(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2010 년 2 월 11 일 (11.02.2010)

PCT

(10) 국제공개번호
WO 2010/016667 A2

(51) 국제특허분류:
G06F 21/00 (2006.01)

(21) 국제출원번호: PCT/KR2009/004029

(22) 국제출원일: 2009 년 7 월 21 일 (21.07.2009)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2008-0077583 2008 년 8 월 7 일 (07.08.2008) KR

(71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): **주식회사 씨디네트웍스 (CDNETWORKS CO., LTD.)** [KR/KR]; 서울특별시 강남구 역삼동 828-7 한동빌딩 2 층, 135-935 Seoul (KR).

(72) 발명자; 겸
(75) 발명자/출원인 (US 에 한하여): **원성욱 (WON, Sung-Wook)** [KR/KR]; 서울특별시 강남구 역삼동 828-7, 135-935 Seoul (KR).

(74) 대리인: **반중혁 (BAN, Jung-Hyuk)**; 서울시 서초구 서초동 1363-2 창원빌딩 4 층, 137-070 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, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 유럽 (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, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

WO 2010/016667 A2

(54) **Title**: METHOD AND APPARATUS FOR PROTECTING DIGITAL CONTENT USING HARDWARE IDENTIFICATION INFORMATION

(54) **발명의 명칭**: 하드웨어 아이디 정보를 이용한 디지털 콘텐츠의 보호 방법 및 장치

(57) **Abstract**: A method and an apparatus for protecting digital content using hardware identification information are disclosed. According to one embodiment of the present invention, a method for protecting digital content using hardware identification information includes the steps of acquiring hardware identification information of a device connected to a client, comparing the acquired hardware identification information with preset hardware identification information, and suspending the reproduction of digital content if the acquired hardware identification information corresponds to the preset hardware identification information. The present invention protects digital content even when digital content is output via another external device, and prevents digital content being output via another external device from being stored again by using another device.

(57) **요약서**: 하드웨어 아이디 정보를 이용한 콘텐츠 보호 방법 및 장치가 개시된다. 본 발명의 바람직한 일 실시예에 따르면, 클라이언트와 연결된 장치의 하드웨어 아이디 정보를 획득하여, 획득된 하드웨어 아이디 정보를 미리 설정된 하드웨어 아이디 정보와 비교하고, 비교 결과 획득된 하드웨어 아이디 정보가 미리 설정된 하드웨어 아이디 정보에 해당하는 경우 디지털 콘텐츠의 재생을 차단한다. 본 발명에 따르면, 다른 외부 장치를 통해 디지털 콘텐츠가 출력되는 경우에도 디지털 콘텐츠를 보호할 수 있고, 다른 외부 장치로 출력되는 디지털 콘텐츠를 다시 다른 장치를 이용하여 저장하는 것을 방지할 수 있는 장점이 있다.

명세서

발명의 명칭: 하드웨어 아이디 정보를 이용한 디지털 콘텐츠의 보호 방법 및 장치

기술분야

[1] 본 발명은 콘텐츠의 보호 방법 및 장치에 관한 것으로서, 보다 상세하게는 디지털 콘텐츠가 재생되는 장치와 연결될 수 있는 외부 장치들의 화면을 통해서도 출력될 수 있는 디지털 콘텐츠를 보호할 수 있는 방법 및 장치에 관한 것이다.

[2]

배경기술

[3] 인터넷과 같은 통신 기술의 발달과 컴퓨터와 같은 디지털 장치들의 발달로 다양한 디지털 콘텐츠의 획득 및 저장이 가능하게 되었다.

[4] 그러나 저장 및 전송 그리고 복제가 용이한 디지털 콘텐츠의 특성상 정당한 권원없이 디지털 콘텐츠를 이용하거나 복제하는 경우가 빈번하게 발생된다.

[5] 이러한 디지털 콘텐츠의 보호를 위해 디지털 콘텐츠 자체의 암호화, 디지털 콘텐츠의 사용을 위한 인증 등 다양한 방법과 기술이 개발되고 있다.

[6] 그러나 이러한 종래의 디지털 콘텐츠의 보호 방법들은 디지털 콘텐츠 자체의 복제를 방지하거나 정당한 권리자의 사용을 인증하기 위한 방안에 지나지 않는다.

[7] 따라서 종래의 디지털 콘텐츠 보호 방법으로는 디지털 콘텐츠를 다른 외부 장치를 이용하여 다수가 시청하거나 다른 외부 장치에서 출력되는 디지털 콘텐츠를 다시 다른 장치를 이용하여 저장하는 경우 이를 방지하기 어려운 문제점이 있다.

[8] 예를 들어, 동영상 강의 시청시 1명의 사용자만 회원으로 가입하여 동영상 강의를 수신하고 다른 외부 장치인 예를 들어 프로젝터(projector)를 통해 수신된 동영상 강의를 출력하여 다수가 시청하는 경우 종래의 디지털 콘텐츠의 보호 방법으로는 디지털 콘텐츠를 보호하기 어려운 문제점이 있다.

[9] 또한, 외부 장치를 통해 출력되는 동영상 강의와 같은 디지털 콘텐츠를 다시 다른 장치를 이용하여 녹화하는 등 저장하는 경우 이를 방지하기 어려운 문제점이 있다.

[10]

발명의 상세한 설명

기술적 과제

[11] 상기한 바와 같은 종래의 문제점을 해결하기 위해, 본 발명은 외부 장치를 통해 디지털 콘텐츠가 출력되는 경우에도 디지털 콘텐츠를 보호할 수 있는 디지털 콘텐츠 보호 방법 및 장치를 제안하는 것이다.

[12] 또한, 외부 장치를 통해 출력되는 디지털 콘텐츠를 다시 다른 장치를 이용하여 저장하는 것을 방지할 수 있는 디지털 콘텐츠 보호 방법 및 장치를 제안하는 것이다.

[13] 본 발명의 또 다른 목적들은 이하의 실시예에 대한 설명을 통해 쉽게 이해될 수 있을 것이다.

[14]

과제 해결 수단

[15] 상기한 바와 같은 목적을 달성하기 위해, 본 발명의 일 측면에 따르면 디지털 콘텐츠 보호 방법이 제공된다.

[16] 본 발명의 바람직한 일 실시예에 따르면, 외부 장치와 연결되는 클라이언트(client)에서 수행되는 디지털 콘텐츠(digital contents)의 보호 방법에 있어서, 상기 외부 장치의 하드웨어 아이디 정보를 획득하는 단계(a); 상기 획득된 하드웨어 아이디 정보를 미리 설정된 외부 장치의 하드웨어 아이디 정보와 비교하는 단계(b)-상기 미리 설정된 외부 장치의 하드웨어 아이디 정보는 상기 클라이언트에서 재생되는 화면이 상기 외부 장치의 화면을 통해 출력되는 것을 차단하도록 하는 외부 장치의 하드웨어 아이디 정보임-; 및 상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 디지털 콘텐츠의 재생을 차단하는 단계(c)를 포함하는 것을 특징으로 하는 디지털 콘텐츠의 보호 방법이 제공된다.

[17] 상기 디지털 콘텐츠는 상기 클라이언트에서 저장된 후 상기 클라이언트에서 재생되는 다운로드 앤드 플레이(download and paly) 방식의 디지털 콘텐츠일 수 있다.

[18] 상기 디지털 콘텐츠는 상기 클라이언트에 실시간으로 재생되는 스트리밍(streaming) 방식의 디지털 콘텐츠일 수 있다.

[19] 상기 단계(a)에서 상기 외부 장치의 하드웨어 아이디 정보는 상기 클라이언트의 플러그앤플레이(Plug and Play) 기능에 의해 상기 클라이언트에서 획득될 수 있다.

[20] 상기 단계(c)에서 상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 디지털 콘텐츠가 상기 외부 장치로 출력되는 것을 차단할 수 있다.

[21] 상기 단계(c)에서 상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 클라이언트로 상기 디지털 콘텐츠를 전송하는 미디어 서버로 상기 디지털 콘텐츠의 전송 중단을 요청할 수 있다.

[22]

[23] 본 발명의 바람직한 다른 일 실시예에 따르면, 외부 장치와 연결되는 클라이언트(client) 및 상기 클라이언트로 디지털 콘텐츠(digital contents)를

전송하는 미디어 서버(media server)를 포함하는 콘텐츠 전송 시스템에서 상기 미디어 서버에서 수행되는 디지털 콘텐츠의 보호 방법에 있어서, 상기 클라이언트로부터 상기 외부 장치의 하드웨어 아이디 정보를 수신하는 단계(a); 상기 수신된 하드웨어 아이디 정보를 미리 설정된 외부 장치의 하드웨어 아이디 정보와 비교하는 단계(b) 상기 미리 설정된 외부 장치의 하드웨어 아이디 정보는 상기 클라이언트에서 재생되는 화면이 상기 외부 장치의 화면을 통해 출력되는 것을 차단하도록 하는 외부 장치의 하드웨어 아이디 정보임-; 및 상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 디지털 콘텐츠의 전송을 중단하는 단계(c)를 포함하는 것을 특징으로 하는 디지털 콘텐츠의 보호 방법이 제공된다.

[24] 상기 디지털 콘텐츠는 상기 클라이언트에서 저장된 후 상기 클라이언트에서 재생되는 다운로드 앤드 플레이(download and paly) 방식의 디지털 콘텐츠일 수 있다.

[25] 상기 디지털 콘텐츠는 상기 클라이언트에 실시간으로 재생되는 스트리밍(streaming) 방식의 디지털 콘텐츠일 수 있다.

[26] 상기 단계(a)에서 상기 외부 장치의 하드웨어 아이디 정보는 상기 클라이언트의 플러그앤플레이(Plug and Play) 기능에 의해 상기 클라이언트에서 획득될 수 있다.

[27] 상기 단계(c)에서 상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 클라이언트로 상기 디지털 콘텐츠가 상기 외부 장치로 출력되는 것을 차단하도록 하는 신호를 전송할 수 있다.

[28] 상기 단계(c)에서 상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 클라이언트로 상기 디지털 콘텐츠가 상기 클라이언트에서 재생되는 것을 차단하도록 하는 신호를 전송할 수 있다.

[29]

[30]

[31] *본 발명의 다른 측면에 의하면, 디지털 콘텐츠 보호 장치가 제공된다.

[32] 본 발명의 바람직한 일 실시예에 따르면, 디지털 콘텐츠(digital contents)의 보호 장치에 있어서, 클라이언트(client)와 연결되는 외부 장치의 하드웨어 아이디 정보를 획득하는 하드웨어 아이디 정보 획득부; 상기 획득된 하드웨어 아이디 정보를 미리 설정된 외부 장치의 하드웨어 아이디 정보와 비교하는 하드웨어 아이디 정보 비교부- 상기 미리 설정된 외부 장치의 하드웨어 아이디 정보는 상기 클라이언트에서 재생되는 화면이 상기 외부 장치의 화면을 통해 출력되는 것을 차단하도록 하는 외부 장치의 하드웨어 아이디 정보임-; 및 상기 하드웨어 아이디 정보 비교부의 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 디지털

콘텐츠의 재생을 중단하는 콘텐츠 재생 차단부를 포함하는 것을 특징으로 하는 디지털 콘텐츠의 보호 장치가 제공된다.

[33] 상기 디지털 콘텐츠는 상기 클라이언트에서 저장된 후 상기 클라이언트에서 재생되는 다운로드 앤드 플레이(download and paly) 방식의 디지털 콘텐츠일 수 있다.

[34] 상기 디지털 콘텐츠는 상기 클라이언트에 실시간으로 재생되는 스트리밍(streaming) 방식의 디지털 콘텐츠일 수 있다.

[35] 상기 외부 장치의 하드웨어 아이디 정보는 상기 클라이언트의 플러그앤플레이(Plug and Play) 기능에 의해 상기 클라이언트에서 획득될 수 있다.

[36] 상기 콘텐츠 재생 차단부는 상기 디지털 콘텐츠가 상기 외부 장치로 출력되는 것을 차단할 수 있다.

[37] 상기 콘텐츠 재생 차단부는 상기 클라이언트로 상기 디지털 콘텐츠를 전송하는 미디어 서버로 상기 디지털 콘텐츠의 전송 중단을 요청할 수 있다.

[38]

[39] 본 발명의 바람직한 다른 일 실시예에 따르면, 디지털 콘텐츠(digital contents)의 보호 장치에 있어서, 클라이언트(client)로부터 수신된 상기 클라이언트와 연결되는 외부 장치의 하드웨어 아이디 정보를 미리 설정된 외부 장치의 하드웨어 아이디 정보와 비교하는 하드웨어 아이디 정보 비교부 상기 미리 설정된 외부 장치의 하드웨어 아이디 정보는 상기 클라이언트에서 재생되는 화면이 상기 외부 장치의 화면을 통해 출력되는 것을 차단하도록 하는 외부 장치의 하드웨어 아이디 정보임-;및 상기 하드웨어 아이디 정보 비교부의 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 디지털 콘텐츠의 전송을 차단하는 콘텐츠 전송 차단부를 포함하는 것을 특징으로 하는 디지털 콘텐츠의 보호 장치가 제공된다.

[40] 상기 디지털 콘텐츠는 상기 클라이언트에서 저장된 후 상기 클라이언트에서 재생되는 다운로드 앤드 플레이(download and paly) 방식의 디지털 콘텐츠일 수 있다.

[41] 상기 디지털 콘텐츠는 상기 클라이언트에 실시간으로 재생되는 스트리밍(streaming) 방식의 디지털 콘텐츠일 수 있다.

[42] 상기 외부 장치의 하드웨어 아이디 정보는 상기 클라이언트의 플러그앤플레이(Plug and Play) 기능에 의해 상기 클라이언트에서 획득될 수 있다.

[43] 상기 콘텐츠 전송 차단부는 상기 클라이언트로 상기 디지털 콘텐츠가 상기 외부 장치로 출력되는 것을 차단하도록 하는 신호를 전송할 수 있다.

[44] 상기 콘텐츠 전송 차단부는 상기 클라이언트로 상기 디지털 콘텐츠가 상기 클라이언트에서 재생되는 것을 차단하도록 하는 신호를 전송할 수 있다.

[45]

[46] 본 발명의 다른 측면에 의하면, 디지털 콘텐츠의 보호 방법을 구현하기 위한 프로그램을 기록한 기록매체가 제공된다.

[47] 본 발명의 바람직한 일 실시예에 따르면, 외부 장치와 연결되는 클라이언트(client)에서 수행되는 디지털 콘텐츠(digital contents)의 보호 방법 방법이 구현되도록, 상기 클라이언트에 의해 실행될 수 있는 명령어들의 프로그램이 구현되어 있으며 상기 클라이언트에 의해 판독될 수 있는 프로그램을 기록한 기록매체에 있어서, 상기 외부 장치의 하드웨어 아이디 정보를 획득하는 단계(a); 상기 획득된 하드웨어 아이디 정보를 미리 설정된 외부 장치의 하드웨어 아이디 정보와 비교하는 단계(b)-상기 미리 설정된 외부 장치의 하드웨어 아이디 정보는 상기 클라이언트에서 재생되는 화면이 상기 외부 장치의 화면을 통해 출력되는 것을 차단하도록 하는 외부 장치의 하드웨어 아이디 정보임-; 및 상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 디지털 콘텐츠의 재생을 차단하는 단계(c)를 포함하는 것을 특징으로 하는 디지털 콘텐츠의 보호 방법을 구현하기 위한 프로그램을 기록한 기록매체가 제공된다.

[48] 상기 디지털 콘텐츠는 상기 클라이언트에서 저장된 후 상기 클라이언트에서 재생되는 다운로드 앤드 플레이(download and paly) 방식의 디지털 콘텐츠일 수 있다.

[49] 상기 디지털 콘텐츠는 상기 클라이언트에 실시간으로 재생되는 스트리밍(streaming) 방식의 디지털 콘텐츠일 수 있다.

[50] 상기 단계(a)에서 상기 외부 장치의 하드웨어 아이디 정보는 상기 클라이언트의 플러그앤플레이(Plug and Play) 기능에 의해 상기 클라이언트에서 획득될 수 있다.

[51] 상기 단계(c)에서 상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 디지털 콘텐츠가 상기 외부 장치로 출력되는 것을 차단할 수 있다.

[52] 상기 단계(c)에서 상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 클라이언트로 상기 디지털 콘텐츠를 전송하는 미디어 서버로 상기 디지털 콘텐츠의 전송 중단을 요청할 수 있다.

[53]

[54] 본 발명의 바람직한 다른 일 실시예에 따르면, 외부 장치와 연결되는 클라이언트(client) 및 상기 클라이언트로 디지털 콘텐츠(digital contents)를 전송하는 미디어 서버(media server)를 포함하는 콘텐츠 전송 시스템에서 상기 미디어 서버에서 수행되는 디지털 콘텐츠의 보호 방법이 구현되도록, 상기 미디어 서버에 의해 실행될 수 있는 명령어들의 프로그램이 구현되어 있으며 상기 미디어 서버에 의해 판독될 수 있는 프로그램을 기록한 기록매체에 있어서,

상기 클라이언트로부터 상기 클라이언트와 연결된 외부 장치의 하드웨어 아이디 정보를 수신하는 단계(a); 상기 획득된 하드웨어 아이디 정보를 미리 설정된 외부 장치의 하드웨어 아이디 정보와 비교하는 단계(b)-상기 미리 설정된 외부 장치의 하드웨어 아이디 정보는 상기 클라이언트에서 재생되는 화면이 상기 외부 장치의 화면을 통해 출력되는 것을 차단하도록 하는 외부 장치의 하드웨어 아이디 정보임-; 및 상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 디지털 콘텐츠의 전송을 중단하는 단계(c)를 포함하는 것을 특징으로 하는 디지털 콘텐츠의 보호 방법을 구현하기 위한 프로그램을 기록한 기록매체가 제공된다.

[55] 상기 디지털 콘텐츠는 상기 클라이언트에서 저장된 후 상기 클라이언트에서 재생되는 다운로드 앤드 플레이(download and paly) 방식의 디지털 콘텐츠일 수 있다.

[56] 상기 디지털 콘텐츠는 상기 클라이언트에 실시간으로 재생되는 스트리밍(streaming) 방식의 디지털 콘텐츠일 수 있다.

[57] 상기 단계(a)에서 상기 외부 장치의 하드웨어 아이디 정보는 상기 클라이언트의 플러그앤플레이(Plug and Play) 기능에 의해 상기 클라이언트에서 획득될 수 있다.

[58] 상기 단계(c)에서 상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 클라이언트로 상기 디지털 콘텐츠가 상기 외부 장치로 출력되는 것을 차단하도록 하는 신호를 전송할 수 있다.

[59] 상기 단계(c)에서 상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 클라이언트로 상기 디지털 콘텐츠가 상기 클라이언트에서 재생되는 것을 차단하도록 하는 신호를 전송할 수 있다.

[60]

발명의 효과

[61] 이상에서 설명한 바와 같이, 본 발명에 의한 하드웨어 아이디 정보를 이용한 디지털 콘텐츠 보호 방법 및 장치에 의하면, 외부 장치를 통해 디지털 콘텐츠가 출력되는 경우에도 디지털 콘텐츠를 보호할 수 있는 장점이 있다.

[62] 또한, 외부 장치를 통해 출력되는 디지털 콘텐츠를 다시 다른 장치를 이용하여 저장하는 것을 방지할 수 있는 장점이 있다.

[63]

도면의 간단한 설명

[64] 도 1은 본 발명의 바람직한 일 실시예에 따른 디지털 콘텐츠 보호 방법이 적용될 수 있는 디지털 콘텐츠 전송 시스템의 구성을 도시한 구성도.

[65] 도 2는 본 발명의 바람직한 제1 실시예에 따라 디지털 콘텐츠 보호 방법이 구현되는 순서를 도시한 순서도.

[66] 도 3은 본 발명의 바람직한 제2 실시예에 따라 디지털 콘텐츠 보호 방법이 구현되는 순서를 도시한 순서도.

[67] 도 4는 본 발명의 바람직한 제1 실시예에 따른 디지털 콘텐츠 보호 방법이 구현하기 위해 클라이언트에 설치될 수 있는 콘텐츠 보호 모듈의 구성을 도시한 구성도.

[68] 도 5는 본 발명의 바람직한 다른 일 실시예에 따른 디지털 콘텐츠 보호 방법이 구현하기 위한 콘텐츠 보호 장치의 구성을 도시한 구성도.

[69]

발명의 실시를 위한 형태

[70] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[71] 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다. 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[72] 제1, 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

[73] 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다.

[74] 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[75] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다.

[76] 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[77] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다.

[78] 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을

포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[79] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다.

[80] 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[81]

[82] 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 실시예를 상세히 설명하되, 도면 부호에 관계없이 동일하거나 대응하는 구성 요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다.

[83] 먼저 도 1을 참조하여 본 발명의 바람직한 일 실시예에 따른 디지털 콘텐츠 보호 방법이 적용될 수 있는 콘텐츠 전송 시스템의 구성을 살펴본다.

[84] 도 1은 본 발명의 바람직한 일 실시예에 따른 디지털 콘텐츠 보호 방법이 적용될 수 있는 디지털 콘텐츠 전송 시스템의 구성을 도시한 구성도이다.

[85] 한편, 이하에서는 설명의 편의를 위해 특별한 구분이 없는 한 디지털 콘텐츠의 경우 디지털 콘텐츠 및 콘텐츠라는 용어를 모두 구분없이 사용하기로 한다.

[86] 도 1에 도시된 바와 같이, 본 발명의 바람직한 일 실시예에 따른 콘텐츠 전송 네트워크(Contents Delivery Networks) 시스템은 프로젝터(projector)(100), 클라이언트(110) 및 미디어 서버(130)를 포함할 수 있다.

[87] 한편, 도 1에서는 설명의 편의를 위해 구성 요소 각각을 하나씩만 도시하였으나, 그 구성요소들이 1개 이상 존재할 수 있음은 자명하다.

[88] 또한, 도 1에서는 디지털 콘텐츠를 화면을 통해 출력할 수 있는 외부 장치로서 프로젝터(100)를 예시하였으나 디지털 신호를 수신하여 수신된 디지털 신호를 디스플레이 화면을 통해 출력할 수 있는 장치이면 아무런 제한이 없다.

[89] 외부 장치(100)는 예를 들면, 도 1에 예시한 프로젝터뿐만 아니라 디지털 TV, 사용자 퍼스널 컴퓨터(PC)의 모니터, 휴대 전화, 개인 휴대 단말기(PDA: Personal Digital Assistant), PMP(Portable Mutimedia Player) 등의 다양한 디지털 장치들이 가능하다.

[90] 클라이언트(110)는 통신망(120)을 통해 연결되어 미디어 서버(130)에 접속하여 디지털 콘텐츠를 수신할 수 있고, 프로젝터(100)와 같은 외부 장치로 화면을 출력할 수 있는 출력 단자와 같은 연결부가 포함되는 장치이다.

[91] 클라이언트(110)에는 미디어 서버(130)에 접속할 수 있게 하는 웹

브라우저(web browser)(미도시)과 콘텐츠가 재생되는 경우 재생에 필요한 어플리케이션(application)(미도시)이 포함될 수 있으며, 웹 브라우저와 어플리케이션은 클라이언트(110)에 프로그램의 형태로 설치될 수 있음은 자명하다.

[92] 또한, 프로젝터(100)와 같은 외부 장치로 화면을 통해 출력할 수 있는 연결부는 예를 들면, USB(Universal Serial Bus), HDMI(High Definition Multimedia Interface), DVI(digital video interactive), D-SUB(digital video interactive-sub) 등의 다양한 포트나 연결부가 가능하나 이에 한정되는 것은 아니다.

[93] 이러한 클라이언트(110)는 통신 기능을 구비하여 미디어 서버(130)에 접속될 수 있으며, 수신된 콘텐츠를 재생할 수 있는 프로그램의 설치가 가능하고, 재생되는 콘텐츠가 출력되는 디스플레이 화면을 포함하는 장치이며, 또한 프로젝터(100)와 같은 외부 장치로 화면을 출력할 수 있는 연결부를 포함할 수 있는 장치이면 아무런 제한이 없다.

[94] 클라이언트(110)는 예를 들면, 사용자 퍼스널 컴퓨터(PC)와 휴대 전화, 개인 휴대 단말기(PDA: Personal Digital Assistant), PMP(Portable Mutimedia Player) 등의 유무선 단말기 등이 있을 수 있으나 이에 한정되는 것은 아니다.

[95] 클라이언트(110)는 통신망(120)을 통해 미디어 서버(130)와 연결되며, 본 발명에서의 통신망(120)은 온라인 및 이동 통신망을 포함할 뿐만 아니라, 온라인은 TCP/IP 프로토콜 및 그 상위 계층에 존재하는 여러 서비스, 즉 HTTP(Hyper Text Transfer Protocol), Telnet, FTP(File Transfer Protocol), DNS(Domain Name System), SMTP(Simple Mail Transfer Protocol), SNMP(Simple Network Management Protocol), NFS(Network File Service) 등을 제공하는 전세계적인 개방형 네트워크 구조를 모두 포함한다.

[96] 또한, 이동 통신망은 기지국(BS: Base Station), 이동전화 교환국(MTSO: Mobile Telephone Switching Office), 홈 위치 등록기(HLR: Home Location Register) 이외에, 무선 패킷 데이터의 송수신을 가능하게 하는 액세스 게이트웨이(Access Gateway), PDSN(Packet Data Serving Node) 등과 같은 구성 요소를 추가로 포함한다.

[97] 미디어 서버(130)는 디지털 콘텐츠를 클라이언트(110)로 전송하며, 도 1에서는 미도시하였으나, 이러한 디지털 콘텐츠가 저장되는 데이터베이스(database)와 연결될 수 있다.

[98] 미디어 서버(130)에서 제공되는 디지털 콘텐츠는 클라이언트(100)에서 실시간으로 재생되는 스트리밍(streaming) 방식의 디지털 콘텐츠 뿐만 아니라 클라이언트(100)에서 다운로드(download)되어 재생되는 다운로드 앤드 플레이(download and play) 방식의 디지털 콘텐츠 등 아무런 제한이 없다.

[99] 특히 다운로드 앤드 플레이 방식의 디지털 콘텐츠의 경우 디지털 콘텐츠의 보호를 위한 DRM(Digital Rights Management) 인증 방법 등이 적용되어 있는 경우가 다수이므로 이 경우 종래의 DRM 인증 방법에 의한 디지털 콘텐츠의

보호 및 본 발명에 의한 디지털 콘텐츠의 보호 등 디지털 콘텐츠의 보호가 더욱 유용할 수 있게 된다.

[100]

[101] *또한, 스트리밍 방식의 경우에도 종래의 스트리밍 콘텐츠의 보호를 위한 다양한 인증 및 보호 방법과 함께 본 발명에 의한 디지털 콘텐츠 보호 방법을 이용함으로써 디지털 콘텐츠의 보호를 더욱 강화할 수 있게 된다.

[102] 한편, 도 1에서는 미디어 서버(130)만을 도시하였으나 클라이언트(110)를 통해 사용자에게 인증을 위해 필요한 정보를 입력하고, 디지털 콘텐츠에 대한 정보를 제공하는 웹 문서를 제공하는 웹 서버(미도시)가 더 포함될 수 있음은 당업자에게 자명하다.

[103] 이러한 콘텐츠 전송 네트워크 시스템에서 본 발명에 의한 디지털 콘텐츠 보호 방법은 다양한 방법에 의해 실시 가능하다.

[104] 먼저 클라이언트(110)에서 클라이언트(110)와 연결되는 외부 장치의 하드웨어 아이디(hardware ID)를 획득한다.

[105] 본 발명에서의 하드웨어 아이디는 하드웨어를 제조한 제조사별 또는 장치의 종류나 방식 등에 따라 해당 장치에 대하여 부여된 고유한 식별 정보이다.

[106] 이러한 하드웨어 아이디 정보는 새로운 장치가 연결되는 경우 자동으로 이를 인식할 수 있는 플러그앤플레이(Plug & Play) 기능을 이용하여 획득될 수 있다.

[107] 한편, 이러한 하드웨어 아이디 정보가 인식되면 인식된 하드웨어 아이디 정보를 이용하여 디지털 콘텐츠의 외부 출력을 차단한다.

[108] 디지털 콘텐츠의 외부 출력의 차단은 클라이언트(110)에서의 차단 및 미디어 서버(130)에서의 디지털 콘텐츠의 전송 중단에 의한 차단 등 다양한 방법에 의해 가능하며, 그 차단 방법은 아무런 제한이 없다.

[109] 한편, 이러한 하드웨어 아이디 정보를 이용하여 선택적으로 디지털 콘텐츠의 외부 출력을 차단하는 것도 가능하다.

[110] 전술한 바와 같이 하드웨어 아이디 정보는 하드웨어를 제조한 제조사별 또는 장치의 종류나 방식 등에 따라 부여된 고유한 식별 정보이므로 예를 들면, 하드웨어 아이디 정보로부터 장치의 종류, 제조사 및 모델 정보를 획득하는 것도 가능하다.

[111] 물론 이러한 정보의 획득은 하드웨어 아이디 정보를 획득하여 해당 하드웨어 아이디 정보와 이에 상응하는 하드웨어 정보를 매칭하여 이루어질 수 있으며, 이러한 정보의 매칭은 클라이언트 또는 서버 중 적어도 하나에서 수행될 수 있다.

[112] 따라서 이러한 하드웨어 아이디 정보로부터 하드웨어에 대한 다양한 정보를 획득하여 클라이언트와 연결되는 외부 장치에 대하여 선택적으로 디지털 콘텐츠의 재생 화면이 출력되지 않도록 차단하는 것도 가능하게 된다.

[113] 또한, 하드웨어 아이디 정보로부터 하드웨어의 종류 즉 외부 장치의 종류 정보도 획득할 수 있으므로 특정 장치에서는 디지털 콘텐츠의 재생 화면이

출력되지 않도록 차단하는 것도 가능할 수 있게 된다.

[114] 한편, 디지털 콘텐츠의 외부 출력의 차단은 클라이언트(110)와 연결되는 외부 장치에서 화면이 출력되는 것 그 자체를 차단하는 방법과 클라이언트(110)를 포함하여 디지털 콘텐츠의 재생이나 전송 자체가 중단되도록 하는 방법 등 다양한 방법으로 가능하다.

[115] 특히 디지털 콘텐츠가 다운로드 앤드 플레이 방식으로 재생되는 경우 디지털 콘텐츠의 재생을 차단하는 것이 본 발명에 의한 디지털의 보호 방법에 보다 효과적일 수 있으며, 디지털 콘텐츠가 스트리밍 방식으로 제공되는 경우 미디어 서버(130)에서의 전송을 차단하는 것이 효과적일 수 있으나 이에 한정되는 것은 아니다.

[116]

[117] 이하에서는 도 2 및 도 3을 참조하여 본 발명의 바람직한 일 실시예에 따라 디지털 콘텐츠 보호 방법이 구현되는 순서를 살펴보기로 한다.

[118] 도 2는 클라이언트(110)에서 하드웨어 아이디 정보를 획득하고 획득된 하드웨어 아이디 정보를 이용하여 콘텐츠의 출력 또는 재생을 중단을 판단하여 콘텐츠를 보호하는 경우를 예시한 것이고, 도 3은 클라이언트(110)에서는 하드웨어 아이디 정보만을 획득하여 미디어 서버(130)로 전달하고 미디어 서버(130)에서 콘텐츠의 출력 또는 재생을 중단을 판단하여 콘텐츠를 보호하는 경우를 예시한 것이다.

[119] 도 2의 예시와 같이 클라이언트(110)에서 하드웨어 아이디 정보의 획득 및 디지털 콘텐츠의 보호가 모두 이루어지는 경우 미디어 서버(130)의 부하가 줄어드는 등의 이점이 있으나 클라이언트(110)에서의 부하가 증가될 수 있다.

[120] 반면 도 3의 예시와 같이 클라이언트(110)에서 하드웨어 아이디 정보만을 획득하여 미디어 서버(130)로 전송하고 미디어 서버(130)에서 디지털 콘텐츠의 보호를 위한 방법이 수행되는 경우 클라이언트(110)의 부하를 줄일 수 있고 디지털 콘텐츠의 종류나 클라이언트와 연결된 외부 장치의 종류 등이 증가하는 경우에도 선택적인 디지털 콘텐츠의 보호를 즉시 수행할 수 있는 등의 이점이 있으나, 미디어 서버(130)의 부하가 증가될 수 있다.

[121] 먼저 도 2를 참조하여 본 발명에 의한 디지털 콘텐츠의 보호 방법을 살펴본다.

[122] 도 2는 본 발명의 바람직한 일 실시예에 따라 디지털 콘텐츠 보호 방법이 구현되는 순서를 도시한 순서도이다.

[123] 도 2에 도시된 바와 같이, 먼저 클라이언트(110)와 연결된 외부 장치의 하드웨어 아이디 정보를 획득한다(S200).

[124] 하드웨어 아이디 정보의 획득은 전술한 바와 같이 플러그앤플레이 기능에 수행될 수 있으나 이에 한정되는 것은 아니다.

[125] 획득된 하드웨어 아이디 정보가 미리 저장된 하드웨어 아이디 정보와 비교하여 획득한 하드웨어 아이디 정보가 예를 들면, 프로젝터인지 여부를 판단한다(S202).

[126] 판단 결과 프로젝터인 경우 콘텐츠 재생을 중단하고(S204), 프로젝터가 아닌 경우 콘텐츠의 재생을 수행한다(S206).

[127] 도 2에서는 클라이언트에서 콘텐츠의 재생 및 중단으로서 콘텐츠를 보호하는 것으로 도시하였으나, 콘텐츠의 보호 방법은 전술한 바와 같이, 클라이언트(110) 내에서의 콘텐츠의 재생은 계속 수행하되, 프로젝터(100)와 같은 외부 장치로의 출력 자체를 차단하거나 미디어 서버(130)로 디지털 콘텐츠의 전송 중단을 요청하는 등의 다양한 방법으로 실시 가능함은 자명하다.

[128] 도 2에서는 클라이언트(110)에서 하드웨어 아이디 정보의 획득 및 디지털 콘텐츠의 보호가 모두 이루어지는 경우를 예시하였으나 전술한 바와 같이 클라이언트(110)에서 하드웨어 아이디 정보만을 획득하여 미디어 서버(130)로 전송하고 미디어 서버(130)에서 디지털 콘텐츠의 보호를 위한 방법이 수행되는 것도 가능하며, 이 경우 본 발명에 의한 디지털 콘텐츠의 보호 방법이 수행되는 순서를 도 3을 참조하여 살펴보기로 한다.

[129] 도 3은 본 발명의 바람직한 다른 일 실시예에 따라 디지털 콘텐츠 보호 방법이 구현되는 순서를 도시한 순서도이다.

[130] 도 3에 도시된 바와 같이, 먼저 클라이언트(110)에서 클라이언트(110)와 연결된 외부 장치(100)의 하드웨어 아이디 정보를 획득하며(S300), 획득된 하드웨어 아이디 정보를 미디어 서버(130)로 전송한다(S302).

[131] 한편, 하드웨어 아이디 정보의 획득은 전술한 바와 같이 플러그앤플레이 기능에 수행될 수 있으나 이에 한정되는 것은 아니다.

[132] 미디어 서버(130)는 획득된 하드웨어 아이디 정보가 미리 저장된 하드웨어 아이디 정보와 비교하여 획득한 하드웨어 아이디 정보가 예를 들면, 프로젝터(100)인지 여부를 판단한다(S304).

[133] 판단 결과, 프로젝터(100)가 아닌 경우 클라이언트(110)로의 콘텐츠의 전송을 수행하며(S306), 전송된 콘텐츠는 클라이언트(110)에서 재생된다(S308).

[134] 판단 결과, 프로젝트(100)인 경우 클라이언트(110)로의 콘텐츠 전송을 중단하고 이 경우 콘텐츠 전송 불가능 신호를 클라이언트(110)로 전송하여(S310) 클라이언트(110)의 화면에 콘텐츠의 재생 또는 전송 불가능이 표시되도록 할 수 있다.

[135] 한편, 이러한 본 발명에 의한 디지털 콘텐츠 보호 방법은 프로그램으로 구현되어 컴퓨터로 읽을 수 있는 기록매체(씨디롬, 램, 롬, 플로피 디스크, 하드디스크, 광자기디스크 등)에 저장될 수 있다.

[136]

[137] 이하에서는 도 4 및 도 5를 참조하여 본 발명에 의한 디지털 콘텐츠 보호 방법을 구현할 수 있는 장치의 구성을 살펴보기로 한다.

[138] 도 4는 본 발명의 바람직한 일 실시예에 따른 디지털 콘텐츠 보호 방법이 구현하기 위해 클라이언트(110)에 설치될 수 있는 콘텐츠 보호 모듈의 구성을 도시한 구성도이다.

[139] 한편, 이러한 콘텐츠 보호 모듈은 클라이언트(110)에 프로그램의 형태로 설치되거나 별도의 장치로 구성될 수 있음은 자명하다.

[140] 도 4는 전술한 실시예 중 클라이언트(110)에서 하드웨어 아이디 정보를 획득하고 획득된 하드웨어 아이디 정보를 이용하여 콘텐츠의 출력 또는 재생을 중단을 판단하여 콘텐츠를 보호하는 경우 콘텐츠 보호 모듈의 구성을 예시한 것이다.

[141] 도 4에 도시된 바와 같이, 본 발명에 의한 콘텐츠 보호 모듈은 하드웨어 아이디 정보 획득부, 하드웨어 아이디 정보 비교부 및 콘텐츠 재생 차단부를 포함할 수 있다.

[142] 하드웨어 아이디 정보 획득부(400)는 클라이언트(110)와 연결되어 클라이언트(110)에서 재생되는 화면이 출력되는 외부 장치의 하드웨어 아이디 정보를 획득한다. 이러한 하드웨어 아이디 정보는 클라이언트(110)에 설치된 프로그램의 본래 기능 예를 들면, 플러그앤플레이 기능에 의해 획득되는 정보를 입력받을 수도 있으며, 또한 다른 방법에 의해 하드웨어 아이디 정보를 획득하는 것도 가능하다.

[143] 하드웨어 아이디 정보 비교부(410)는 하드웨어 아이디 정보 획득부(400)에서 획득된 하드웨어 아이디 정보를 미리 설정된 화면의 외부 출력을 차단하기 위한 장치의 하드웨어 아이디 정보와 비교한다.

[144] 이러한 하드웨어 아이디 정보 비교부(410)에서의 비교를 통해 획득된 하드웨어 아이디 정보가 예를 들면, 프로젝터(100)인지 여부를 판단하게 된다.

[145] 콘텐츠 재생 차단부(420)는 하드웨어 아이디 정보 비교부(410)에서 판단된 결과 프로젝터인 경우 수신된 디지털 콘텐츠의 재생을 차단한다.

[146] 도 4에서는 디지털 콘텐츠의 재생 차단으로 예시하였으나, 디지털 콘텐츠가 외부 장치로 출력되지 않도록 하는 것은 전술한 바와 같이 클라이언트(110)와 연결되는 외부 장치에서 화면이 출력되는 자체를 차단하는 방법과 클라이언트(110)에서의 콘텐츠의 재생이 중단되도록 하는 방법이나 미디어 서버(130)에서 콘텐츠의 전송 자체가 중단되도록 하는 방법 등 다양한 방법으로 가능하며 그 방법은 아무런 제한이 없다.

[147] 한편, 도 4에서는 미도시하였으나, 본 발명에 의한 콘텐츠 보호 모듈은 하드웨어 아이디 정보 획득부(400)에서 획득된 하드웨어 아이디 정보를 화면의 외부 출력을 차단하기 위한 장치의 하드웨어 아이디 정보가 저장되는 하드웨어 아이디 정보 저장부(미도시)를 더 포함할 수 있다.

[148]

[149] 도 5는 전술한 실시예 중 클라이언트(110)에서는 하드웨어 아이디 정보만을 획득하여 미디어 서버(130)로 전송하고 미디어 서버(130)에서 획득된 하드웨어 아이디 정보를 이용하여 콘텐츠의 출력 또는 재생을 중단을 판단하여 콘텐츠를 보호하는 경우 콘텐츠 보호 장치의 구성을 예시한 것이다.

[150] 한편, 이러한 콘텐츠 보호 장치는 미디어 서버(130)에 프로그램의 형태로

설치되거나 미디어 서버(130)와 연결될 수 있는 별도의 장치로 구성될 수 있음은 자명하다.

[151] 도 5는 본 발명의 바람직한 다른 일 실시예에 따른 디지털 콘텐츠 보호 방법이 구현하기 위한 콘텐츠 보호 장치의 구성을 도시한 구성도이다.

[152] 도 5에 도시된 바와 같이 본 발명의 바람직한 다른 일 실시예에 따른 디지털 콘텐츠 보호 방법이 구현하기 위한 콘텐츠 보호 장치는 하드웨어 아이디 정보 비교부(500) 및 콘텐츠 전송 차단부(510)를 포함할 수 있다.

[153] 본 발명에 의한 콘텐츠 보호 장치는 먼저 클라이언트(110)와 연결되어 클라이언트(110)에서 재생되는 화면이 출력되는 외부 장치의 하드웨어 아이디 정보를 클라이언트(110)로부터 수신한다. 이러한 하드웨어 아이디 정보는 본 발명에 의한 콘텐츠 보호 장치에 포함될 수 있는 통신부(미도시)를 통해 수신될 수 있다.

[154] 하드웨어 아이디 정보 비교부(500)는 도 4의 설명에서와 같이 수신된 하드웨어 아이디 정보를 미리 설정된 화면의 외부 출력을 차단하기 위한 장치의 하드웨어 아이디 정보와 비교한다.

[155] 이러한 하드웨어 아이디 정보 비교부(500)에서의 비교를 통해 획득된 하드웨어 아이디 정보가 예를 들면, 프로젝트(100)인지 여부를 판단하게 된다.

[156] 콘텐츠 전송 차단부(510)는 하드웨어 아이디 정보 비교부(500)에서 판단된 결과 예시한 것과 같이 프로젝터(100)인 경우 클라이언트(110)로 콘텐츠의 전송을 차단한다.

[157] 도 5에서는 디지털 콘텐츠의 전송 차단으로 예시하였으나, 디지털 콘텐츠가 클라이언트(110)와 연결되는 외부 장치로 출력되지 않도록 하는 것은 전술한 바와 같이 클라이언트(110)와 연결되는 외부 장치에서 화면이 출력되는 자체를 차단하는 방법과 클라이언트(110)에서의 콘텐츠의 재생이 중단되도록 하는 방법 등 다양한 방법으로 가능하며 그 방법은 아무런 제한이 없다.

[158] 한편, 본 발명에 의한 콘텐츠 보호 장치는 화면의 외부 출력을 차단하기 위한 외부 장치의 하드웨어 아이디 정보가 저장되는 하드웨어 아이디 정보 데이터베이스와 연결될 수 있다.

[159]

[160] 상기한 본 발명의 바람직한 실시예는 예시의 목적을 위해 개시된 것이고, 본 발명에 대해 통상의 지식을 가진 당업자라면 본 발명의 사상과 범위 안에서 다양한 수정, 변경, 부가가 가능할 것이며, 이러한 수정, 변경 및 부가는 하기의 특허청구범위에 속하는 것으로 보아야 할 것이다.

청구범위

[청구항 1] 외부 장치와 연결되는 클라이언트(client)에서 디지털 콘텐츠가 재생되는 화면을 상기 외부 장치의 화면으로 표시되는 것을 차단하여 수행되는 상기 클라이언트에서의 디지털 콘텐츠(digital contents)의 보호 방법에 있어서,
상기 외부 장치로부터 상기 외부 장치의 하드웨어 아이디 정보를 획득하는 단계(a);
상기 획득된 하드웨어 아이디 정보를 미리 설정된 하드웨어 아이디 정보와 비교하는 단계(b); 및
상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 디지털 콘텐츠의 재생을 차단하여 상기 디지털 콘텐츠가 상기 외부 장치로 표시되는 것을 차단하는 단계(c)를 포함하는 것을 특징으로 하는 디지털 콘텐츠의 보호 방법.

[청구항 2] 외부 장치와 연결되는 클라이언트(client) 및 상기 클라이언트로 디지털 콘텐츠(digital contents)를 전송하는 미디어 서버(media server)를 포함하는 콘텐츠 전송 시스템에서 상기 클라이언트에서 디지털 콘텐츠가 재생되는 화면을 상기 외부 장치의 화면으로 표시되는 것을 차단하여 수행되는 상기 미디어 서버에서의 디지털 콘텐츠의 보호 방법에 있어서,
상기 클라이언트로부터 상기 클라이언트에서 획득된 상기 외부 장치의 하드웨어 아이디 정보를 수신하는 단계(a);
상기 수신된 하드웨어 아이디 정보를 미리 설정된 하드웨어 아이디 정보와 비교하는 단계(b); 및
상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 클라이언트로 상기 디지털 콘텐츠를 전송하는 것을 중단하여 상기 디지털 콘텐츠가 상기 외부 장치로 표시되는 것이 차단되도록 하는 단계(c)를 포함하는 것을 특징으로 하는 디지털 콘텐츠의 보호 방법.

[청구항 3] 제1항 또는 제2항에 있어서,
상기 단계(a)에서,
상기 외부 장치의 하드웨어 아이디 정보는 상기 클라이언트의 플러그앤플레이(Plug and Play) 기능에 의해 상기 클라이언트에서 획득되는 것을 특징으로 하는 디지털 콘텐츠 보호 방법.

[청구항 4] 제1항에 있어서,
상기 단계(c)에서,

상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 디지털 콘텐츠가 상기 외부 장치로 출력되는 것을 차단하는 것은 특징으로 하는 디지털 콘텐츠의 보호 방법.

[청구항 5] 제1항에 있어서,
상기 단계(c)에서,
상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 클라이언트로 상기 디지털 콘텐츠를 전송하는 미디어 서버로 상기 디지털 콘텐츠의 전송 중단을 요청하는 것을 특징으로 하는 디지털 콘텐츠의 보호 방법.

[청구항 6] 제2항에 있어서,
상기 단계(c)에서,
상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 클라이언트로 상기 디지털 콘텐츠가 상기 외부 장치로 출력되는 것을 차단하도록 하는 신호를 전송하는 것은 특징으로 하는 디지털 콘텐츠의 보호 방법.

[청구항 7] 제2항에 있어서,
상기 단계(c)에서,
상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 클라이언트로 상기 디지털 콘텐츠가 상기 클라이언트에서 재생되는 것을 차단하도록 하는 신호를 전송하는 것을 특징으로 하는 디지털 콘텐츠의 보호 방법.

[청구항 8] 외부 장치와 연결되는 클라이언트(client)에서 디지털 콘텐츠(digital contents)가 재생되는 화면을 상기 외부 장치의 화면으로 표시되는 것을 차단하여 수행되는 상기 클라이언트에서의 디지털 콘텐츠의 보호 방법을 수행하는 디지털 콘텐츠(digital contents)의 보호 장치에 있어서,
상기 외부 장치로부터 상기 외부 장치의 하드웨어 아이디 정보를 획득하는 하드웨어 아이디 정보 획득부;
상기 획득된 하드웨어 아이디 정보를 미리 설정된 하드웨어 아이디 정보와 비교하는 하드웨어 아이디 정보 비교부; 및
상기 하드웨어 아이디 정보 비교부의 비교 결과 상기 하드웨어 아이디 정보 획득부에서 획득된 하드웨어 아이디 정보가 미리 설정된 하드웨어 아이디 정보에 해당하는 경우 상기 디지털 콘텐츠의 재생을 차단하여 상기 디지털 콘텐츠가 상기 외부

장치로 표시되는 것을 차단하는 콘텐츠 재생 차단부를 포함하는 것을 특징으로 하는 디지털 콘텐츠의 보호 장치.

[청구항 9] 외부 장치와 연결되는 클라이언트(client)에서 디지털 콘텐츠(digital contents)가 재생되는 화면을 상기 외부 장치의 화면으로 표시되는 것을 차단하여 수행되는 상기 클라이언트에서의 디지털 콘텐츠의 보호 방법을 수행하는 디지털 콘텐츠의 보호 장치에 있어서,
상기 클라이언트로부터 수신된 상기 클라이언트에서 획득한 상기 외부 장치의 하드웨어 아이디 정보를 미리 설정된 하드웨어 아이디 정보와 비교하는 하드웨어 아이디 정보 비교부; 및
상기 하드웨어 아이디 정보 비교부의 비교 결과 상기 클라이언트로부터 수신된 하드웨어 아이디 정보가 미리 설정된 하드웨어 아이디 정보에 해당하는 경우 상기 클라이언트로 상기 디지털 콘텐츠를 전송하는 것을 중단하여 상기 디지털 콘텐츠가 상기 외부 장치로 표시되는 것이 차단되도록 하는 콘텐츠 전송 차단부를 포함하는 것을 특징으로 하는 디지털 콘텐츠의 보호 장치.

[청구항 10] 제8항 또는 제9항에 있어서,
상기 외부 장치의 하드웨어 아이디 정보는 상기 클라이언트의 플러그앤플레이(Plug and Play) 기능에 의해 상기 클라이언트에서 획득되는 것을 특징으로 하는 디지털 콘텐츠 보호 장치.

[청구항 11] 제8항에 있어서,
상기 콘텐츠 재생 차단부는,
상기 디지털 콘텐츠가 상기 외부 장치로 출력되는 것을 차단하는 것을 특징으로 하는 디지털 콘텐츠의 보호 장치.

[청구항 12] 제8항에 있어서,
상기 콘텐츠 재생 차단부는,
상기 클라이언트로 상기 디지털 콘텐츠를 전송하는 미디어 서버로 상기 디지털 콘텐츠의 전송 중단을 요청하는 것을 특징으로 하는 디지털 콘텐츠의 보호 장치.

[청구항 13] 제9항에 있어서,
상기 콘텐츠 전송 차단부는,
상기 클라이언트로 상기 디지털 콘텐츠가 상기 외부 장치로 출력되는 것을 차단하도록 하는 신호를 전송하는 것은 특징으로 하는 디지털 콘텐츠의 보호 장치.

[청구항 14] 제9항에 있어서,
상기 콘텐츠 전송 차단부는,
상기 클라이언트로 상기 디지털 콘텐츠가 상기 클라이언트에서

재생되는 것을 차단하도록 하는 신호를 전송하는 것은 특징으로 하는 디지털 콘텐츠의 보호 장치.

[청구항 15] 외부 장치와 연결되는 클라이언트(client)에서 디지털 콘텐츠가 재생되는 화면을 상기 외부 장치의 화면으로 표시되는 것을 차단하여 수행되는 상기 클라이언트에서의 디지털 콘텐츠(digital contents)의 보호 방법이 구현되도록, 상기 클라이언트에 의해 실행될 수 있는 명령어들의 프로그램이 구현되어 있으며 상기 클라이언트에 의해 판독될 수 있는 프로그램을 기록한 기록매체에 있어서,

상기 외부 장치로부터 상기 외부 장치의 하드웨어 아이디 정보를 획득하는 단계(a);

상기 획득된 하드웨어 아이디 정보를 미리 설정된 하드웨어 아이디 정보와 비교하는 단계(b); 및

상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 디지털 콘텐츠의 재생을 차단하여 상기 디지털 콘텐츠가 상기 외부 장치로 표시되는 것을 차단하는 단계(c)를 포함하는 것을 특징으로 하는 디지털 콘텐츠의 보호 방법을 구현하기 위한 프로그램을 기록한 기록매체.

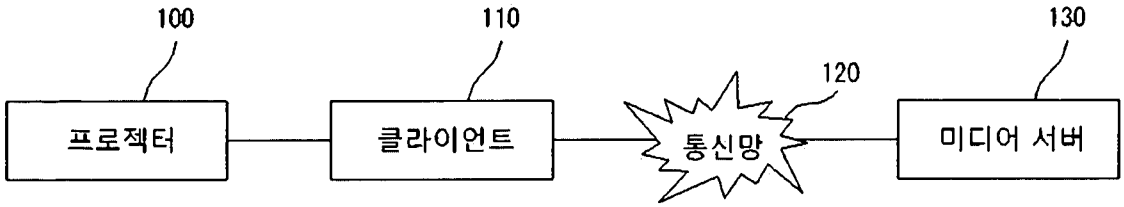
[청구항 16] 외부 장치와 연결되는 클라이언트(client) 및 상기 클라이언트로 디지털 콘텐츠(digital contents)를 전송하는 미디어 서버(media server)를 포함하는 콘텐츠 전송 시스템에서 상기 클라이언트에서 디지털 콘텐츠가 재생되는 화면을 상기 외부 장치의 화면으로 출력되는 것을 차단하여 수행되는 상기 미디어 서버에서의 디지털 콘텐츠의 보호 방법이 구현되도록, 상기 미디어 서버에 의해 실행될 수 있는 명령어들의 프로그램이 구현되어 있으며 상기 미디어 서버에 의해 판독될 수 있는 프로그램을 기록한 기록매체에 있어서,

상기 클라이언트로부터 상기 클라이언트에서 획득된 상기 외부 장치의 하드웨어 아이디 정보를 수신하는 단계(a);

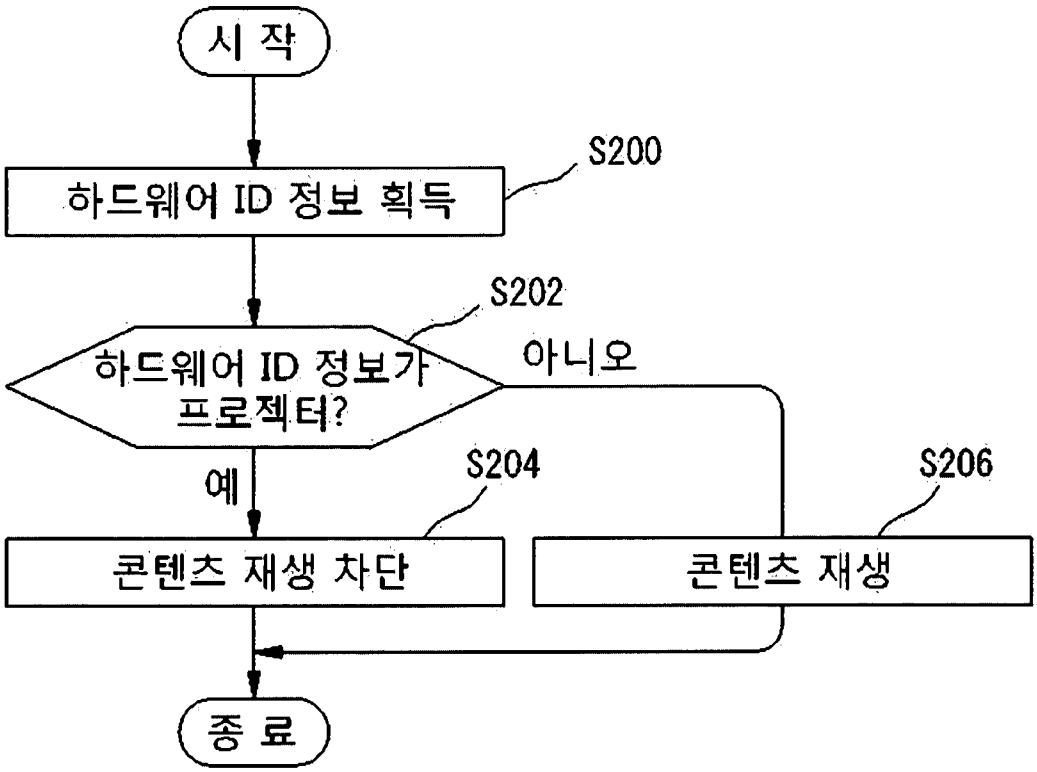
상기 수신된 하드웨어 아이디 정보를 미리 설정된 하드웨어 아이디 정보와 비교하는 단계(b); 및

상기 비교 결과 상기 획득된 하드웨어 아이디 정보가 미리 설정된 외부 장치의 하드웨어 아이디 정보에 해당하는 경우 상기 클라이언트로 상기 디지털 콘텐츠를 전송하는 것을 중단하여 상기 디지털 콘텐츠가 상기 외부 장치로 표시되는 것이 차단되도록 하는 단계(c)를 포함하는 것을 특징으로 하는 디지털 콘텐츠의 보호 방법을 구현하기 위한 프로그램을 기록한 기록매체.

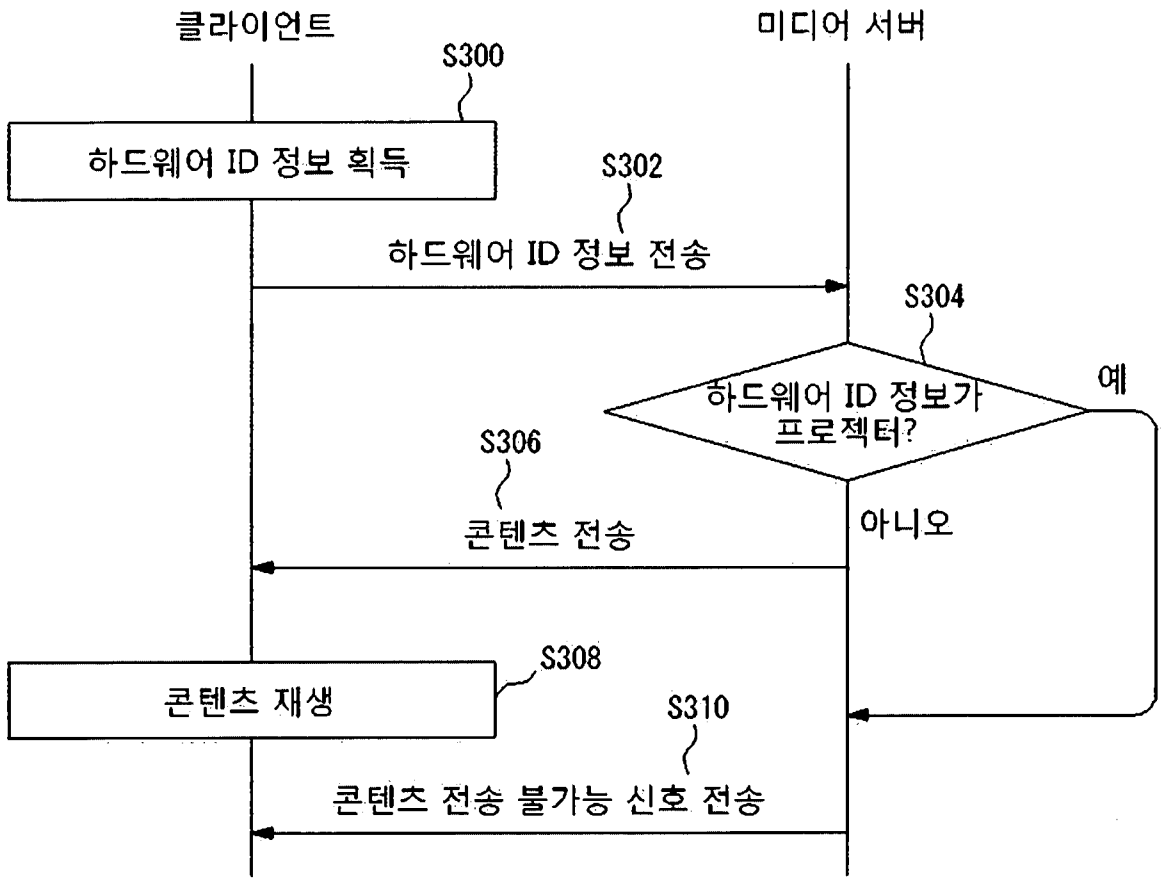
[Fig. 1]


100
110
120
130
프로젝터
클라이언트
통신망
미디어 서버

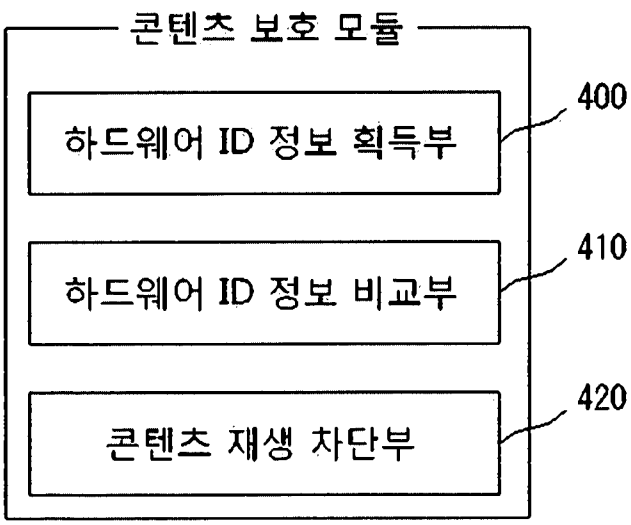
[Fig. 2]


시 작
S200
하드웨어 ID 정보 획득
S202
하드웨어 ID 정보가 프로젝터?
아니오
예
S204
S206
콘텐츠 재생 차단
콘텐츠 재생
종 료

[Fig. 3]


클라이언트
미디어 서버
S300
하드웨어 ID 정보 획득
S302
하드웨어 ID 정보 전송
S304
하드웨어 ID 정보가 프로젝터?
예
아니오
S306
콘텐츠 전송
S308
콘텐츠 재생
S310
콘텐츠 전송 불가능 신호 전송

[Fig. 4]


콘텐츠 보호 모듈
하드웨어 ID 정보 획득부
400
하드웨어 ID 정보 비교부
410
콘텐츠 재생 차단부
420

[Fig. 5]