 없도록 설정할 수 있다.

대 표 도 - 도2



특허청구의 범위

청구항 1

복수의 객체를 포함하는 디지털 콘텐츠의 소스코드 중 상기 복수의 객체 각각에 대응되는 부분인 데이터 영역을 상기 복수의 객체별로 검출하는 데이터 검출부;

상기 데이터 영역 중 보호 대상 객체에 대응하는 데이터 영역을 암호화하는 데이터 암호화부; 및

상기 암호화된 데이터 영역을 포함하는 상기 디지털 콘텐츠의 소스코드를 사용자 단말로 전송하는 데이터 전송부;를 포함하며,

상기 데이터 암호화부는 상기 사용자 단말에서 DRM 프로그램이 실행되지 않는 경우 또는 상기 사용자에게 상기 보호 대상 객체에 대한 사용 권한이 없는 경우에, 상기 사용자 단말을 통해 상기 보호 대상 객체를 대신하여 상기 DRM 프로그램을 다운받을 수 있는 링크 정보를 포함하는 접근 불가 정보가 출력되도록, 상기 소스코드에 상기 암호화된 데이터 영역에 대응하는 상기 접근 불가 정보를 추가적으로 삽입하는 것을 특징으로 하는 콘텐츠의 객체별 권한 설정 장치.

청구항 2

제 1항에 있어서,

상기 데이터 암호화부는 상기 보호 대상 객체에 대응하는 데이터 영역은 DRM 프로그램에 의해 추출되고, 상기 보호 대상 객체 이외의 객체에 대응하는 데이터 영역은 상기 디지털 콘텐츠의 포맷에 대응하는 프로그램에 의해 추출되도록 하는 것을 특징으로 하는 콘텐츠의 객체별 권한 설정 장치.

청구항 3

삭제

청구항 4

제 1항에 있어서,

상기 데이터 암호화부는 상기 접근 불가 정보에 대응하는 데이터 영역을 삽입할 때, 상기 보호 대상 객체 이외의 객체에 대응하는 데이터 영역을 추출할 수 있는 상기 디지털 콘텐츠의 포맷에 대응하는 프로그램에 따른 표준화된 형식을 유지하는 것을 특징으로 하는 콘텐츠의 객체별 권한 설정 장치.

청구항 5

제 1항에 있어서,

상기 데이터 전송부는 상기 사용자의 식별 정보 및 상기 보호 대상 객체에 대응하는 상기 사용자의 사용 권한 정보 중 적어도 하나를 포함하는 암호화 정보를 상기 디지털 콘텐츠의 소스코드와 함께 상기 사용자 단말로 전송하는 것을 특징으로 하는 콘텐츠의 객체별 권한 설정 장치.

청구항 6

제 1항에 있어서,

상기 디지털 콘텐츠에 포함된 객체는 동영상, 이미지, 음원, 텍스트 중 적어도 하나인 것을 특징으로 하는 콘텐츠의 객체별 권한 설정 장치.

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

복수의 객체를 포함하는 디지털 콘텐츠의 소스코드 중 상기 복수의 객체 각각에 대응되는 부분인 데이터 영역을 상기 복수의 객체별로 검출하는 데이터 검출단계;

상기 데이터 영역 중 보호 대상 객체에 대응하는 데이터 영역을 암호화하는 데이터 암호화단계; 및

상기 암호화된 데이터 영역을 포함하는 상기 디지털 콘텐츠의 소스코드를 사용자 단말로 전송하는 데이터 전송단계;를 포함하며,

상기 데이터 암호화단계에서, 상기 사용자 단말에서 DRM 프로그램이 실행되지 않는 경우 또는 사용자에게 상기 보호 대상 객체에 대한 사용 권한이 없는 경우에, 상기 사용자 단말을 통해 상기 보호 대상 객체를 대신하여 상기 DRM 프로그램을 다운받을 수 있는 링크 정보를 포함하는 접근 불가 정보가 출력되도록, 상기 소스코드에 상기 암호화된 데이터 영역에 대응하는 상기 접근 불가 정보를 추가적으로 삽입하는 것을 특징으로 하는 콘텐츠의 객체별 권한 설정 방법.

청구항 11

제 10항에 있어서,

상기 데이터 암호화단계에서, 상기 보호 대상 객체에 대응하는 데이터 영역은 DRM 프로그램에 의해 추출되고, 상기 보호 대상 객체 이외의 객체에 대응하는 데이터 영역은 상기 디지털 콘텐츠의 포맷에 대응하는 프로그램에 의해 추출되도록 하는 것을 특징으로 하는 콘텐츠의 객체별 권한 설정 방법.

청구항 12

삭제

청구항 13

제 10항에 있어서,

상기 데이터 암호화단계에서, 상기 접근 불가 정보에 대응하는 데이터 영역을 삽입할 때, 상기 보호 대상 객체 이외의 객체에 대응하는 데이터 영역을 추출할 수 있는 상기 디지털 콘텐츠의 포맷에 대응하는 프로그램에 따른 표준화된 형식을 유지하는 것을 특징으로 하는 콘텐츠의 객체별 권한 설정 방법.

청구항 14

제 10항에 있어서,

상기 데이터 전송단계에서, 상기 사용자의 식별 정보 및 상기 보호 대상 객체에 대응하는 상기 사용자의 사용 권한 정보 중 적어도 하나를 포함하는 암호화 정보를 상기 디지털 콘텐츠의 소스코드와 함께 상기 사용자 단말로 전송하는 것을 특징으로 하는 콘텐츠의 객체별 권한 설정 방법.

청구항 15

제 10항에 있어서,

상기 디지털 콘텐츠에 포함된 객체는 동영상, 이미지, 음원, 텍스트 중 적어도 하나인 것을 특징으로 하는 콘텐츠의 객체별 권한 설정 방법.

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 콘텐츠의 객체별 권한 설정 장치 및 방법에 관한 것으로, 보다 상세하게는, 사용자의 디지털 콘텐츠 접근을 제어할 수 있는 콘텐츠의 객체별 권한 설정 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 디지털 권한 관리(Digital Rights Management : DRM)는 디지털 미디어의 불법 또는 비 인가된 사용을 제한하기 위하여 저작권 소유자나 판권 소유자가 이용하는 정보 보호 기술의 일종인 접근 제어 기술이다. 이는 인터넷의 보급과 더불어 디지털 콘텐츠가 활발히 보급되면서 등장한 새로운 개념이라고 할 수 있다.

[0003] 디지털 콘텐츠는 아날로그 콘텐츠와 달리 컴퓨터를 이용하여 쉽고 빠르게 복사할 수 있으며, 복제품은 원본에 비해 질적인 저하가 없고 확산 속도가 빠른 속성을 가진다. 이것은 초기 인터넷상에서 콘텐츠는 무료라는 사용자들의 인식과 더불어 콘텐츠의 불법 복제 및 비정상적인 유통 문제를 야기하고 있다. 또한 이와 같이 제작에 많은 비용과 노력 및 시간을 필요로 하는 디지털 콘텐츠의 불법 복제 및 배포가 용인될 경우, 디지털 콘텐츠 제작자의 이익을 침해하게 되고 디지털 콘텐츠 제작자의 창작 의욕은 저하되어 디지털 콘텐츠 산업의 활성화에 큰 저해요소가 된다.

[0004] 디지털 콘텐츠 중 문서는 보안이 취약한 분야로 문서를 암호화하고 권한에 따라 복호화하는 방식으로 사용자에게 문서에 대한 권한을 부여한다. 이러한 암복호화 방식의 DRM은 파일 단위로 파일 자체를 암호화하는 것이 일반적이다. 즉, 파일에 포함된 동영상, 텍스트, 이미지 등의 객체에 관계없이 파일 전체를 암호화하고 사용자는 파일의 열람, 인쇄, 수정, 복사 등 주어진 사용 권한에 대응하여 파일을 복호화할 수 있다.

[0005] 예를 들어, A 사용자에게는 문서의 열람, 인쇄, 수정 및 복사의 사용 권한이 주어지고 B 사용자에게는 문서의 열람 및 복사의 사용 권한이 주어질 수 있다. 이때 암호화된 문서 전체에 대해 A 사용자는 열람, 인쇄, 수정 및 복사가 가능하고, B 사용자는 열람 및 복사가 가능하다.

[0006] 그러나 이와 같이 파일 단위로 문서를 암호화하는 경우 파일 내 객체의 중요도를 고려할 수 없으며 객체별로 사용 권한을 설정할 수도 없기 때문에 사용자에게는 모든 객체에 대해 획일적으로 사용 권한이 부여되거나 부여되지 않게 된다. 즉, 파일 전체에 대한 사용 권한이 부여되는 경우 파일 내 포함된 객체 중 저작권 보호 대상이 아닌 객체도 이용할 수 없다는 문제점이 있다.

[0007] 한국공개특허 제2009-0016282호에는 콘텐츠의 선택적인 부분 암호화를 위한 DRM 시스템 및 방법이 개시되어 있다. 개시된 방법에 의하면 특정 콘텐츠를 암호화할 때 일반적인 전체 암호화가 아닌 일부만 선택적으로 암호화할 수 있어 대용량 콘텐츠를 복호화하는데 소요되는 시간을 단축할 수 있다.

[0008] 그러나 콘텐츠에 포함된 객체의 중요도를 고려하거나 객체별로 권한을 설정할 수 없으며, 콘텐츠의 암호화된 부분을 복호화하지 못할 경우 전체 콘텐츠를 이용할 수 없다는 문제점이 있다.

발명의 내용

해결하려는 과제

[0009] 본 발명이 이루고자 하는 기술적 과제는, 디지털 콘텐츠에 포함된 객체별로 사용자의 사용 권한을 설정하고, 디지털 콘텐츠의 암호화된 객체를 제외한 부분은 제약없이 이용 가능하도록 하는 콘텐츠의 객체별 권한 설정 장치 및 방법, 그리고 객체별 권한에 따른 콘텐츠 제공 장치 및 방법을 제공함에 있다.

과제의 해결 수단

[0010] 상기의 기술적 과제를 달성하기 위한, 본 발명에 따른 콘텐츠의 객체별 권한 설정 장치는, 복수의 객체를 포함하는 디지털 콘텐츠의 소스코드 중 상기 복수의 객체 각각에 대응되는 부분인 데이터 영역을 상기 복수의 객체별로 검출하는 데이터 검출부; 상기 데이터 영역 중 보호 대상 객체에 대응하는 데이터 영역을 암호화하는 데이

터 암호화부; 및 상기 암호화된 데이터 영역을 포함하는 상기 디지털 콘텐츠의 소스코드를 사용자 단말로 전송하는 데이터 전송부;를 구비하며, 상기 데이터 암호화부는 상기 사용자 단말에서 DRM 프로그램이 실행되지 않는 경우 또는 상기 사용자에게 상기 보호 대상 객체에 대한 사용 권한이 없는 경우에, 상기 사용자 단말을 통해 상기 보호 대상 객체를 대신하여 상기 DRM 프로그램을 다운받을 수 있는 링크 정보를 포함하는 접근 불가 정보가 출력되도록 상기 소스코드에 상기 접근 불가 정보에 대응하는 데이터 영역을 삽입한다.

[0011] 상기의 기술적 과제를 달성하기 위한, 본 발명에 따른 콘텐츠의 객체별 권한 설정 방법은, 복수의 객체를 포함하는 디지털 콘텐츠의 소스코드 중 상기 복수의 객체 각각에 대응되는 부분인 데이터 영역을 상기 복수의 객체별로 검출하는 데이터 검출단계; 상기 데이터 영역 중 보호 대상 객체에 대응하는 데이터 영역을 암호화하는 데이터 암호화단계; 및 상기 암호화된 데이터 영역을 포함하는 상기 디지털 콘텐츠의 소스코드를 사용자 단말로 전송하는 데이터 전송단계;를 가지며, 상기 데이터 암호화단계에서, 상기 사용자 단말에서 DRM 프로그램이 실행되지 않는 경우 또는 사용자에게 상기 보호 대상 객체에 대한 사용 권한이 없는 경우에, 상기 사용자 단말을 통해 상기 보호 대상 객체를 대신하여 상기 DRM 프로그램을 다운받을 수 있는 링크 정보를 포함하는 접근 불가 정보가 출력되도록 상기 소스코드에 상기 접근 불가 정보에 대응하는 데이터 영역을 삽입한다.

발명의 효과

[0012] 본 발명에 따른 콘텐츠의 객체별 권한 설정 장치 및 방법, 그리고 객체별 권한에 따른 콘텐츠 제공 장치 및 방법에 의하면, 콘텐츠에 포함된 객체별로 이용 권한을 부여하여 동일한 콘텐츠일지라도 사용자는 권한에 따라 선택된 객체를 제공받을 수 있다. 또한 DRM 프로그램이 깔려있지 않은 컴퓨터에서도 파일은 실행될 수 있으며, 실행되는 파일에서 암호화된 객체에만 접근할 수 없도록 설정할 수 있다.

도면의 간단한 설명

[0013] 도 1은 본 발명에 따른 콘텐츠의 객체별 권한 설정 장치 및 객체별 권한에 따른 콘텐츠 제공 장치를 포함하는 전체 권한 관리 시스템을 나타낸 도면,

도 2는 본 발명에 따른 콘텐츠의 객체별 권한 설정 장치에 대한 바람직한 실시예의 구성을 도시한 블록도,

도 3은 디지털 콘텐츠 및 디지털 콘텐츠를 구성하는 객체의 일 실시예를 나타낸 도면,

도 4a는 사용자 단말에서 접근 불가 정보가 출력된 실시예를 나타낸 도면,

도 4b는 사용자 단말에서 보호 대상 객체가 출력된 실시예를 나타낸 도면,

도 5는 데이터 암호화부에 의해 디지털 콘텐츠의 구성이 변환되는 일 실시예를 나타낸 도면

도 6은 본 발명에 따른 객체별 권한에 따른 콘텐츠 제공 장치에 대한 바람직한 실시예의 구성을 도시한 블록도

도 7은 본 발명에 따른 콘텐츠의 객체별 권한 설정 방법에 대한 바람직한 실시예의 수행과정을 도시한 흐름도, 그리고,

도 8은 본 발명에 따른 객체별 권한에 따른 콘텐츠 제공 방법에 대한 바람직한 실시예의 수행 과정을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0014] 이하에서 첨부된 도면들을 참조하여 본 발명에 따른 콘텐츠의 객체별 권한 설정 장치 및 방법, 그리고 객체별 권한에 따른 콘텐츠 제공 장치 및 방법의 바람직한 실시예에 대해 상세하게 설명한다.

[0015] 도 1은 본 발명에 따른 콘텐츠의 객체별 권한 설정 장치 및 객체별 권한에 따른 콘텐츠 제공 장치를 포함하는 전체 권한 관리 시스템을 나타낸 도면이다.

[0016] 도 1을 참조하면, 권한 관리 시스템은 콘텐츠의 객체별 권한 설정 장치(100), 객체별 권한에 따른 콘텐츠 제공 장치(200) 및 사용자 단말(300)을 포함한다.

[0017] 본 발명에 따른 콘텐츠의 객체별 권한 설정 장치(100)는 디지털 콘텐츠의 공급자 측 서버에 위치할 수 있으며, 복수의 객체로 이루어진 디지털 콘텐츠의 소스코드 중 보호 대상 객체에 대응하는 부분을 암호화하여 사용자 단말(300)로 전송한다.

[0018] 또한 본 발명에 따른 객체별 권한에 따른 콘텐츠 제공 장치(200)는 사용자 단말(300)로 전송된 디지털 콘텐츠의

소스코드 중 암호화된 부분을 복호화하는 동작을 수행하며, DRM(Digital Rights Management) 프로그램의 형태로 구현될 수 있다. 본 발명에 따른 객체별 권한에 따른 콘텐츠 제공 장치(200)는 도 1에 도시된 바와 같이 사용자 단말(300) 내에 설치되거나 별도의 장치로 구현되어 사용자 단말(300)과 데이터를 송수신할 수 있다.

[0019] 이하, 본 발명에 따른 콘텐츠의 객체별 권한 설정 장치(100) 및 객체별 권한에 따른 콘텐츠 제공 장치(200)의 구체적인 동작을 상세하게 설명한다.

[0020] 도 2는 본 발명에 따른 콘텐츠의 객체별 권한 설정 장치(100)에 대한 바람직한 실시예의 구성을 도시한 블록도이다.

[0021] 도 2를 참조하면, 본 발명에 따른 콘텐츠의 객체별 권한 설정 장치(100)는 데이터 검출부(110), 데이터 암호화부(120) 및 데이터 전송부(130)를 포함한다.

[0022] 데이터 검출부(110)는 복수의 객체를 포함하는 디지털 콘텐츠의 소스코드 중 복수의 객체 각각에 대응되는 부분인 데이터 영역을 복수의 객체별로 검출한다.

[0023] 디지털 콘텐츠는 웹 페이지, 문서 등 다양한 형태로 사용자 단말(300)을 통해 출력되어 사용자에게 정보를 제공하며 텍스트, 동영상, 이미지, 음원 등 다양한 형태의 객체를 포함할 수 있다.

[0024] 도 3은 디지털 콘텐츠 및 디지털 콘텐츠를 구성하는 객체의 일 실시예를 나타낸 도면이다.

[0025] 도 3을 참조하면, 디지털 콘텐츠는 사용자 단말(300)을 통해 출력되는 PDF 포맷의 문서 전체를 의미한다. 그리고 PDF 문서에 포함된 텍스트(A) 및 이미지(B)는 디지털 콘텐츠를 구성하는 개별 객체를 의미한다.

[0026] 디지털 콘텐츠의 소스코드 중 복수의 객체 각각에 대응되는 부분인 데이터 영역은 사용자 단말(300)에서 객체를 출력하기 위한 이진(binary) 데이터 영역을 의미한다. 객체별 데이터 영역은 디지털 콘텐츠의 내용에 대응하는 이진 데이터 영역뿐 아니라, 디지털 콘텐츠의 내용이 사용자 단말(300)을 통해 출력되는 형식, 예를 들면 레이아웃에 대응하는 이진 데이터 영역도 포함할 수 있다. 이와 같은 이진 데이터 영역은 사용자 단말(300)에 설치된 소프트웨어나 하드웨어에 의해 해석되어, 사용자 단말(300)의 출력 장치를 통해 사용자가 인지할 수 있는 형태로 출력된다.

[0027] 다시 도 2를 참조하면, 데이터 암호화부(120)는 복수의 데이터 영역 중 보호 대상 객체에 대응하는 데이터 영역을 암호화한다. 데이터 암호화부(120)는 보호 대상 객체에 대응하는 데이터 영역은 DRM 프로그램, 즉 본 발명에 따른 객체별 권한에 따른 콘텐츠 제공 장치(200)에 의해 추출되고, 보호 대상 객체 이외의 객체에 대응하는 데이터 영역은 디지털 콘텐츠의 포맷에 대응하는 프로그램(이하, '전용 프로그램'이라 한다)에 의해 추출되도록 할 수 있다. 이때 DRM 프로그램과 전용 프로그램은 디지털 콘텐츠가 사용자 단말(300)을 통해 출력될 때 동작하는 프로그램이다.

[0028] 구체적으로, 사용자의 사용 권한은 사용자가 디지털 콘텐츠에 대해 열람, 편집, 인쇄 및 수정 등의 접근을 할 수 있는 권리로서, 디지털 콘텐츠를 구성하는 객체 각각에 대응하여 사전에 설정될 수 있다. 이때 디지털 콘텐츠를 구성하는 모든 객체에 대응하여 사용 권한이 설정되는 것은 아니며, 복수의 객체 중 보호가 필요한 객체인 보호 대상 객체에 대하여만 사용 권한이 설정될 수 있다.

[0029] 또한 동일한 보호 대상 객체에 대해서도 디지털 콘텐츠에 접근하는 사용자별로 상이한 사용 권한이 설정될 수 있다. 즉, 디지털 콘텐츠에 대한 사용자의 사용 권한은 사용자 및 보호 대상 객체에 따라 상이하게 설정될 수 있는 것이다.

[0030] 도 3에 도시된 실시예를 참조하면, 텍스트(A) 및 이미지(B)는 보호 대상 객체에 해당할 수 있다. 또한 사용자(a)는 텍스트(A)를 열람할 수 있고 이미지(B)를 열람 및 편집할 수 있으며, 사용자(b)는 텍스트(A)만 열람할 수 있고 이미지(B)는 열람할 수 없도록 사전에 사용 권한이 설정될 수 있다.

[0031] 도 3에 도시된 것과 같은 디지털 콘텐츠의 소스코드에 대하여, 먼저 데이터 검출부(110)는 텍스트(A) 및 이미지(B)를 포함하는 복수의 객체 각각에 대응되는 부분인 데이터 영역을 검출한다.

[0032] 그리고 데이터 암호화부(120)는 보호 대상 객체인 텍스트(A) 및 이미지(B)에 대응하는 데이터 영역은 사용자 단말(300)에서 DRM 프로그램에 의해 추출되고, 이외의 객체에 대응하는 데이터 영역은 PDF 포맷에 대응하는 전용 프로그램인 아크로뱃(Acrobat) 프로그램에 의해 추출되도록 텍스트(A) 및 이미지(B)에 대응하는 데이터 영역을 암호화한다.

[0033] 다시 도 2를 참조하면, 데이터 암호화부(120)는 사용자 단말(300)에서 DRM 프로그램이 실행되지 않는 경우 또는 사용자에게 보호 대상 객체에 대한 사용 권한이 없는 경우에, 사용자 단말(300)을 통해 보호 대상 객체를 대신하여 접근 불가 정보가 출력되도록 디지털 콘텐츠의 소스코드에 접근 불가 정보에 대응하는 데이터 영역을 삽입할 수 있다. 이때 접근 불가 정보에 대응하는 데이터 영역은 데이터 영역에 대한 표준화된 형식을 유지한다. 또한 접근 불가 정보는 "접근 권한이 없습니다" 등의 문구, 보호 대상 객체가 사용자 단말(300)을 통해 출력되는 원본 내용으로부터 변형된 정보, DRM 프로그램을 다운받기 위한 링크 등으로 다양하게 설정할 수 있다.

[0034] 사용자는 DRM 프로그램을 실행하여 디지털 콘텐츠의 암호화된 부분을 제공받기 위해 DRM 프로그램에 로그인할 수 있는 아이디, 고유 번호 등의 식별 정보가 있어야 한다. 즉, 사용자 단말(300)에서 DRM 프로그램이 실행되지 않는 경우에는 사용자 단말(300)에 DRM 프로그램이 설치되어 있지 않거나 사용자에게 식별 정보가 없는 경우, 또는 사용자에게 식별 정보가 있어도 보호 대상 객체에 대한 사용 권한이 없는 경우 등이 포함된다.

[0035] 데이터 암호화부(120)는 디지털 콘텐츠의 소스코드에 접근 불가 정보에 대응하는 데이터 영역을 삽입할 때 데이터 영역에 대한 표준화된 형식을 유지하는 것이 바람직하다. 구체적으로, 데이터 암호화부(120)는 이진 데이터를 해석하는 사용자 단말(300)에 설치된 소프트웨어나 하드웨어가 계속 이용 가능하도록 이진 데이터의 종래 표준화된 규격(포맷)을 준수하고 커스터마이징(customizing)이 가능한 규격을 사용하여 소스코드를 변환한다. 또한 호환성 유지를 위해 소스코드 중 해석되지 않는 비 해석 영역 또는 가비지(garbage)로 인식되는 영역을 사용할 수 있다.

[0036] 도 4a는 사용자 단말(300)에서 접근 불가 정보가 출력된 실시예를, 도 4b는 사용자 단말(300)에서 보호 대상 객체가 출력된 실시예를 나타낸 도면이다.

[0037] 도 4a를 참조하면, 도 4a의 (a)는 사용자 단말(300)에서 접근 불가 정보가 출력된 경우를, (b)는 사용자 단말(300) 내에 본 발명에 따른 객체별 권한에 따른 콘텐츠 제공 장치(200), 즉 DRM 프로그램이 설치되어 있지 않은 경우의 객체별 데이터 영역 처리 과정을 나타낸다.

[0038] 본 발명에 따른 콘텐츠의 객체별 권한 설정 장치(100)는 보호 대상 객체를 대신하여 접근 불가 정보가 출력되도록 소스코드에 접근 불가 정보에 대응하는 데이터 영역, 즉 위조(fake) 정보(410)를 삽입한다. 이때 사용자 단말(300)에는 DRM 프로그램이 설치되어 있지 않기 때문에 전용 프로그램은 링크된 암호화된 데이터 영역(420)을 복호화할 수 없다. 그 결과 사용자 단말(300)에서는 접근 불가 정보가 출력된다.

[0039] 도 4b를 참조하면, 도 4b의 (a)는 사용자 단말(300)에서 보호 대상 객체가 출력된 경우를, (b)는 사용자 단말(300) 내에 본 발명에 따른 객체별 권한에 따른 콘텐츠 제공 장치(200), 즉 DRM 프로그램이 설치되어 있는 경우의 객체별 데이터 영역 처리 과정을 나타낸다.

[0040] 마찬가지로, 본 발명에 따른 콘텐츠의 객체별 권한 설정 장치(100)는 보호 대상 객체를 대신하여 접근 불가 정보가 출력되도록 소스코드에 접근 불가 정보에 대응하는 데이터 영역, 즉 위조(fake) 정보(410)를 삽입한다. 이때 사용자 단말(300)에는 DRM 프로그램이 설치되어 있기 때문에 사용자 단말(300)에서 암호화된 데이터 영역(420)을 복호화할 수 있다. 구체적으로, DRM 프로그램은 위조(fake) 정보(410)에 링크된 정보를 통해 암호화된 보호 대상 객체를 호출하고, 암호화된 보호 대상 객체를 복호화하여 보호 대상 객체를 사용자 단말(300)에 출력한다.

[0041] 도 5는 데이터 암호화부(120)에 의해 디지털 콘텐츠의 구성이 변환되는 일 실시예를 나타낸 도면이다.

[0042] 도 5를 참조하면, 도 5의 (a)는 도 3에 도시된 것과 같은 PDF 포맷의 디지털 콘텐츠의 구성, (b)는 기존의 객체별 데이터 영역, (c)는 데이터 암호화부(120)에 의해 암호화된 객체별 데이터 영역을 나타낸다.

[0043] (a)를 참조하면 PDF 포맷의 디지털 콘텐츠의 소스코드는 헤더(Header), 바디(Body) 및 테일(Tail)로 구성된다. 이 중 바디 부분에는 텍스트, 이미지(1) 및 이미지(2)의 객체와 객체별 사용 권한 정보, 다른 객체를 호출하는 정보, 사용자의 식별 정보 등이 포함되어 있다.

[0044] (b)는 이미지(1)에 대한 기존의 데이터 영역을 나타낸다. Obj 01<BBOX 가로4, 세로2.5, resource img 02R>를 해석하면, Obj 01은 이미지(1)이 삽입되는 가로 4, 세로 2.5의 박스를 생성하며 resource는 이미지(1)의 형식을 나타낸다. 그리고 Obj 2를 의미하는 02R(Reference)을 호출한다. Obj 2에는 삽입될 이미지(1)에 대한 정보(이미지 파일)가 포함되어 있다.

[0045] (c)는 데이터 암호화부(120)에 의해 암호화된 이미지(1)에 대한 데이터 영역을 나타낸다. 데이터 암호화부(120)는 기존의 이미지(1)에 대한 데이터 영역을 Obj 01<BBOX 가로4, 세로2.5, resource img 03R, DRM 02R, DRM

04R>로 변환함으로써 암호화한다.

[0046] 구체적으로, 기존 방식과 달리 데이터 암호화부(120)는 Obj 02를 호출하는 정보인 02R을 03R로 변경하고 DRM 02R 및 DRM 04R를 추가하여 암호화한다. DRM 02R은 Obj 2를 호출하는 정보이며 Obj 2에는 삽입될 이미지(1)에 대한 정보(이미지 파일)가 포함되어 있다. Obj 03에는 "접근 권한이 없습니다" 등의 문구와 같은 접근 불가 정보가, Obj 04에는 Obj 02의 복호화를 위한 데이터인 사용 권한 정보가 삽입되어 있다.

[0047] 앞서 설명한 바와 같이, 데이터 암호화부(120)는 사용자의 단말에 DRM 프로그램이 실행되지 않는 경우 또는 사용자에게 보호 대상 객체에 대한 사용 권한이 없는 경우에, 사용자의 단말을 통해 보호 대상 객체를 대신하여 접근 불가 정보가 출력되도록 소스코드에 접근 불가 정보에 대응하는 데이터 영역을 삽입할 수 있다.

[0048] 구체적으로, 사용자 단말에서 PDF 포맷에 대응하는 전용 프로그램이 실행되면 이미지(1)에 대응하는 Obj 01은 Obj 03을 호출한다. Obj 03에는 "접근 권한이 없습니다" 등의 접근 불가 정보가 포함되어 있기 때문에, 원래 표시되어야 하는 이미지(1)이 아닌 "접근 권한이 없습니다" 등의 접근 불가 정보가 출력된다.

[0049] 이때 출력되는 접근 불가 정보로 "접근 권한이 없습니다" 등의 문구, X 표시, DRM 프로그램을 다운받기 위한 링크 또는 이미지(1)과 관련되지 않은 다른 이미지 등이 설정될 수 있다. 그러나 이미지(1)을 제외한 텍스트 및 이미지(2)는 암호화되지 않은 정보이므로 PDF 전용 프로그램을 통해 사용자 단말(300)에 표시될 수 있다.

[0050] 암호화된 이미지(1)이 사용자 단말(300)에 표시되도록 하기 위해서는 사용자가 사용자 단말(300)에 DRM 프로그램을 설치하고, 이미지(1)를 디스플레이하는 사용 권한을 가지고 있어야 한다. 구체적으로, 사용자가 DRM 프로그램을 실행하여 로그인하고 사용자에게 이미지(1)를 디스플레이하는 사용 권한이 있다면, DRM 프로그램은 Obj 02를 호출한다. Obj 02는 암호화되어 있으므로 DRM 프로그램에 의해 복호화되어야 하고, DRM 프로그램은 Obj 04에 포함되어 있는 사용 권한 정보를 이용하여 Obj 02를 복호화하여 PDF 전용 프로그램에 제공한다.

[0051] 데이터 암호화부(120)가 데이터 영역의 표준 포맷을 유지시키면서 데이터 영역을 변환하기 때문에, 데이터 영역은 DRM 프로그램 및 전용 프로그램에서 모두 해석될 수 있다. 구체적으로, DRM 프로그램은 Obj 01<BBOX 가로4, 세로2.5, resource img 03R, DRM 02R, DRM 04R>에서 Obj 03보다 DRM으로 구성된 Obj 02 및 Obj 04를 먼저 호출한다. 반면, 전용 프로그램은 Obj 03을 먼저 호출하고 전용 프로그램에서 해석되지 않는 Obj 02 및 Obj 04는 무시하기 때문에 디지털 콘텐츠를 실행하는데 문제가 발생하지 않는다. 또한 데이터 암호화부(120)는 이상에서 설명한 것과 동일한 방식으로 텍스트 및 이미지(2)를 암호화할 수 있다.

[0052] 또 다른 실시예로, 디지털 콘텐츠가 문서가 아닌 웹 기반의 포맷을 가지는 경우에도 사용자 단말(300)에 DRM 프로그램이 설치되어 있지 않으면 보호 대상 객체가 출력되지 않고 접근 불가 정보가 출력된다. 일반적으로 웹 기반 콘텐츠는 HTML과 JAVA 스크립트로 구성되어 있으며, 웹에서 표시될 정보가 동영상일 경우 동영상 태그만 포함되고 데이터는 URL 링크 등을 통해 별도로 제공받는다.

[0053] 구체적으로, 데이터 암호화부(120)는 동영상이 포함된 웹 기반 디지털 콘텐츠에 대하여 사용자 단말(300)에 DRM 프로그램이 설치되어 있지 않으면 동영상이 재생되지 않도록 하기 위해 HTML 포맷을 유지하면서 동영상의 URL 정보가 있던 위치에 가짜 URL을 삽입한다. 그리고 하단에 DRM 정보(동영상의 진짜 URL)를 삽입하여 DRM 프로그램은 DRM 정보를 처리하도록 하고, DRM 프로그램이 설치되어 있지 않은 경우 가짜 URL 또는 DRM 프로그램이 설치되기 위한 URL이 열리도록 할 수 있다.

[0054] 다시 도 2를 참조하면, 데이터 전송부(130)는 암호화된 데이터 영역을 포함하는 디지털 콘텐츠의 소스코드를 사용자 단말(300)로 전송한다.

[0055] 또한 데이터 전송부(130)는 사용자의 식별 정보 및 보호 대상 객체에 대응하는 사용자의 사용 권한 정보 중 적어도 하나를 포함하는 암호화 정보를 디지털 콘텐츠의 소스코드와 함께 사용자 단말(300)로 전송할 수 있다.

[0056] 또한 암호화 정보에는 복수의 사용자의 식별 정보 및 각각의 식별 정보에 대응하여 별도로 설정된 사용 권한 정보가 포함될 수 있다. 이러한 경우, 사용자 단말(300)에 설치된 DRM 프로그램은 사용자로부터 입력받은 식별 정보와 암호화 정보에 포함된 식별 정보를 대비하여 대응하는 사용 권한에 따라 디지털 콘텐츠의 암호화된 보호 대상 객체를 복호화할 수 있다.

[0057] 도 6은 본 발명에 따른 객체별 권한에 따른 콘텐츠 제공 장치(200)에 대한 바람직한 실시예의 구성을 도시한 블록도이다.

[0058] 앞에서 설명한 바와 같이, 본 발명에 따른 객체별 권한에 따른 콘텐츠 제공 장치(200)는 사용자 단말(300)에 설

치되는 DRM 프로그램의 형태로 구현될 수 있다.

[0059] 도 6을 참조하면, 본 발명에 따른 객체별 권한에 따른 콘텐츠 제공 장치(200)는 검출부(210), 복호화부(220) 및 전송부(230)를 포함한다.

[0060] 검출부(210)는 사용자 단말(300)을 통해 출력되는 디지털 콘텐츠의 소스코드로부터 디지털 콘텐츠를 구성하는 복수의 객체 중 보호 대상 객체에 대응하는 암호화된 데이터 영역을 검출한다.

[0061] 구체적으로, 검출부(210)는 본 발명에 따른 콘텐츠의 객체별 권한 설정 장치(100)의 데이터 암호화부(120)에 의해 암호화된 데이터 영역을 검출할 수 있다. 또한 암호화된 데이터 영역을 포함하는 디지털 콘텐츠의 소스코드를 데이터 전송부(130) 또는 사용자 단말(300)로부터 전송받을 수 있다.

[0062] 그리고 복호화부(220)는 사용자로부터 입력받은 사용자의 식별 정보에 대응하여 사전에 설정된 사용자의 사용 권한 정보에 따라 암호화된 데이터 영역을 복호화한다.

[0063] 그 후, 전송부(230)는 복호화된 데이터 영역을 디지털 콘텐츠의 포맷에 대응하는 전용 프로그램에 전송한다. 전용 프로그램은 사용자 단말(300)에 설치되어 있을 수 있다. 또한 전송부(230)는 복호화된 데이터 영역 및 복호화된 데이터 영역에 대응하는 사용자의 사용 권한 정보를 전용 프로그램에 전송함으로써, 전용 프로그램에서 사용 권한 정보를 참고하여 디지털 콘텐츠를 실행하도록 할 수 있다.

[0064] 한편, 복호화부(220)는 사용자로부터 보호 대상 객체에 대응하는 결제 정보가 입력되면 결제 정보에 대응하여 암호화된 데이터 영역을 복호화할 수 있다. 이때 보호 대상 객체가 복수 개이고 사용자가 일부 객체에 대응하는 금액만을 결제한 경우, 복호화부(220)는 결제 정보에 포함된 금액 정보에 대응하는 개수만큼 암호화된 데이터 영역을 복호화할 수 있다.

[0065] 예를 들어, 기존에는 논문 사이트에서 유료로 제공되는 특정 논문을 다운로드 받기 위해서 논문에 맞는 가격을 결제해야 사용자가 논문을 제공받을 수 있었고, 결제가 이루어지지 않으면 논문 전체를 다운로드 할 수 없었다.

[0066] 그러나 본 발명에 따른 객체별 권한에 따른 콘텐츠 제공 장치(200), 즉 DRM 프로그램을 사용하면 결제 여부에 상관없이 논문이 먼저 다운받아 지고 대신 논문을 실행하면 보호 대상 객체들이 열리지 않는 방식으로 서비스를 구현할 수 있다. 보호 대상 객체를 제공받고 싶을 경우 DRM 프로그램을 설치하고 결제 정보를 입력하면 논문을 제공받을 수 있다.

[0067] 또한, 결제 금액에 따라 논문에서 출력되는 보호 대상 객체의 개수를 차별화할 수 있다. 예를 들어, 1000원 결제 시 다섯 개의 보호 대상 객체 중 한 개가 출력되고 5000원 결제 시 다섯 개의 보호 대상 객체 모두 출력될 수 있다.

[0068] 도 7은 본 발명에 따른 콘텐츠의 객체별 권한 설정 방법에 대한 바람직한 실시예의 수행과정을 도시한 흐름도이다.

[0069] 데이터 검출부(110)는 복수의 객체를 포함하는 디지털 콘텐츠의 소스코드 중 복수의 객체 각각에 대응되는 부분인 데이터 영역을 복수의 객체별로 검출한다(S710).

[0070] 데이터 암호화부(120)는 복수의 데이터 영역 중 보호 대상 객체에 대응하는 데이터 영역을 암호화한다. 구체적으로, 데이터 암호화부(120)는 보호 대상 객체에 대응하는 데이터 영역은 DRM 프로그램에 의해 추출되고, 보호 대상 객체 이외의 객체에 대응하는 데이터 영역은 디지털 콘텐츠의 포맷에 대응하는 프로그램에 의해 추출되도록 할 수 있다(S720).

[0071] 그리고 데이터 암호화부(120)는 사용자 단말(300)에서 DRM 프로그램이 실행되지 않는 경우 또는 사용자에게 보호 대상 객체에 대한 사용 권한이 없는 경우에, 사용자의 단말을 통해 보호 대상 객체를 대신하여 접근 불가 정보가 출력되도록 소스코드에 접근 불가 정보에 대응하는 데이터 영역을 삽입할 수 있다.

[0072] 데이터 전송부(130)는 암호화된 데이터 영역을 포함하는 디지털 콘텐츠의 소스코드를 사용자 단말(300)로 전송한다(S730).

[0073] 도 8은 본 발명에 따른 객체별 권한에 따른 콘텐츠 제공 방법에 대한 바람직한 실시예의 수행 과정을 도시한 흐름도이다.

[0074] 검출부(210)는 사용자 단말(300)을 통해 출력되는 디지털 콘텐츠의 소스코드로부터 디지털 콘텐츠를 구성하는 복수의 객체 중 보호 대상 객체에 대응하는 암호화된 데이터 영역을 검출한다(S810).

[0075] 검출부(210)는 본 발명에 따른 콘텐츠의 객체별 권한 설정 장치(100)의 데이터 암호화부(120)에 의해 암호화된 데이터 영역을 검출할 수 있다. 또한 암호화된 데이터 영역을 포함하는 디지털 콘텐츠의 소스코드를 데이터 전송부(130)나 사용자 단말(300)로부터 전송받을 수 있다.

[0076] 그리고 복호화부(220)는 사용자로부터 입력받은 사용자의 식별 정보에 대응하여 사전에 설정된 사용자의 사용 권한 정보에 따라 암호화된 데이터 영역을 복호화한다(S820).

[0077] 그 후, 전송부(230)는 복호화된 데이터 영역을 디지털 콘텐츠의 포맷에 대응하는 프로그램에 전송한다(S830). 디지털 콘텐츠의 포맷에 대응하는 전용 프로그램은 사용자 단말(300)에 설치되어 있을 수 있다.

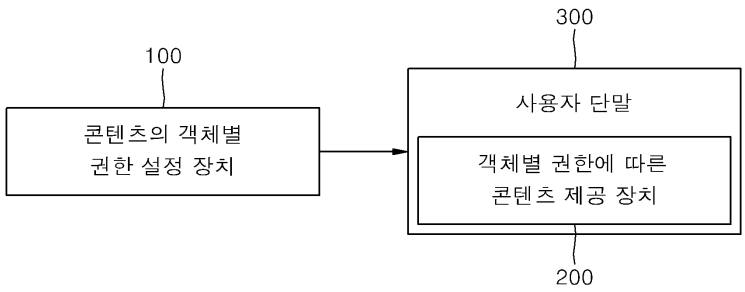
[0078] 또한 전송부(230)는 복호화된 데이터 영역 및 복호화된 데이터 영역에 대응하는 사용자의 사용 권한 정보를 전용 프로그램에 전송할 수 있다.

[0079] 본 발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

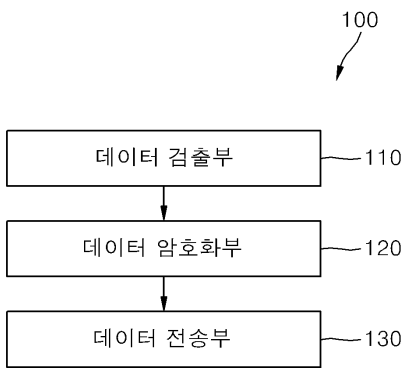
[0080] 이상에서 본 발명의 바람직한 실시예에 대해 도시하고 설명하였으나, 본 발명은 상술한 특정의 바람직한 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형 실시가 가능한 것은 물론이고, 그와 같은 변경은 청구범위 기재의 범위 내에 있게 된다.

도면

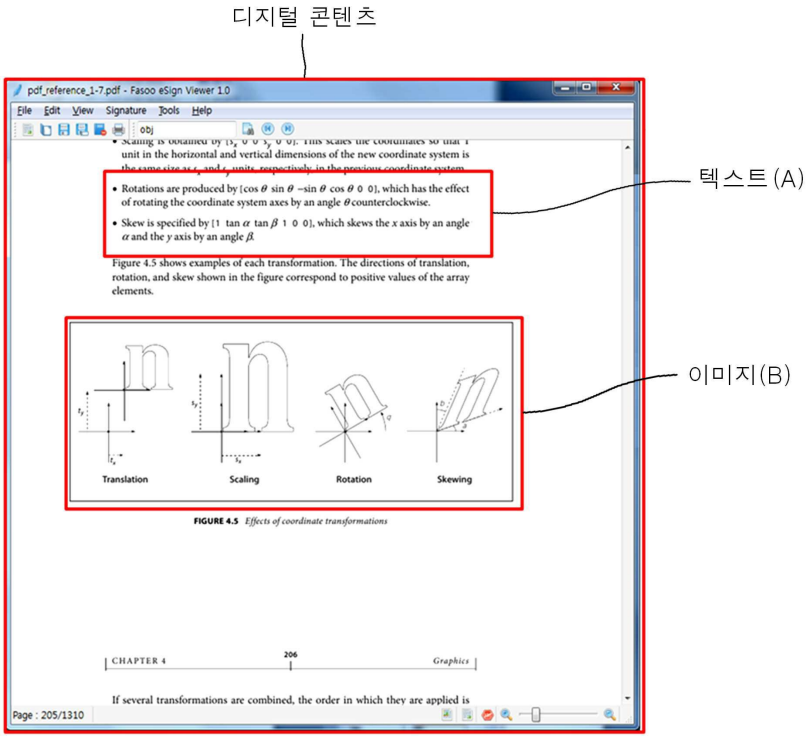
도면1



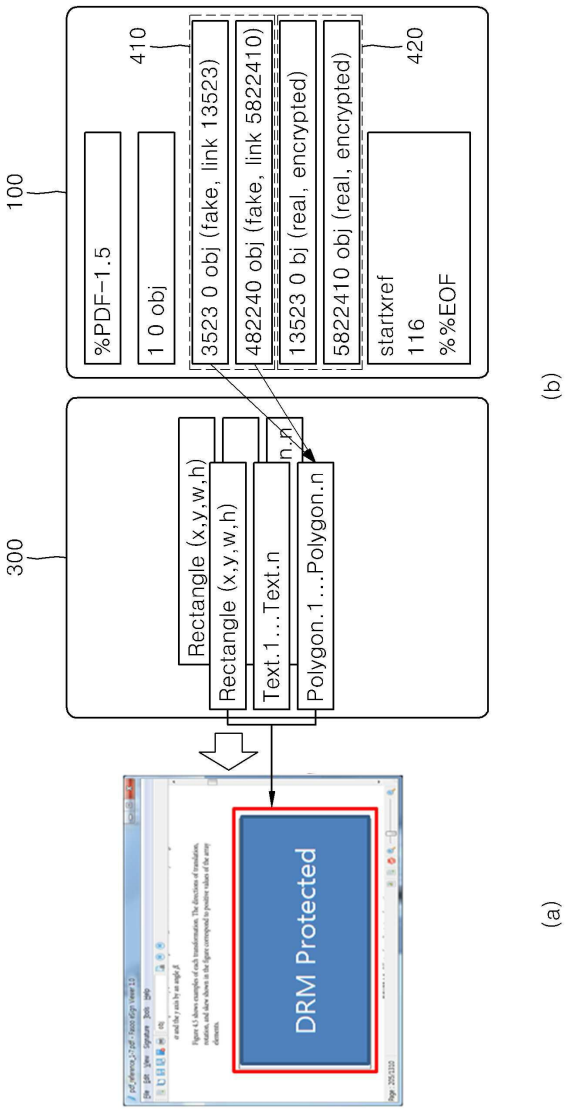
도면2



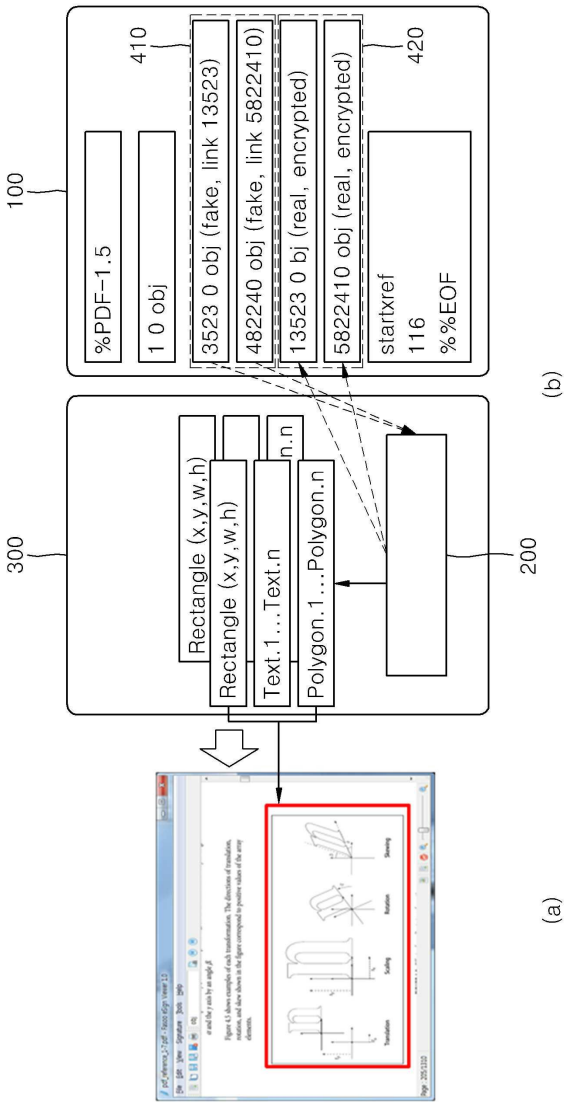
도면3


디지털 콘텐츠
pdf_reference_1-7.pdf - Fasoo eSign Viewer 1.0
File Edit View Signature Tools Help
텍스트(A)
이미지(B)
Translation
Scaling
Rotation
Skewing
FIGURE 4.5 Effects of coordinate transformations
CHAPTER 4
206
Graphics
Page : 205/1310

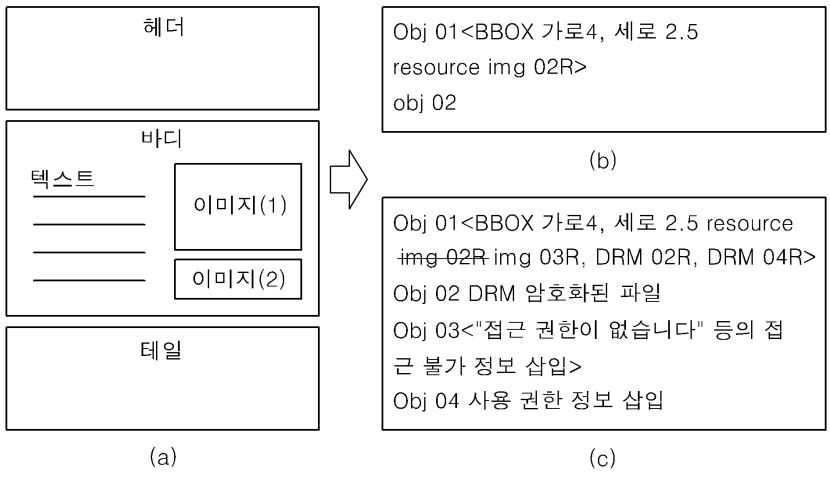
도면4a


100
%PDF-1.5
1 0 obj
410
3523 0 obj (fake, link 13523)
482240 obj (fake, link 5822410)
13523 0 bj (real, encrypted)
5822410 obj (real, encrypted)
startxref
116
%%EOF
420
(b)
300
Rectangle (x,y,w,h)
Rectangle (x,y,w,h)
Text.1...Text.n
n,n
Polygon.1...Polygon.n
DRM Protected
(a)

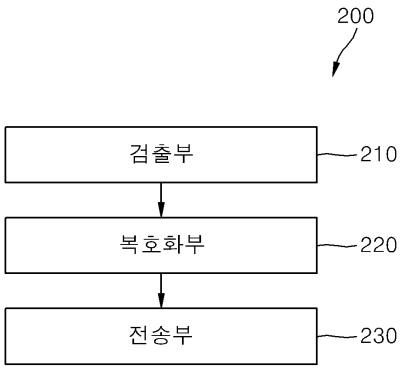
도면4b


100
410
420
%PDF-1.5
1 0 obj
3523 0 obj (fake, link 13523)
482240 obj (fake, link 5822410)
13523 0 bj (real, encrypted)
5822410 obj (real, encrypted)
startxref
116
%%EOF
(b)
300
200
Rectangle (x,y,w,h)
Rectangle (x,y,w,h)
Text.1...Text.n
Polygon.1...Polygon.n
(a)

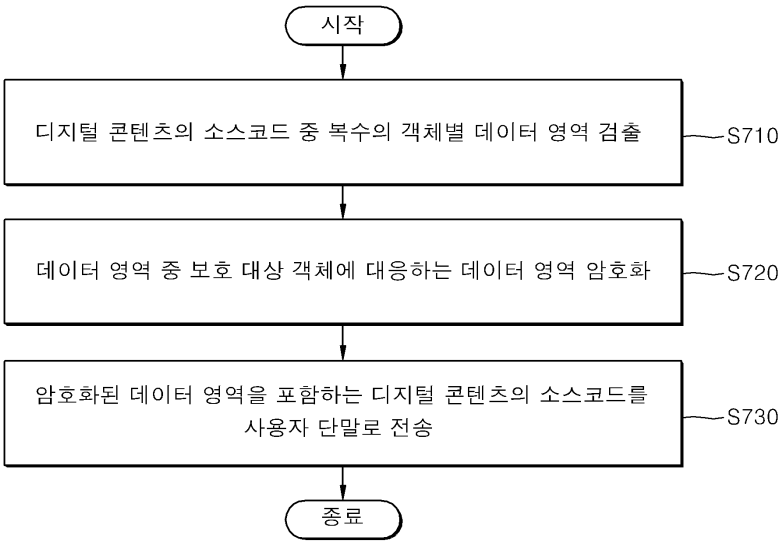
도면5


헤더
바디
텍스트
이미지(1)
이미지(2)
테일
(a)
Obj 01<BBOX 가로4, 세로 2.5
resource img 02R>
obj 02
(b)
Obj 01<BBOX 가로4, 세로 2.5 resource
~~img 02R~~ img 03R, DRM 02R, DRM 04R>
Obj 02 DRM 암호화된 파일
Obj 03<"접근 권한이 없습니다" 등의 접
근 불가 정보 삽입>
Obj 04 사용 권한 정보 삽입
(c)

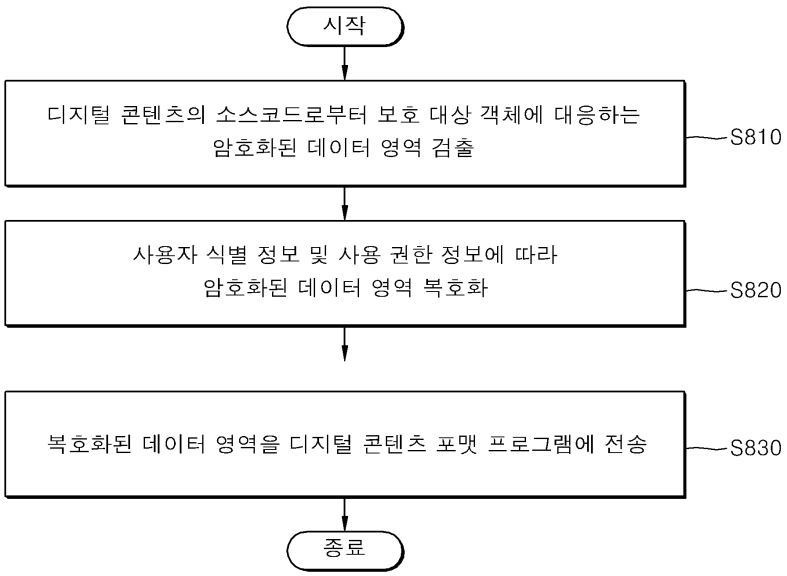
도면6


200
검출부
210
복호화부
220
전송부
230

도면7


시작
디지털 콘텐츠의 소스코드 중 복수의 객체별 데이터 영역 검출
S710
데이터 영역 중 보호 대상 객체에 대응하는 데이터 영역 암호화
S720
암호화된 데이터 영역을 포함하는 디지털 콘텐츠의 소스코드를 사용자 단말로 전송
S730
종료

도면8


시작
디지털 콘텐츠의 소스코드로부터 보호 대상 객체에 대응하는 암호화된 데이터 영역 검출
S810
사용자 식별 정보 및 사용 권한 정보에 따라 암호화된 데이터 영역 복호화
S820
복호화된 데이터 영역을 디지털 콘텐츠 포맷 프로그램에 전송
S830
종료