(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년08월04일
(11) 등록번호 10-1425315
(24) 등록일자 2014년07월24일

(51) 국제특허분류(Int. Cl.)
G06F 21/12 (2013.01) *G06F 21/30* (2013.01)
(21) 출원번호 10-2013-0023391
(22) 출원일자 2013년03월05일
심사청구일자 2013년03월05일
(30) 우선권주장
1020130009180 2013년01월28일 대한민국(KR)
(56) 선행기술조사문헌
KR1020090062437 A*
JP2007213490 A
KR1020030038995 A
*는 심사관에 의하여 인용된 문헌
기술이전 희망 : **기술양도**, **실시권허여**, **기술지도**

(73) 특허권자
숭실대학교산학협력단
서울특별시 동작구 상도로 369 (상도동)
(72) 발명자
김강희
경기 성남시 분당구 판교원로 207, 502동 1902호 (판교동, 판교원마을5단지아파트)
백한별
경기도 남양주시 호평동 금강아파트 2011동 503호
홍성길
서울 금천구 독산로44길 69, 105호 (시흥동)
(74) 대리인
민영준, **최관락**, **송인호**

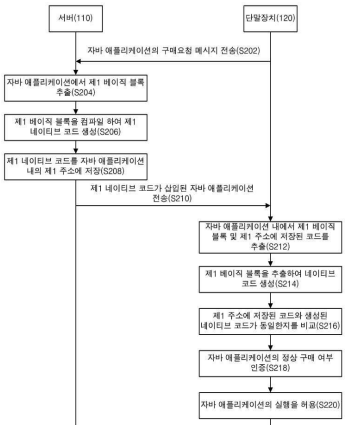
전체 청구항 수 : 총 5 항 심사관 : 문남두

(54) 발명의 명칭 **자바 애플리케이션의 불법 복제를 방지하기 위한 자바 가상 머신이 탑재된 단말장치 및 서버와, 상기 단말장치에서의 자바 애플리케이션의 인증 방법**

(57) 요 약

자바 애플리케이션의 불법 복제를 방지하기 위한 자바 가상 머신이 탑재된 단말장치 및 서버와, 상기 단말장치에서의 자바 애플리케이션의 인증 방법이 개시된다. 개시된 단말장치는 자바 애플리케이션을 구성하는 다수의 베이직 블록들 중 제1 베이직 블록을 컴파일하여 제1 네이티브 코드를 생성하는 컴파일부; 상기 자바 애플리케이션 내의 제1 주소에 저장된 코드와 상기 제1 네이티브 코드가 동일한지를 비교하는 비교부; 및 상기 제1 주소에 저장된 코드와 상기 제1 네이티브 코드가 동일한 경우, 상기 자바 애플리케이션을 정상적으로 구매된 것으로 인증하는 제어부;를 포함한다.

대 표 도 - 도2



이 발명을 지원한 국가연구개발사업

과제고유번호	2011-mobile_app-9500
부처명	문화체육관광부
연구사업명	저작권기술개발사업
연구과제명	시스템 소프트웨어 기반 모바일 애플리케이션 불법복제방지 기술 연구 개발
기 여 율	1/1
주관기관	숭실대학교 산학협력단
연구기간	2011.10.14 ~ 2014.03.31

특허청구의 범위

청구항 1

자바 애플리케이션을 구성하는 다수의 베이직 블록들 중 제1 베이직 블록을 컴파일하여 제1 네이티브 코드를 생성하는 컴파일부;

상기 자바 애플리케이션 내의 제1 주소에 저장된 코드와 상기 제1 네이티브 코드가 동일한지를 비교하는 비교부; 및

상기 제1 주소에 저장된 코드와 상기 제1 네이티브 코드가 동일한 경우, 상기 자바 애플리케이션을 정상적으로 구매된 것으로 인증하고, 상기 애플리케이션의 실행을 허용하는 제어부;를 포함하는 것을 특징으로 하는 자바 애플리케이션의 불법 복제를 방지하기 위한 자바 가상 머신이 탑재된 단말장치.

청구항 2

제1항에 있어서,

상기 단말장치는 상기 제1 베이직 블록의 식별정보 및 상기 제1 주소의 정보를 포함하는 메시지를 서버로 전송하는 전송부;를 더 포함하되,

상기 서버는 상기 제1 베이직 블록의 식별정보를 이용하여 원본 자바 애플리케이션 내에서 상기 제1 베이직 블록을 추출하고, 상기 추출된 제1 베이직 블록을 컴파일하여 상기 제1 네이티브 코드를 생성하며, 상기 제1 주소의 정보를 이용하여 상기 제1 네이티브 코드를 상기 원본 자바 애플리케이션 내의 상기 제1 주소에 저장하여 상기 자바 애플리케이션을 생성하는 것을 특징으로 하는 자바 애플리케이션의 불법 복제를 방지하기 위한 자바 가상 머신이 탑재된 단말장치.

청구항 3

제2항에 있어서,

상기 단말장치는 상기 서버로부터 상기 자바 애플리케이션을 수신하는 수신부;를 더 포함하되,

상기 메시지를 상기 자바 애플리케이션의 구매요청 메시지이고, 상기 수신부는 상기 구매요청 메시지에 대응하여 구매가 완료된 상기 자바 애플리케이션을 상기 서버로부터 수신하는 것을 특징으로 하는 자바 애플리케이션의 불법 복제를 방지하기 위한 자바 가상 머신이 탑재된 단말장치.

청구항 4

삭제

청구항 5

자바 애플리케이션을 구성하는 다수의 베이직 블록들 중 제1 베이직 블록에 대한 식별정보 및 상기 자바 애플리케이션 내의 제1 주소의 정보를 포함하는 상기 자바 애플리케이션의 구매요청 메시지를 단말장치로부터 수신하는 수신부; 및

상기 제1 베이직 블록의 식별정보를 이용하여 상기 자바 애플리케이션 내에서 상기 제1 베이직 블록을 추출하고, 상기 추출된 제1 베이직 블록을 컴파일하여 제1 네이티브 코드를 생성하며, 상기 제1 주소의 정보를 이용하여 상기 제1 네이티브 코드를 상기 자바 애플리케이션 내의 상기 제1 주소에 저장하는 컴파일부; 및

상기 구매요청 메시지에 대응하여 구매가 완료된 상기 제1 네이티브 코드가 삽입된 자바 애플리케이션을 상기 단말장치로 전송하는 전송부;를 포함하되,

상기 제1 주소에 삽입된 상기 제1 네이티브 코드는 상기 자바 애플리케이션에 대한 불법 복제 방지용 식별정보로서 활용되는 것을 특징으로 하는 자바 애플리케이션의 불법 복제를 방지하기 위한 자바 가상 머신이 탑재된 서버.

청구항 6

삭제

청구항 7

자바 애플리케이션을 구성하는 다수의 베이직 블록들 중 제1 베이직 블록을 컴파일하여 제1 네이티브 코드를 생성하는 단계;

상기 자바 애플리케이션 내의 제1 주소에 저장된 코드와 상기 제1 네이티브 코드가 동일한지를 비교하는 단계; 및

상기 제1 주소에 저장된 코드와 상기 제1 네이티브 코드가 동일한 경우, 상기 자바 애플리케이션을 정상적으로 구매된 것으로 인증하고, 상기 애플리케이션의 실행을 허용하는 단계;를 포함하는 것을 특징으로 하는 자바 가상 머신이 탑재된 단말장치에서의 자바 애플리케이션의 인증 방법.

명 세 서

기 술 분 야

[0001] 본 발명의 실시예들은 자바 애플리케이션의 불법 복제를 효율적으로 방지할 수 있는 자바 가상 머신이 탑재된 단말장치 및 서버와, 상기 단말장치에서의 자바 애플리케이션의 인증 방법에 관한 것이다.

배 경 기 술

[0002] 스마트폰, 태블릿 PC 등과 같은 스마트 기기에 설치되는 응용 소프트웨어(이하, "모바일 앱"이라 함)은 크기가 작고 변조가 용이하며 기존의 PC 응용 소프트웨어에 비해 보호 기술이 미비하다. 이로 인해, 모바일 앱은 비정상적인 스마트 기기로의 접근에 의해 쉽게 추출이 가능하고, 컴퓨터 시스템, 인터넷, 이동식 저장매체 등을 통해 쉽게 유포될 수 있다. 이에 따라 사용자는 앱 마켓(스토어)을 통하지 않고 비정상적 경로를 통해 유포된 모바일 앱을 설치하여 사용할 수 있다.

[0003] 이와 같은 모바일 앱의 불법 복제는 모바일 앱 개발자의 개발 의욕을 저하시키며, 모바일 앱 시장의 성장을 방해하는 요소로 작용한다. 이에 따라 모바일 앱의 불법 복제를 방지하기 위한 다양한 방법들이 제안되고 있다.

[0004] 모바일 앱의 불법 복제를 방지하기 위한 종래의 기술들로, 스마트 기기 내의 애플리케이션 실행파일의 복제 권한을 제한하는 방법(제1 종래기술), 인증서버를 통해 모바일 앱의 불법 복제 여부를 판단하여 정상적인 모바일 앱 만이 실행될 수 있도록 제한하는 방법(제2 종래기술), 모바일 앱에 애플리케이션 DRM(Digital Right Management)을 적용하는 방법(제3 종래기술) 및 공개키/개인키 기반의 암호화 기술을 이용하는 방법(제4 종래기술) 등이 제안되었다.

[0005] 그러나, 상기한 제1 종래기술은 불법 복제 및 유포 목적이 아닌 백업 목적을 위한 모바일 앱의 복제까지 차단하며, 불법 복제된 모바일 앱이 다운로드될 때 경유하는 모든 지점을 차단하는 것이 실질적으로 불가능하다는 문제점이 있다.

[0006] 그리고, 상기한 제2 종래기술은 인증서버를 통해 모바일 앱을 인증받는 경우에 발생하는 데이터 요금을 사용자가 부담하게 되고, 데이터 네트워크를 사용할 수 없는 환경에서는 불법 복제 여부의 인증이 불가능하다는 문제점이 있다.

[0007] 또한, 상기한 제3 종래기술은 모바일 앱의 실행파일에 보안을 위한 라이브러리가 추가되었다는 사실이 실행파일을 통해 쉽게 노출되는 문제점이 있다.

[0008] 그리고, 상기한 제4 종래기술은 공개키/개인키의 관리가 어렵고, 암호화/복호화를 위한 추가적인 모듈이 필요하다는 문제점이 있다.

발명의 내용

해결하려는 과제

[0009] 상기한 바와 같은 종래기술의 문제점을 해결하기 위해, 본 발명에서는 자바 애플리케이션의 불법 복제를 효율적으로 방지할 수 있는 자바 가상 머신이 탑재된 단말장치 및 서버와, 상기 단말장치에서의 자바 애플리케이션의 인증 방법을 제안하고자 한다.

[0010] 본 발명의 다른 목적들은 하기의 실시예를 통해 당업자에 의해 도출될 수 있을 것이다.

과제의 해결 수단

[0011] 상기한 목적을 달성하기 위해 본 발명의 바람직한 일 실시예에 따르면, 자바 애플리케이션을 구성하는 다수의 베이직 블록들 중 제1 베이직 블록을 컴파일하여 제1 네이티브 코드를 생성하는 컴파일부; 상기 자바 애플리케이션 내의 제1 주소에 저장된 코드와 상기 제1 네이티브 코드가 동일한지를 비교하는 비교부; 및 상기 제1 주소에 저장된 코드와 상기 제1 네이티브 코드가 동일한 경우, 상기 자바 애플리케이션을 정상적으로 구매된 것으로 인증하는 제어부;를 포함하는 것을 특징으로 하는 자바 애플리케이션의 불법 복제를 방지하기 위한 자바 가상 머신이 탑재된 단말장치가 제공된다.

[0012] 상기 단말장치는 상기 제1 베이직 블록의 식별정보 및 상기 제1 주소의 정보를 포함하는 메시지를 서버로 전송하는 전송부;를 더 포함하되, 상기 서버는 상기 제1 베이직 블록의 식별정보를 이용하여 원본 자바 애플리케이션 내에서 상기 제1 베이직 블록을 추출하고, 상기 추출된 제1 베이직 블록을 컴파일하여 상기 제1 네이티브 코드를 생성하며, 상기 제1 주소의 정보를 이용하여 상기 제1 네이티브 코드를 상기 원본 자바 애플리케이션 내의 상기 제1 주소에 저장하여 상기 자바 애플리케이션을 생성할 수 있다.

[0013] 상기 단말장치는 상기 서버로부터 상기 자바 애플리케이션을 수신하는 수신부;를 더 포함하되, 상기 메시지를 상기 자바 애플리케이션의 구매요청 메시지이고, 상기 수신부는 상기 구매요청 메시지에 대응하여 구매가 완료된 상기 자바 애플리케이션을 상기 서버로부터 수신할 수 있다.

[0014] 상기 제어부는 상기 자바 애플리케이션이 정상적으로 구매된 것으로 인증된 경우, 상기 애플리케이션의 실행을 허용할 수 있다.

[0015] 또한, 본 발명의 다른 실시예에 따르면, 자바 애플리케이션을 구성하는 다수의 베이직 블록들 중 제1 베이직 블록에 대한 식별정보 및 상기 자바 애플리케이션 내의 제1 주소의 정보를 포함하는 메시지를 단말장치로부터 수신하는 수신부; 및 상기 제1 베이직 블록의 식별정보를 이용하여 상기 자바 애플리케이션 내에서 상기 제1 베이직 블록을 추출하고, 상기 추출된 제1 베이직 블록을 컴파일하여 제1 네이티브 코드를 생성하며, 상기 제1 주소의 정보를 이용하여 상기 제1 네이티브 코드를 상기 자바 애플리케이션 내의 상기 제1 주소에 저장하는 컴파일부;를 포함하되, 상기 제1 주소에 삽입된 상기 제1 네이티브 코드는 상기 자바 애플리케이션에 대한 불법 복제 방지용 식별정보로서 활용되는 것을 특징으로 하는 자바 애플리케이션의 불법 복제를 방지하기 위한 자바 가상 머신이 탑재된 서버가 제공된다.

[0016] 또한, 본 발명의 또 다른 실시예에 따르면, 자바 애플리케이션을 구성하는 다수의 베이직 블록들 중 제1 베이직 블록을 컴파일하여 제1 네이티브 코드를 생성하는 단계; 상기 자바 애플리케이션 내의 제1 주소에 저장된 코드와 상기 제1 네이티브 코드가 동일한지를 비교하는 단계; 및 상기 제1 주소에 저장된 코드와 상기 제1 네이티브 코드가 동일한 경우, 상기 자바 애플리케이션을 정상적으로 구매된 것으로 인증하는 단계;를 포함하는 것을 특징으로 하는 자바 가상 머신이 탑재된 단말장치에서의 자바 애플리케이션의 인증 방법이 제공된다.

발명의 효과

[0017] 본 발명에 따르면, 자바 애플리케이션의 불법 복제를 효율적으로 방지할 수 있게 된다.

도면의 간단한 설명

[0018] 도 1은 본 발명의 일 실시예에 따른 자바 애플리케이션의 불법 복제 방지를 위한 시스템의 전체적인 구성을 도시한 도면이다.

도 2는 본 발명의 일 실시예에 따른 자바 애플리케이션의 불법 복제 방지를 위한 방법의 전체적인 흐름을 도시한 순서도이다.

도 3 내지 도 6은 본 발명의 일 실시예에 따라서, 자바 애플리케이션의 불법 복제 방지를 위한 시스템을 구성하는 각 구성요소의 동작의 개념을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0019] 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. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0020] 이하에서, 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다.

[0021] 도 1은 본 발명의 일 실시예에 따른 자바 애플리케이션의 불법 복제 방지를 위한 시스템의 전체적인 구성을 도시한 도면이다.

[0022] 도 1을 참조하면, 본 발명의 일 실시예에 따른 시스템(100)은 서버(110) 및 단말장치(120)를 포함한다.

[0023] 서버(110)는 자바 애플리케이션인 모바일 앱의 구매/판매를 관리하는 앱 마켓(스토어) 서버로서, 도 1에 도시된 바와 같이 수신부(111), 전송부(112) 및 컴파일부(113)를 포함한다. 상기 자바 애플리케이션은 자바 애플리케이션 실행파일일 수 있다.

[0024] 단말장치(120)는 스마트폰, 태블릿 PC 등과 같이 자바 애플리케이션인 모바일 앱이 실행되는 모든 종류의 장치로서, 도 1에 도시된 바와 같이 수신부(121), 전송부(122), 컴파일부(123), 비교부(124) 및 제어부(125)를 포함한다.

[0025] 도 2는 본 발명의 일 실시예에 따른 자바 애플리케이션의 불법 복제 방지를 위한 방법의 전체적인 흐름을 도시한 순서도이다.

[0026] 이하, 도 1 및 도 2를 참조하여, 본 발명의 일 실시예에 따른 자바 애플리케이션의 불법 복제 방지를 위한 시스템(100)의 동작에 대해 상세하게 설명하기로 한다.

[0027] 먼저, 단계(S202)에서 단말장치(120)는 전송부(122)를 통해 특정 자바 애플리케이션의 구매요청 메시지를 전송한다. 전송된 구매요청 메시지는 수신부(111)를 통해 서버(110)로 수신된다.

[0028] 구매 요청된 자바 애플리케이션은 다수의 베이직 블록으로 구성되는데, 본 발명에 따르면, 구매요청 메시지는 구매하고자 하는 자바 애플리케이션을 구성하는 다수의 베이직 블록 중 특정 베이직 블록에 대한 식별정보(예를 들어, 번호) 및 자바 애플리케이션 내의 특정 주소에 대한 정보를 포함할 수 있다. 이하, 설명의 편의를 위해, 특정 베이직 블록을 "제1 베이직 블록"으로, 특정 주소를 "제1 주소"라 칭하기로 한다.

[0029] 한편, 제1 베이직 블록 및 제1 주소의 선정은 단말장치(120)에 탑재된 자바 가상 머신에 의해 수행될 수 있다. 다시 말해, 제1 베이직 블록 및 제1 주소의 선택은 사용자의 관여 없이 자바 가상 머신에 의해 자동적으로 수행될 수 있다.

[0030] 또한, 서버(110)는 서로 다른 단말장치(120)로부터 구매요청 메시지를 각각 수신할 수 있는데, 이 경우 서로 다른 단말장치(120)로부터 수신된 제1 베이직 블록의 식별번호 및 제1 주소는 서로 상이할 수 있다.

[0031] 한편, 도 3에서는 상기한 구매요청 메시지의 전송 절차의 개념을 도시하고 있다.

[0032] 다음으로, 단계(S204)에서 서버(110)는 제1 베이직 블록의 식별정보를 이용하여 구매 요청된 자바 애플리케이션(이하, "원본 자바 애플리케이션"이라고 함) 내에서 제1 베이직 블록을 추출한다.

[0033] 그리고, 단계(S206)에서 서버(110)는 추출된 제1 베이직 블록을 컴파일하여 네이티브 코드(이하, "제1 네이티브 코드"라고 함)를 생성한다. 본 발명의 일 실시예에 따르면, 단계(S230)에서 서버(110)는 JIT(Just-In-Time) 컴파일러를 이용하여 제1 베이직 블록을 컴파일할 수 있다.

[0034] 계속하여, 단계(S208)에서 서버(110)는 구매요청 메시지에 포함된 제1 주소의 정보를 이용하여 상기 생성된 제1 네이티브 코드를 원본 자바 애플리케이션 내의 제1 주소에 저장(삽입)한다.

[0035] 이와 같이, 자바 애플리케이션 내의 제1 주소에 삽입된 제1 네이티브 코드는 해당 자바 애플리케이션에 대한 불법 복제 방지용 식별정보, 즉 지문/워터마크와 같이 활용된다. 이에 대한 보다 상세한 설명은 후술하기로 한다.

[0036] 한편, 상기한 단계(S204) 내지 단계(S208)는 서버(110) 내의 컴파일부(113)를 통해 수행된다. 그리고, 이하에서는 설명의 편의를 위해, 제1 네이티브 코드가 삽입된 자바 애플리케이션을 "변형 자바 애플리케이션"이라 칭하기로 한다.

[0037] 이외에도, 서버(110)는 구매요청 메시지의 수신에 대응하여 자바 애플리케이션의 판매/구매를 위한 일련의 동작들을 수행한다.

[0038] 한편, 도 4에서는 상기한 서버(110)에서 수행되는 일련의 동작들의 개념을 도시하고 있다.

[0039] 다음으로, 단계(S210)에서 서버(110)는 구매요청 메시지에 대응하여 구매가 완료된 변형 자바 애플리케이션(즉, 제1 네이티브 코드가 삽입된 자바 애플리케이션)을 전송부(112)를 통해 전송한다. 전송된 변형 자바 애플리케이션은 수신부(121)를 통해 단말장치(120)로 수신된다.

[0040] 이 후, 단계(S212)에서 단말장치(120)는 컴파일부(123)를 통해 변형 자바 애플리케이션을 구성하는 다수의 베이직 블록들 중 제1 베이직 블록을 추출하고, 변형 자바 애플리케이션 내의 제1 주소에 저장된 코드(즉, 제1 네이티브 코드)를 추출한다. 이 때, 단말장치(120)는 자신이 서버(110)로 전송하였던 제1 베이직 블록의 식별정보 및 제1 주소의 정보를 이미 알고 있으므로, 상기한 제1 베이직 블록의 추출 및 제1 주소에 저장된 코드의 추출이 가능하게 된다.

[0041] 그리고, 단계(S214)에서 단말장치(120)는 컴파일부(123)를 통해 제1 베이직 블록을 컴파일하여 네이티브 코드를 생성한다. 이 경우에도 JIT 컴파일러가 이용될 수 있다.

[0042] 다음으로, 단계(S216)에서 단말장치(120)는 비교부(124)를 통해 제1 주소에 저장된 코드와 컴파일을 통해 생성된 네이티브 코드가 동일한지를 비교한다.

[0043] 만약, 단말장치(120)가 해당 자바 애플리케이션을 정상적으로 구매한 사용자의 단말장치라면, 제1 주소에 저장된 코드와 컴파일을 통해 생성된 네이티브 코드는 제1 네이티브 코드로 동일하다. 이는 앞서 설명한 바와 같이 서버(110)는 구매요청을 한 단말장치(120)에서 전송된 제1 베이직 블록의 식별정보 및 제1 주소의 정보를 이용하여 제1 주소에 제1 네이티브 코드를 삽입하였기 때문이다.

[0044] 반대로, 단말장치(120)가 해당 자바 애플리케이션을 정상적으로 구매한 사용자의 단말장치가 아니고 불법 복제된 자바 애플리케이션을 획득한 단말장치라면, 단말장치(120)는 제1 베이직 코드 및 제1 주소에 대한 정보를 알지 못하며, 다른 베이직 코드 및 주소에 대한 정보를 이용하여 상기한 동작들을 수행하게 되므로 제1 주소에 저장된 코드와 컴파일을 통해 생성된 네이티브 코드는 서로 상이하게 된다.

[0045] 따라서, 단계(S218)에서 단말장치(120)는 제1 주소에 저장된 코드와 컴파일을 통해 생성된 네이티브 코드가 동일한 경우, 해당 자바 애플리케이션을 정상적으로 구매된 것으로 인증하고, 제1 주소에 저장된 코드와 컴파일을 통해 생성된 네이티브 코드가 상이한 경우, 해당 자바 애플리케이션을 불법 복제된 것으로 인식한다. 이러한 인증 동작은 단말장치(120) 내의 제어부(125)를 통해 수행된다.

[0046] 만약, 자바 애플리케이션이 정상적으로 구매된 것으로 인증된 경우, 단계(S220)에서 단말장치(120)의 제어부(125)는 해당 자바 애플리케이션의 실행을 허용한다. 반대로, 자바 애플리케이션이 불법 복제된 것으로 인식된 경우, 단말장치(120)의 제어부(125)는 해당 자바 애플리케이션의 실행을 차단한다(미도시).

[0047] 한편, 도 5에서는 단말장치(120)에서 수행되는 자바 애플리케이션의 실행의 허용 동작의 개념을 도시하고 있고, 도 6에서는 단말장치(120)에서 수행되는 자바 애플리케이션의 실행의 차단 동작의 개념을 도시하고 있다.

[0048] 이와 같이, 본 발명의 일 실시예에 따른 자바 애플리케이션의 불법 복제 방지를 위한 시스템(100)은 별도의 지문 내지 워터마크를 사용하지 않고서도 자바 애플리케이션이 정상 구매된 것인지 불법 복제된 것인지의 여부를 용이하게 인증하여 불법 복제된 자바 애플리케이션의 실행을 원천적으로 차단할 수 있는 효과를 가진다.

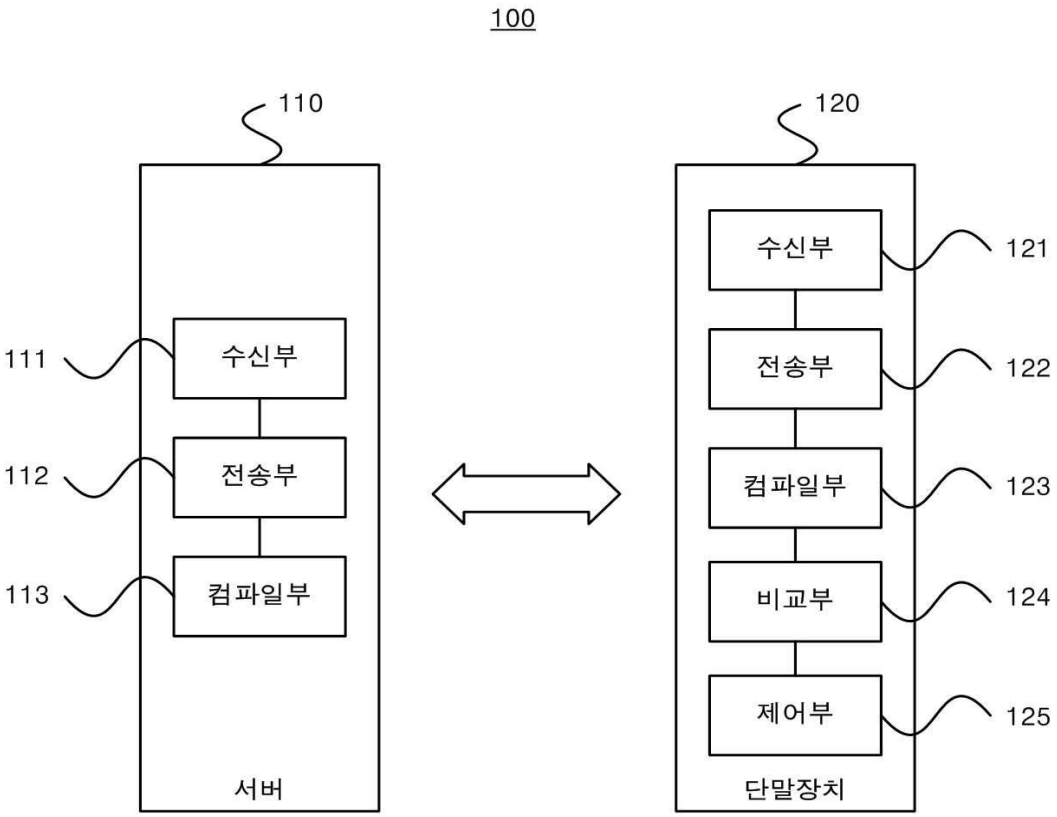
[0049] 한편, 상기에서 설명한 본 발명의 실시예들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령의 예에는 컴

파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 일 실시예들의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

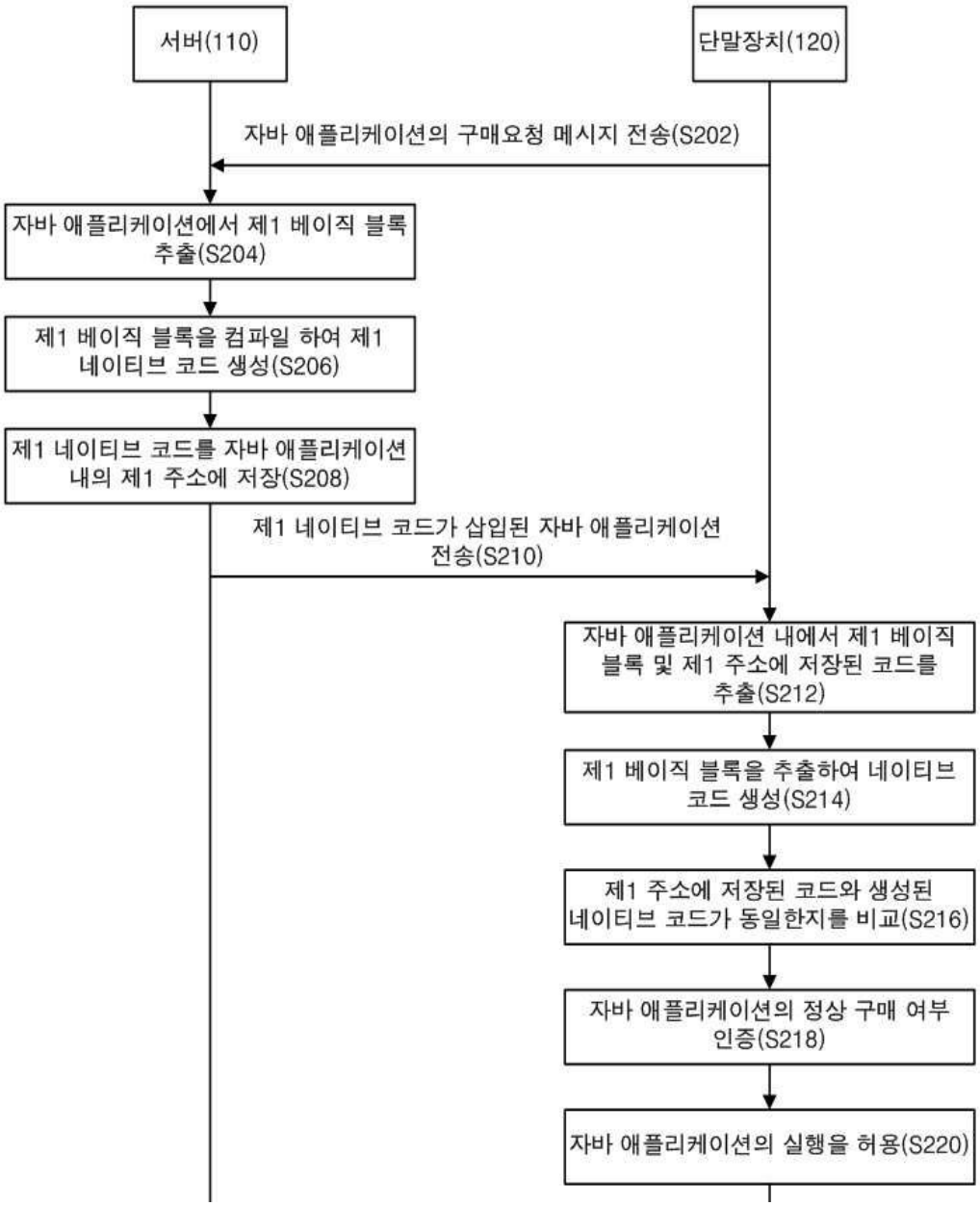
[0050] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

도면

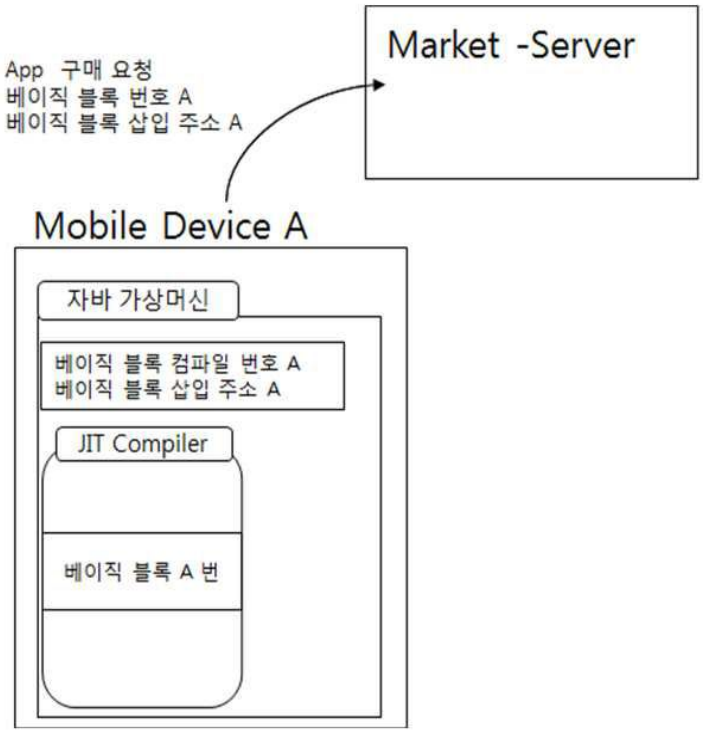
도면1



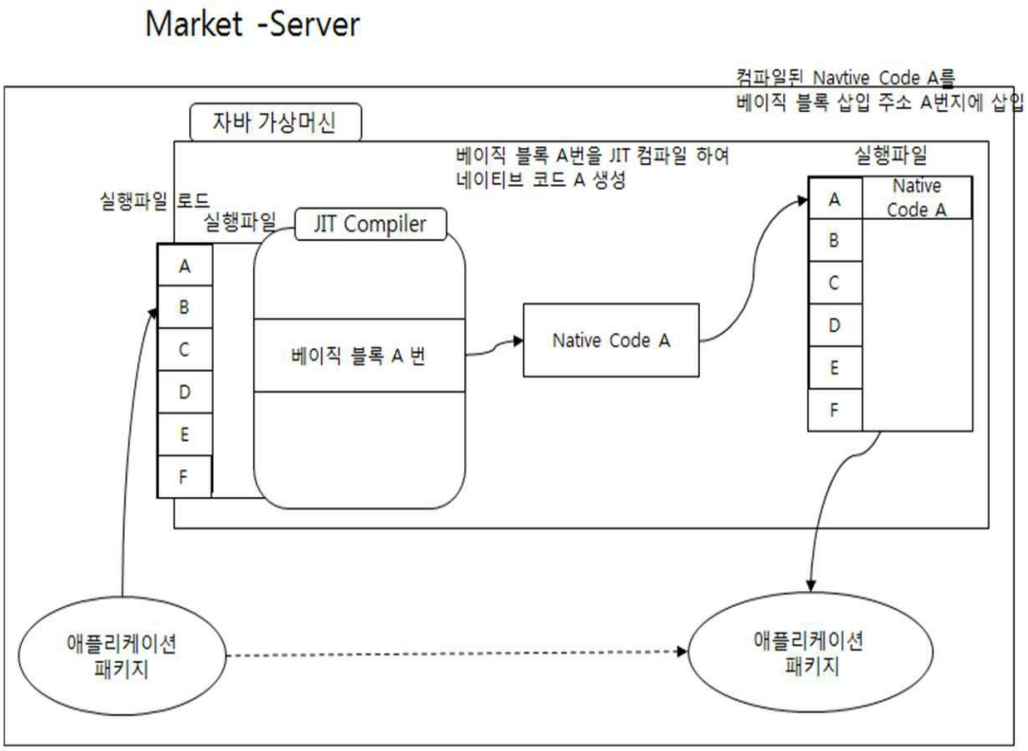
도면2


서버(110)
단말장치(120)
자바 애플리케이션의 구매요청 메시지 전송(S202)
자바 애플리케이션에서 제1 베이직 블록 추출(S204)
제1 베이직 블록을 컴파일 하여 제1 네이티브 코드 생성(S206)
제1 네이티브 코드를 자바 애플리케이션 내의 제1 주소에 저장(S208)
제1 네이티브 코드가 삽입된 자바 애플리케이션 전송(S210)
자바 애플리케이션 내에서 제1 베이직 블록 및 제1 주소에 저장된 코드를 추출(S212)
제1 베이직 블록을 추출하여 네이티브 코드 생성(S214)
제1 주소에 저장된 코드와 생성된 네이티브 코드가 동일한지를 비교(S216)
자바 애플리케이션의 정상 구매 여부 인증(S218)
자바 애플리케이션의 실행을 허용(S220)

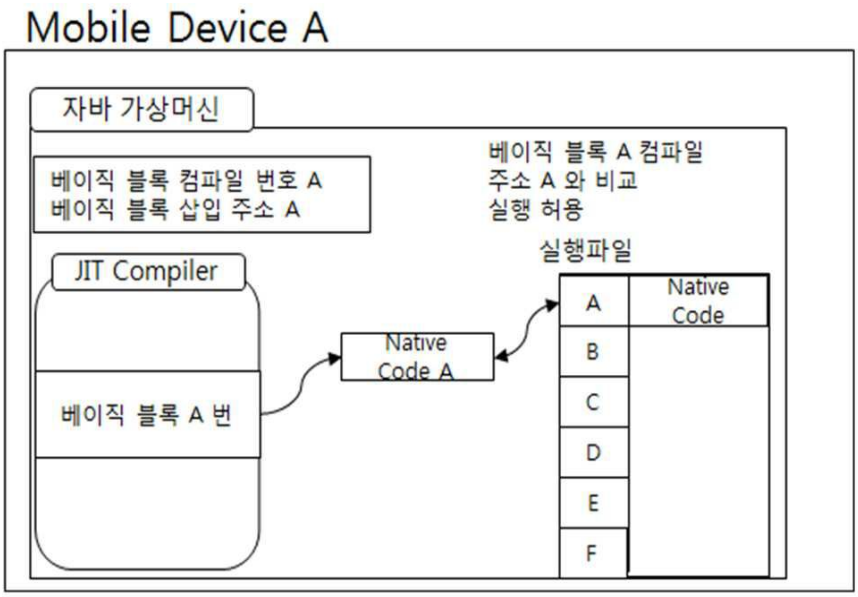
도면3


Market -Server
App 구매 요청
베이직 블록 번호 A
베이직 블록 삽입 주소 A
Mobile Device A
자바 가상머신
베이직 블록 컴파일 번호 A
베이직 블록 삽입 주소 A
JIT Compiler
베이직 블록 A 번

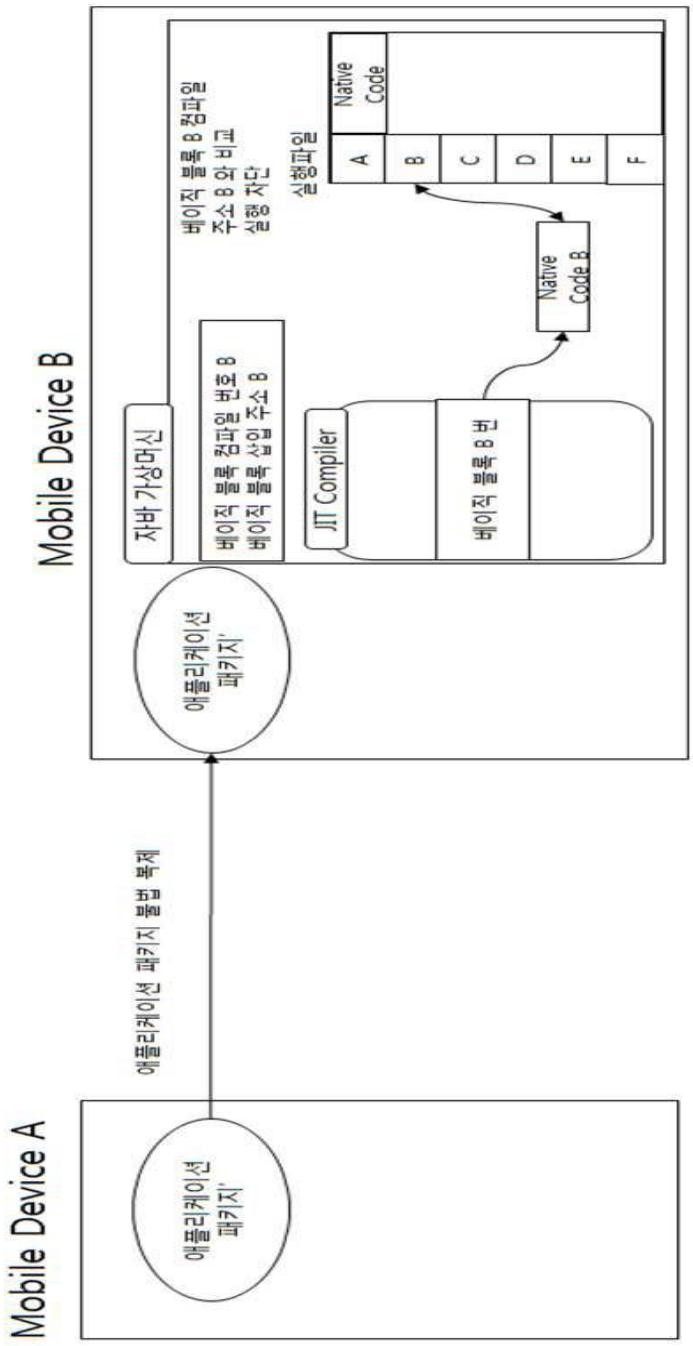
도면4


Market -Server
컴파일된 Navtive Code A를
베이직 블록 삽입 주소 A번지에 삽입
자바 가상머신
베이직 블록 A번을 JIT 컴파일 하여
네이티브 코드 A 생성
실행파일
실행파일 로드
실행파일
JIT Compiler
A
B
C
D
E
F
베이직 블록 A 번
Native Code A
Native Code A
애플리케이션 패키지
애플리케이션 패키지

도면5


Mobile Device A
자바 가상머신
베이직 블록 컴파일 번호 A
베이직 블록 삽입 주소 A
베이직 블록 A 컴파일
주소 A 와 비교
실행 허용
실행파일
JIT Compiler
베이직 블록 A 번
Native
Code A
A
B
C
D
E
F
Native
Code

도면6


Mobile Device A
애플리케이션 패키지 불법 복제
애플리케이션 패키지'
Mobile Device B
애플리케이션 패키지'
자바 가상머신
베이직 블록 컴파일 번호 B
베이직 블록 삽입 주소 B
베이직 블록 B 컴파일
주소 B 와 비교
실행 차단
실행파일
Native Code
A
B
C
D
E
F
JIT Compiler
베이직 블록 B 번
Native Code B