(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0021395
(43) 공개일자 2010년02월24일

(51) Int. Cl.
A61B 17/00 (2006.01) *A61B 19/00* (2006.01)
(21) 출원번호 10-2009-0109480(분할)
(22) 출원일자 2009년11월13일
심사청구일자 없음
(62) 원출원 특허 10-2009-0074718
원출원일자 2009년08월13일
심사청구일자 2009년08월13일

(71) 출원인
(주)미래컴퍼니
경기도 화성시 양감면 정문리 285-15
(72) 발명자
최승욱
경기도 성남시 분당구 구미동 275 베스티아2 102동 202호
(74) 대리인
안태현

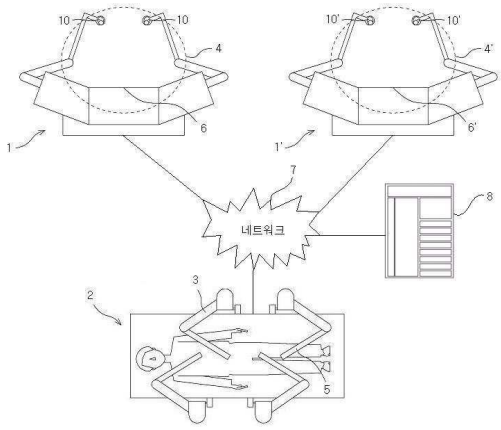
전체 청구항 수 : 총 1 항

(54) 서버 클라이언트 방식의 수술용 로봇 시스템

(57) 요 약

서버 클라이언트 방식의 수술용 로봇 시스템이 개시된다. 본 발명의 일 측면에 따르면, 제어 신호를 생성하는 복수의 컨트롤 클라이언트 및 인증된 컨트롤 클라이언트로부터 수신한 제어 신호에 상응하여 조작되는 서지컬 서버를 포함하는 수술용 로봇 시스템은 하나의 서지컬 서버를 조작하는 복수의 컨트롤 클라이언트를 구비할 수 있고, 서버 클라이언트 방식에 따른 로봇 수술 시 보안 기술을 접목하여 안전하게 수술을 수행할 수 있는 효과가 있다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호	10030794
부처명	지식경제부
연구사업명	국제공동기술개발사업
연구과제명	복강경 수술용 로봇 개발
주관기관	㈜미래컴퍼니
연구기간	2007년 12월 01일 ~ 2010년 11월 30일

특허청구의 범위

청구항 1

제어 신호를 생성하는 복수의 컨트롤 클라이언트와;

인증된 상기 컨트롤 클라이언트로부터 수신한 상기 제어 신호에 상응하여 조작되는 서지컬 서버를 포함하는 수술용 로봇 시스템.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 수술용 로봇 시스템에 관한 것으로, 특히, 서버 클라이언트 방식의 수술용 로봇 시스템에 관한 것이다.

배 경 기 술

[0002] 의학적으로 수술이란 피부나 점막, 기타 조직을 의료 기계를 사용하여 자르거나 째거나 조작을 가하여 병을 고치는 것을 말한다. 이러한 수술 중 개복수술은 복강이나 안면의 피부(skin)를 갈라서 열고 그 내부에 있는 기관 등을 치료, 성형하거나 제거하는 수술에 해당한다.

[0003] 특히, 개복수술 등을 시술할 때에는, 피부를 절개하여 들어 올림으로써 피부와 조직 사이에 소정의 공간이 형성되도록 한 후, 그 공간을 통해 수술 행위를 수행하게 된다. 따라서 개복수술은 상처가 많이 나기 때문에 수술 후 치유가 더디는 문제점이 있어서, 현재 복강경 수술이 주목받고 있다. 일반적으로 복강경 수술은 환자의 복부에 작은 구멍을 뚫은 후 이 구멍을 통해 복강의 수술부위를 관찰하면서 수술하는 방식으로, 담낭제거술, 충수돌기 절제술, 위절제술, 대장절제술 등의 외과 수술과 비뇨기과 및 산부인과 영역 등에서도 널리 이용되고 있다. 이는 신체의 내부기관을 화상 진단하는 장비로서 통상적으로 소형 카메라가 형성된 기기로 신체, 내부기관에 삽입하여 소형카메라 등으로부터 검출된 화상정보를 외부에 설치된 모니터를 통해서 관찰 할 수 있게 되어 있다.

[0004] 또한, 최근 환자에게 접근하기 어려운 환경, 예를 들면, 전장, 우주선, 전문 의료진의 접근 불능 등의 환경에서 원격 수술 시스템을 이용하여 원격수술이 수행되고 있다. 이는 통신을 이용하여 의사가 원격에서 마스터 로봇을 조작함으로써 환자가 위치한 슬레이브 로봇을 제어하여 수술을 수행하는 것이다. 종래의 수술로봇은 마스터-슬레이브 개념으로 마스터 측에서 조종을 하면 슬레이브 측에서는 그대로 따라 하는 방식이었다. 그러나 1개의 로봇을 여러 명의 의사가 조종해야 할 필요가 있을 경우, 예를 들어, 수술현장에 있는 의사와 원격지에 있는 전문의사가 같이 집도를 하는 경우에는 복수의 조작용 로봇이 필요하기 때문에 마스터-슬레이브라는 개념이 적절하지 않은 문제점이 있다.

발명의 내용

해결 하고자하는 과제

[0005] 본 발명은 하나의 서지컬 서버를 조작하는 복수의 컨트롤 클라이언트를 구비하는 수술용 로봇 시스템을 제공하기 위한 것이다.

[0006] 또한, 본 발명은 서버-클라이언트 개념에 따른 로봇 수술 시 보안 기술을 접목하여 안전하게 수술을 수행할 수 있는 수술용 로봇 시스템을 제공하기 위한 것이다.

[0007] 본 발명이 제시하는 이외의 기술적 과제들은 하기의 설명을 통해 쉽게 이해될 수 있을 것이다.

과제 해결수단

[0008] 본 발명의 일 측면에 따르면, 제어 신호를 생성하는 복수의 컨트롤 클라이언트와, 인증된 컨트롤 클라이언트로부터 수신한 제어 신호에 상응하여 조작되는 서지컬 서버를 포함하는 수술용 로봇 시스템이 제공된다.

[0009] 본 실시예는 컨트롤 클라이언트로부터 식별자를 수신하여 컨트롤 클라이언트별로 인증을 수행하는 보안 서버를

더 포함할 수 있으며, 보안 서버는 복수의 서지컬 서버 및 복수의 컨트롤 클라이언트와 통신하며, 서지컬 서버별로 컨트롤 클라이언트의 인증을 수행할 수 있다.

[0010] 또한, 보안 서버는, 컨트롤 클라이언트로부터 식별자를 수신하여 컨트롤 클라이언트별로 인증을 수행하며, 보안과 관련된 보안 정보를 저장하는 제1 보안 서버와, 제1 보안 서버와 통신하며, 제1 보안 서버에 저장된 보안 정보를 추출하는 제2 보안 서버를 포함할 수 있다.

[0011] 여기서, 식별자는 컨트롤 클라이언트를 사용하는 사용자의 사용자 ID, 지문 정보, 음성 정보 및 홍채 정보 중 어느 하나 이상의 정보가 될 수 있다.

[0012] 또한, 보안 서버는, 복수의 컨트롤 클라이언트별, 컨트롤 클라이언트를 사용하는 사용자별, 인스트루먼트 종류별 및 조작별 중 어느 하나에 상응하여 서로 다른 기능을 수행하는 권한을 설정할 수 있으며, 보안 서버는 전자서명 방식에 의해 컨트롤 클라이언트를 인증할 수 있고, 보안 서버는 컨트롤 클라이언트에 대한 보안 정보를 저장하는 디렉토리 서버에 결합할 수도 있다.

[0013] 또한, 복수의 컨트롤 클라이언트는, 서지컬 서버에 포함되는 수술용 인스트루먼트를 제어하는 인스트루먼트 제어 신호를 서지컬 서버에 전송하는 제1 컨트롤 클라이언트와, 서지컬 서버에 포함되는 비젼 시스템을 제어하는 비젼 제어 신호를 서지컬 서버에 전송하는 제2 컨트롤 클라이언트를 포함할 수 있다.

[0014] 여기서, 제어 신호는 암호화되어 서지컬 서버로 전송될 수 있으며, 제어 신호는 가상사설망(VPN)에 의해 서지컬 서버로 전송될 수 있다.

[0015] 또한, 본 실시예는 복수의 컨트롤 클라이언트가 서지컬 서버에 접속한 이력 정보를 저장하는 저장부를 더 포함할 수 있으며, 여기서, 이력 정보는 복수의 컨트롤 클라이언트의 식별자, 접속 시간, 세션 정보, 작업 내용 및 이들의 조합으로 구성된 군으로부터 선택되는 하나 이상의 정보가 될 수 있다.

[0016] 또한, 본 실시예는 컨트롤 클라이언트는 호출 정보를 생성하여 호출 정보를 다른 컨트롤 클라이언트에게 전송하는 호출 수단을 포함할 수 있으며, 호출 정보는 텍스트 정보, 영상 정보, 음성 정보, 음향 정보 및 이들의 조합으로 구성된 군으로부터 선택되는 하나 이상의 정보가 될 수 있다.

[0017] 또한, 본 실시예는 복수의 컨트롤 클라이언트 중에서 특정 컨트롤 클라이언트가 서지컬 서버를 조작하도록 설정하는 제어권 설정부를 더 포함할 수도 있다.

[0018] 또한, 컨트롤 클라이언트는 커베로스(Kerberos) 인증 방식에 의해 인증될 수 있고, 보안 서버는 인증된 컨트롤 클라이언트에 인증 티켓을 전송하며, 컨트롤 클라이언트는 수신한 인증 티켓을 이용하여 서지컬 서버에 접속할 수 있다.

[0019] 전술한 것 외의 다른 측면, 특징, 잇점이 이하의 도면, 특허청구범위 및 발명의 상세한 설명으로부터 명확해질 것이다.

효 과

[0020] 본 발명에 따른 서버 클라이언트 방식의 수술용 로봇 시스템은 하나의 서지컬 서버를 조작하는 복수의 컨트롤 클라이언트를 구비할 수 있고, 서버-클라이언트 개념에 따른 로봇 수술 시 보안 기술을 접목하여 안전하게 수술을 수행할 수 있는 효과가 있다.

발명의 실시를 위한 구체적인 내용

[0021] 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.

[0022] 제1, 제2 등과 같이 서수를 포함하는 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되지는 않는다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

[0023] 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 이

해되어야 할 것이다.

[0024] 본 명세서에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "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.

[0025] 또한, 첨부 도면을 참조하여 설명함에 있어, 도면 부호에 관계없이 동일한 구성 요소는 동일한 참조부호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다. 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0026] 도 1은 본 발명의 실시예에 따른 서버 클라이언트 방식의 수술용 로봇 시스템의 구성도이다. 도 1을 참조하면, 컨트롤 클라이언트(1, 1'), 서지컬 서버(2), 로봇 암(3), 컨트롤 인터페이스(4, 4'), 복강경(5), 모니터(6, 6'), 보안 서버(8) 및 핸들(10, 10')이 도시되어 있다. 본 실시예에 따르면, 수술시 영상을 제공하는 비젼(vision) 시스템, 예를 들면, 복강경(laparoscope), 내시경(endoscope), 현미경(microscope), 확대경, 반사경 등과 같은 기기를 제어하는 시스템이 서지컬 서버(2)에 결합할 수 있다. 이하에서는 비젼 시스템이 복강경을 제어하는 시스템인 경우를 중심으로 설명한다.

[0027] 본 실시예는 실제 환자를 대상으로 수술을 시행하는 서지컬 서버(2)를 조작하는 복수의 컨트롤 클라이언트(1, 1')를 구비함으로써, 수술의 난이도, 수술 부위, 전문 의사의 참여 등에 따라 다양한 복수의 컨트롤 클라이언트(1, 1')가 서지컬 서버(2)를 조작할 수 있도록 하는데 특징이 있다. 여기서, 복수의 컨트롤 클라이언트(1, 1')는 2개를 도시하였으나, 그 개수는 그 이상이 될 수 있음은 물론이다.

[0028] 본 실시예에 따른 컨트롤 인터페이스(4, 4')는 수술용 컨트롤 클라이언트(1, 1')에 장착되는 조작 핸들 및 핸들에 연결되는 신호 처리용 프로세서, 콘솔(console), 모니터(6, 6'), 기타 작동 스위치를 포함하는 개념으로서, 컨트롤 클라이언트(1, 1')에 대한 사용자 조작을 인식하여 서지컬 서버(2)를 작동시키기 위한 인터페이스가 되는 부분이다.

[0029] 수술을 집도하는 사용자는 컨트롤 클라이언트(1, 1')에 마련된 핸들(10, 10')을 조작함으로서 서지컬 서버(2)가 조작될 수 있도록 한다. 핸들(10, 10')은 사용자가 직접 조작할 수 있는 컨트롤 클라이언트(1, 1')와 연결된다. 컨트롤 클라이언트(1, 1')는 서지컬 서버(2)와 결합한 로봇 암(3)과 복강경이 공간상에서 이동, 회전하며, 수술 부위를 절단하거나 비추도록 하는 등 수술을 수행할 수 있도록 원격 제어한다.

[0030] 사용자는 한손 또는 양손으로 핸들(10, 10') 및 이에 부착된 버튼을 이용하여 로봇 암(3)의 위치 이동, 회전, 절단 작업 등을 수행한다. 수술 과정에서 수술 부위를 시각적으로 확인하기 위해 복강경(laparoscope)(5)이 삽입될 수 있다. 복강경(5)은 로봇 암(3)이 삽입되는 수술 부위에 근접하게 삽입될 수 있다.

[0031] 핸들(10, 10')은 그 조작방식에 따라 다양한 기구적 구성을 가질 수 있으며, 예를 들면, 조이스틱 형태, 키패드, 트랙볼, 터치스크린 등 로봇 암(3) 및 기타 수술 장비를 작동시키기 위한 다양한 입력수단이 사용될 수 있다.

[0032] 사용자는 서지컬 서버(2)가 위치한 수술실 내부를 촬영한 영상을 디스플레이부(6, 6')로 보면서 핸들(10, 10')을 조작할 수 있다. 수술실 촬영을 위한 카메라(미도시)는 수술실 내의 중요한 장면을 선별하여 촬영할 수 있다. 또한, 디스플레이부(6, 6')는 복강경이 촬영한 복강 내의 영상도 출력할 수 있다. 디스플레이부(6, 6')는 복수의 영상을 출력할 수 있다. 이 경우 디스플레이부(6, 6')의 영역은 하드웨어 또는 소프트웨어로 구현될 수 있다. 복수의 하드웨어로 구성된 모니터의 각 창에서 수신한 영상 정보를 영역별로 출력하거나 또는 하나의 모니터에 소프트웨어적으로 복수의 창을 구분하여 여러 정보를 출력할 수도 있다.

[0033] 컨트롤 클라이언트(1, 1')는 유무선 네트워크에 의해 환자가 수술을 받는 장소에 위치한 서지컬 서버(2)와 결합한다. 컨트롤 클라이언트(1, 1')와 서지컬 서버(2)는 네트워크 통신을 위한 송수신부를 구비하고 있으며, 서버-클라이언트 방식으로 네트워크가 구성될 수 있다. 즉, 서지컬 서버(2)는 네트워크 작업을 전담해서 처리하는 서버가 되며, 컨트롤 클라이언트(1, 1')는 서지컬 서버(2)에 수술용 인스트루먼트, 복강경, 로봇 암(3)과 같은 소정의 장치를 제어하는 제어 신호를 전송하여 서지컬 서버(2)를 조작하는 기능을 한다. 제어 신호는 핸들(10, 10')의 조작에 의해 생성될 수 있다. 여기서, 로봇 암(3)은 수술용 인스트루먼트, 복강경, 석션(suction) 장비, 세척(irrigation) 장비와 같이 다양한 종류의 인스트루먼트가 장착될 수 있다.

[0034] 여기서, 수술용 인스트루먼트는 일단에 조작자(미도시)를 포함하며, 조작자는 수술 환자의 체내로 삽입됨으로써 실제 수술시 수술 부위와 접촉하는 부재이다. 수술용 인스트루먼트의 조작자는 집게 동작(grip)이나 절단 동작(cutting)을 수행하는 한 쌍의 죠(jaw)를 포함할 수 있다.

[0035] 복수의 컨트롤 클라이언트(1, 1')는 동시에 하나의 서지컬 서버(2)를 제어할 수 있다. 예를 들면, 제1 컨트롤 클라이언트(1)가 서지컬 서버(2)에 결합한 인스트루먼트를 조종하여 수술을 수행하고, 제2 컨트롤 클라이언트(1')는 서지컬 서버(2)에 결합한 복강경을 조종하며, 또 다른 컨트롤 클라이언트는 서지컬 서버(2)에 결합된 기기를 이용하여 기타 보조의가 수행하는 흡인(suction), 세척(irrigation) 등과 같은 작업을 수행할 수도 있다. 이를 위해 제1 컨트롤 클라이언트(1)는 인스트루먼트를 제어하는 인스트루먼트 제어 신호를 서지컬 서버(2)에 전송하고, 제2 컨트롤 클라이언트(1')는 비젼 시스템(예를 들면, 복강경)을 제어하는 비젼 제어 신호(예를 들면, 복강경 제어 신호)를 서지컬 서버(2)에 전송한다. 서지컬 서버(2)는 해당 제어 신호를 수신하고 이에 상응하여 수술용 인스트루먼트, 복강경과 같이 결합된 장치를 조작할 수 있다.

[0036] 또한, 본 실시예에 따르면, 사용자의 전문성에 맞게 특정 컨트롤 클라이언트(1, 1')가 서지컬 서버(2)에 대한 제어권을 가지도록 설정할 수 있다. 예를 들면, 수술현장에서 하나의 컨트롤 클라이언트(1)가 서지컬 서버(2)를 조종하여 수술을 수행하고, 고난도 수술이 요구되는 시점에서 다른 컨트롤 클라이언트(1')에 서지컬 서버(2)의 제어권이 전달될 수도 있다.

[0037] 보안 서버(8)는 복수의 컨트롤 클라이언트(1, 1')와 서지컬 서버(2)의 통신에 보안 기술을 적용하기 위해 마련되는 서버이다. 보안 서버(8)는 서지컬 서버(2)에 모듈화되어 구비되거나 별도의 장비로 구비될 수 있다. 보안 서버(8)는 컨트롤 클라이언트(1, 1') 및 서지컬 서버(2)와 병렬 또는 직렬로 결합할 수 있다. 통신 보안을 위해서는 하나의 서지컬 서버(2)에 복수의 컨트롤 클라이언트(1, 1')가 접속하기 때문에 접속하는 주체가 누구인지, 권한은 어떠한지 확인할 필요가 있다. 이러한 필요에 의해 통신 보안 기술은, 예를 들면, 식별(Identification), 인증(Authentication), 인가(Authorization), 기밀성(Confidentiality), 무결성(Integrity), 감사 증적(Audit Trail)과 같은 기능을 충족할 수 있다. 이에 대해서는, 도 3을 참조하여 자세히 설명하도록 한다.

[0038] 서지컬 서버(2)의 제어권은 다양한 방식으로 복수의 컨트롤 클라이언트(1, 1')들 간에 전달될 수 있다. 보안 서버(8)의 인가(Authorization) 여부에 따라 컨트롤 클라이언트(1, 1')의 제어권을 설정할 수 있다. 본 발명의 일 실시예에 따르면, 하나의 컨트롤 클라이언트(1)가 특정 기능에 대한 제어권 설정 신호를 서지컬 서버(2)에 전달하면, 보안 서버(8)는 컨트롤 클라이언트(1)의 해당 기능에 대한 권한 유무를 판단하여 해당 기능에 대한 인가 여부를 판단하고, 만약, 인가된 경우 해당 컨트롤 클라이언트(1)는 해당 기능에 대해 서지컬 서버(2)를 제어할 수 있다. 제어권 설정 신호는 이를 생성하는 컨트롤 클라이언트(1)에 서지컬 서버(2)의 제어권을 설정하도록 요청하거나 다른 컨트롤 클라이언트(1')에 서지컬 서버(2)의 제어권을 설정하도록 요청하는 신호가 될 수 있다. 후자의 경우 컨트롤 클라이언트(1)를 조작하는 한 의사가 다른 컨트롤 클라이언트(1')를 조작하는 의사에게 수술을 집도하도록 요청하기 위한 기능이 될 수 있다.

[0039] 이러한 제어권 설정 신호는 각 기능별로 구분될 수 있다. 예를 들면, 하나의 컨트롤 클라이언트(1)는 수술용 인스트루먼트 조작, 복강경 조작, 석션 장치 조작, 세척 장치 조작과 같은 다양한 기능을 수행할 수 있으므로, 컨트롤 클라이언트(1)는 각 기능별 제어권 설정 신호를 서지컬 서버(2)에 전달함으로써, 제어권 설정을 요청할 수 있다. 보안 서버(8)는 컨트롤 클라이언트(1)의 권한 유무를 각 기능별로 판단하여 제어권 설정 요청에 응답함으로써, 컨트롤 클라이언트(1)가 서지컬 서버(2)를 제어할 수 있도록 한다. 보안 서버(8)는 각 컨트롤 클라이언트(1, 1')의 권한 여부를 미리 저장부에 저장하고 있으며, 해당 제어권 설정 요청이 있는 경우 각 기능별로 제어 가능 여부에 대해서 저장부에 저장함으로써 각 컨트롤 클라이언트(1, 1')의 제어권을 설정할 수 있다.

[0040] 본 발명의 다른 실시예에 의하면, 사용자가 서지컬 서버(2)에 결합한 서지컬 콘솔(미도시)을 이용하여 해당 기능을 수행할 특정 컨트롤 클라이언트(1, 1')를 직접 지정할 수도 있다. 서지컬 콘솔(미도시)은 컨트롤 클라이언트(1, 1') 중 특정 컨트롤 클라이언트일 수도 있다. 예를 들면, 수술을 전체적으로 관리하며 서지컬 서버(2)에 결합한 서지컬 콘솔을 조작하는 사용자는, 제1 컨트롤 클라이언트(1)가 가지고 있던 서지컬 서버(2)의 제어권을 제2 컨트롤 클라이언트(1')에게 할당할 수 있다. 이러한 방식에 따르면, 수술을 전체적으로 관리하는 사용자가 전문적 기술 요청, 단계적 수술 진행과 같은 필요에 의해 수술을 집도하는 컨트롤 클라이언트를 직접 바꿀 수 있는 장점이 있다. 이 경우 제1 컨트롤 클라이언트(1)의 서지컬 서버(2)에 대한 제어권은 그대로 유지되거나 또는 상실될 수 있다. 제어권의 유지 유무는 서지컬 콘솔의 사용자가 설정하는 바에 따라서 달라질 수 있다.

[0041] 이러한 제어권 할당을 위해서 서지컬 콘솔은 제어권 설정부를 포함할 수 있다. 제어권 설정부는 서지컬 서버

(2)와 결합된 각 기기에 대한 제어권을 컨트롤 클라이언트별로 할당할 수 있도록 한다. 예를 들면, 제어권 설정부는 수술용 인스트루먼트에 대한 제어권은 제1 컨트롤 클라이언트(1)에게 할당하고, 복강경에 대한 제어권은 컨트롤 클라이언트(1')에게 할당할 수 있다. 이러한 제어권 할당 정보는 데이터베이스에 저장되며, 사용자 인터페이스(UI)를 이용하는 사용자에 의해 수정될 수 있다. 여기서, 사용자 인터페이스는 버튼과 화면(터치스크린을 포함함)을 구비하고, 사용자가 특정 기기에 대한 제어권을 특정 컨트롤 클라이언트에게 할당할 수 있도록 한다.

[0042] 도 2는 본 발명의 실시예에 따른 서버 클라이언트 방식의 수술용 로봇 시스템의 제1 컨트롤 클라이언트(1)의 도면이다. 도 2를 참조하면, 제1 컨트롤 클라이언트(1)는 디스플레이부(6), 핸들(10), 호출 수단(20)을 포함할 수 있다. 상술한 바와의 차이점을 설명한다.

[0043] 호출 수단(20)은 호출 정보를 생성하여 제2 컨트롤 클라이언트(1')에게 전송한다. 호출 정보는 컨트롤 클라이언트(1, 1')들 간에 교환되는 정보를 나타내거나 또는 서로 호출하는 정보가 될 수 있다. 예를 들면, 제1 컨트롤 클라이언트(1)를 조작하는 의사가 제2 컨트롤 클라이언트(1')를 조작하는 의사에게 의사전달을 하거나 서지컬 서버(2)의 제어권 설정을 요청하는 경우 호출 수단(20)을 이용하여 해당 정보를 전송할 수 있다.

[0044] 호출 정보는 텍스트 정보, 영상 정보, 음성 정보, 음향 정보 및 이들의 조합으로 구성된 군으로부터 선택되는 하나 이상의 정보가 될 수 있다. 호출 정보가 텍스트 정보인 경우, 호출 수단(20)은 텍스트 입력기(예를 들면, 미리 정해진 문구 입력기, 자판기 등)가 될 수 있으며, 해당 텍스트 정보는 제2 컨트롤 클라이언트(1')의 디스플레이부(6')에 출력될 수 있다.

[0045] 호출 정보가 음성 정보인 경우 호출 수단(20)은 마이크가 될 수 있으며, 입력된 음성 정보는 제2 컨트롤 클라이언트(1')에 구비된 스피커(미도시)에서 출력될 수 있다. 컨트롤 클라이언트(1, 1')의 사용자간 의사 소통을 위해 제1 컨트롤 클라이언트(1)에도 스피커가 구비될 수 있다. 이러한 호출 수단(20)을 이용하여 사용자는 컨트롤 클라이언트(1, 1')의 사용자간 의사 소통, 설정 요청 등의 작업을 수행할 수 있다.

[0046] 도 3은 본 발명의 실시예에 따른 서버 클라이언트 방식의 수술용 로봇 시스템의 보안 서버(8)의 블록 구성도이다. 도 3을 참조하면, 권한 설정부(81), 암호화부(83), 인증부(85), 저장부(87), 제어권 설정부(89)가 도시된다. 여기서는 설명의 편의상 보안 서버(8)가 별도의 장치인 경우를 설명하지만, 후술할 내용은 서지컬 서버(2)에 모듈로 구현된 경우에도 적용될 수 있음은 물론이다.

[0047] 보안 서버(8)는 식별(Identification), 인증(Authentication), 인가(Authorization), 기밀성(Confidentiality), 무결성(Integrity), 감사 증적(Audit Trail)과 같은 기능을 수행할 수 있다.

[0048] 식별(Identification)은 식별자, 예를 들면, 컨트롤 클라이언트(1, 1')를 사용하는 사용자의 사용자 ID, 지문인식, 음성 인식 및 홍채인식 등과 같은 바이오 인식기능을 통해 "누가"(어떤 사용자가) 접속하는지를 확인하는 과정이다. 보안 서버(8)는 복수의 컨트롤 클라이언트(1, 1')로부터 그 사용자의 ID, 지문 정보, 음성 정보 및 홍채 정보 중 어느 하나 이상의 정보를 수신하며, 이를 저장부(87)에 미리 저장된 기준 정보와 비교하고 동일 여부를 판단함으로써 접촉 주체를 식별한다. 컨트롤 클라이언트(1, 1')가 자신의 식별자를 보안 서버(8)에 전송하면, 인증부(85)는 이를 이용하여, 접속 가능한 주체인지를 판단한다. 컨트롤 클라이언트(1, 1')의 식별자는 각 장치의 신원을 나타내기 때문에 사용자의 책임추적성(Accountability)을 분석하는 자료로 사용될 수도 있다.

[0049] 인증(Authentication)은 접속한 사용자가 "진짜"인지 확인하는 과정이다. 인증 방식은 사용자가 알고 있는 지식 기반의 인증 방식(예를 들면, 패스워드), 사용자가 소유하는 인증장비를 이용한 인증 방식(예를 들면, 키, 스마트 카드, 토큰 등), 사용자의 물리적인 인증 특성을 이용하는 방식(예를 들면, 손가락 지문, 음성 인식, 홍채 인식 등), 사용자의 무의식적인 행위에 의한 인증 방식(예를 들면, 사인(signature) 인증) 등이 있다. 상술한 바와 같이 보안 서버(8)는 복수의 컨트롤 클라이언트(1, 1')로부터 그 사용자의 사용자 ID, 지문 정보, 음성 정보 및 홍채 정보 중 어느 하나 이상의 정보를 수신하며, 이를 저장부(87)에 미리 저장된 기준 정보와 비교하고 동일 여부를 판단함으로써 인증할 수 있다.

[0050] 또한, 병원/원격지에 여러 개의 컨트롤 클라이언트(1, 1')가 있는 경우 어느 컨트롤 클라이언트(1, 1')에서 접근하는지를 제어하기 위해 컨트롤 클라이언트(1, 1')별로 부여된 식별자를 이용하여 인증하거나 사용자가 지정된 장치로부터 접속하는지를 확인하는 노드 인증(Node Authentication)을 수행할 수도 있다. 이를 위해 인증부(85)는 미리 해당 노드에 대한 식별자(예를 들면, 프로토콜)를 저장부(87)에 저장하고, 접속된 장치에 대한 노드 식별자를 이용하여 인증을 수행할 수 있다. 이 때 컨트롤 클라이언트(1, 1')와 보안 서버(8)는 전자인증서를 사용하여 상호 확인할 수도 있다.

[0051] 또한, 다른 실시예에 따르면, 상술한 사용자 인증을 위하여 커베로스(Kerberos) 인증 프로토콜이 사용될 수 있

다. 예를 들면, 사용자가 컨트롤 클라이언트(1, 1')를 이용하여 보안 서버(8)에 접속하면, 보안 서버(8)는 접속한 컨트롤 클라이언트(1, 1')에 대해 상술한 다양한 인증 방식을 이용하여 인증을 수행한 후 소정의 인증 티켓을 인증된 컨트롤 클라이언트(1, 1')에 전송한다. 이후 컨트롤 클라이언트(1, 1')는 수신한 인증 티켓을 이용하여 서지컬 서버(2)에 접속할 수 있다. 서지컬 서버(2)는 접속한 컨트롤 클라이언트(1, 1')의 접속 신호에서 해당 인증 티켓의 유무를 확인하여 인증 티켓이 있는 경우 접속이 가능하도록 할 수 있다.

[0052] 인증 티켓은 발송일시, 유효 사용 기간에 대한 정보를 포함할 수 있으며, 이 경우 컨트롤 클라이언트(1, 1')는 유효 사용 기간 동안에만 서지컬 서버(2)에 접속하여 관련 기능을 수행하도록 설정됨으로써, 제3자의 접근 가능성을 제한하고, 상술한 다양한 인증 방식에 사용된 사용자의 식별자(예를 들면, 사용자 ID, 지문 정보, 음성 정보 및 홍채 정보 등)가 누설되는 위험 부담을 줄일 수 있는 장점이 있다. 여기서는 커베로스(Kerberos) 인증시 키 분배 센터(KDC)가 보안 서버(8)인 경우를 설명하였으나, 별도의 서버로 구현되거나 또는 보안 서버(8)와 물리적으로 동일한 서버에 위치하며 소프트웨어적으로 상술한 기능을 수행하도록 구현될 수도 있음은 물론이다. 상술한 인증 티켓은 그 명칭에 한정되지 않고 신분 증명서, TGT(ticket-granting ticket), 티켓, 인증 정보 등 다양한 명칭으로 표현될 수 있으며, 상술한 바와 다른 방식의 커베로스 인증 방식이 본 발명에 적용될 수 있음은 물론이다.

[0053] 또한, 인증 티켓은 후술할 바와 같이 컨트롤 클라이언트(1, 1')별, 사용자별, 인스트루먼트 종류별 및 조작별로 다르게 부여된 권한에 대한 정보를 포함할 수도 있다. 예를 들면, 컨트롤 클라이언트(1, 1')가 서지컬 서버(2)에 접속시 서지컬 서버(2)는 해당 정보를 독취하여 컨트롤 클라이언트(1, 1')가 인증 티켓에 포함된 권한에 대한 정보 내에서 다양한 기능별로 작업을 수행할 수 있도록 한다.

[0054] 인가(Authorization)는 접근한 컨트롤 클라이언트(1, 1')가 집도를 할 권한이 있는지, 복강경만 움직일 수 있는지 등, 어떤 권한을 가지고 있는지 확인하는 권한 확인 과정이다. 이를 위해 권한 설정부(81)는 컨트롤 클라이언트(1, 1')별, 사용자별, 각 기능별 권한 유무를 미리 저장부(87)에 저장할 수 있다. 권한 설정부(81)는 어떤 사용자가 그 시스템을 액세스할 수 있는지, 그리고 부여된 사용권한은 어디까지인지(허용된 액세스 시간, 제어가 허용된 장치 종류)를 미리 정의함으로써 어떤 사용자가 컴퓨터 운영체제나 응용프로그램에 로그온 했을 때, 그 시스템이나 응용프로그램은 그 세션 동안 그 사용자에게 어떤 자원의 이용을 허락해야 하는지 결정하도록 할 수 있다.

[0055] 본 실시예에 따른 권한은 다양한 기능별로 구분될 수 있으며, 예를 들면, 로봇 암(3)의 위치 이동, 회전 등의 권한, 수술용 인스트루먼트의 이동, 회전, 절단 등의 권한, 복강경(5)의 이동 및 복강경(5)이 촬영한 이미지의 관찰 권한 등 조작별로 구분될 수 있다. 이러한 권한은 컨트롤 클라이언트(1, 1')별, 사용자별, 인스트루먼트 종류별 및 조작별로 다르게 부여되어 저장부(87)에 저장될 수 있다. 예를 들면, 저장부(87)는 컨트롤 클라이언트(1, 1')별, 사용자별, 인스트루먼트 종류별 및 조작별 필드를 가지는 데이터베이스가 포함되며, 각 필드별로 권한 유무가 저장될 수 있다. 이러한 권한부여는 권한 설정부(81)에 의해 미리 설정되는 권한들과 컨트롤 클라이언트(1, 1')가 액세스를 해 왔을 때 미리 설정된 권한을 실제로 확인하는 과정이다.

[0056] 기밀성(Confidentiality)은 컨트롤 클라이언트(1, 1')와 서지컬 서버(2) 간의 통신을 암호화하여 중간에서 내용을 알아볼 수 없도록 하는 기술과 관련된다. 통신에 사용되는 다양한 암호화 기법이 본 실시예에 적용될 수 있을 뿐만 아니라 가상사설망(VPN : Virtual Private Network)이 컨트롤 클라이언트(1, 1')와 서지컬 서버(2) 간에 설정되어 사용될 수도 있다. 암호화부(83)는 암호 방식을 미리 설정하고, 암호 방식에 따라 정보를 송신하거나 수신된 정보를 해석하는 기능을 수행한다.

[0057] 무결성(Integrity)은 컨트롤 클라이언트(1, 1')와 서지컬 서버(2) 간의 통신이 무결한지를 보증하기 위한 과정으로, 본 실시예에 전자 서명(Digital signature)과 같은 기술이 적용될 수 있다. 즉, 인증부(8)는 전자 서명 방식에 의해 접속한 컨트롤 클라이언트의 식별자 및 전자인증서를 이용하여 인증할 수 있다. 여기서, 전자인증서는 PKI(Public Key Infrastructure) 방식의 전자인증서일 수 있다.

[0058] 감사 증적(Audit Trail)은 컨트롤 클라이언트(1, 1')와 서지컬 서버(2)의 모든 동작상황을 로그 형태로 관리하는 과정이다. 저장부(87)는 복수의 컨트롤 클라이언트(1, 1')가 서지컬 서버(2)에 접속한 이력 정보를 저장할 수 있다. 여기서, 저장 형태는 로그를 그 자체로 저장할 수도 있고, 로그를 별도의 로그 서버로 전송할 수도 있다. 로그 형태는 단순 텍스트(text) 파일일 수도 있으며 XML 문서일 수도 있고, 제3의 다른 형태일 수도 있다. 이러한 이력 정보는 복수의 컨트롤 클라이언트(1, 1')의 식별자, 접속 시간, 세션 정보, 작업 내용 및 이들의 조합으로 구성된 군으로부터 선택되는 하나 이상의 정보가 될 수 있다.

[0059] 보안 서버(8)는 복수의 컨트롤 클라이언트(1, 1') 중에서 특정 컨트롤 클라이언트가 서지컬 서버(2)를 조작하도록 설정하는 제어권 설정부(89)를 더 포함할 수 있다. 상술한 바와 같이 사용자가 특정 기능을 수행할 컨트롤 클라이언트(1, 1')를 직접 지정하는 경우 사용자는 제어권 설정부(89)를 통해 특정 컨트롤 클라이언트(1, 1')가 특정 기능에 대한 제어권을 가지도록 설정할 수 있다. 제어권 설정부(89)는 컨트롤 클라이언트(1, 1')별, 사용자별로 기능별 권한을 다르게 설정하여 저장부(87)에 저장한다. 이 경우 제어권 설정부(89)는 해당 제어권을 설정하기 위한 인터페이스, 소스 편집기와 같이 저장부(87)에 저장된 제어권에 대한 정보를 수정할 수 있는 수단이 될 수 있다.

[0060] 또한, 다른 실시예에 따르면, 보안 서버(8)는 복수의 서지컬 서버(2) 및 복수의 컨트롤 클라이언트(1, 1')와 통신하여, 서지컬 서버(2)별로 컨트롤 클라이언트(1, 1')의 인증을 수행할 수 있다. 즉, 보안 서버(8)는 상술한 바와 같이 하나의 서지컬 서버(2)에 대해 복수의 컨트롤 클라이언트(1, 1')를 인증함으로써 보안을 지원할 뿐만 아니라 복수의 서지컬 서버(2) 및 복수의 컨트롤 클라이언트(1, 1')의 보안을 지원할 수도 있다. 예를 들면, 복수의 서지컬 서버(2) 중 특정 서지컬 서버(2)에 대해서 복수의 컨트롤 클라이언트(1, 1')는 서로 다르게 인증되거나 권한이 부여될 수 있으므로, 보안 서버(8)는 각 서지컬 서버(2)에 대한 각 컨트롤 클라이언트(1, 1')의 보안 정보를 달리 설정 및 저장할 수 있다. 이러한 실시예에 따르면, 하나의 보안 서버(8)가 복수의 서지컬 서버(2) 및 복수의 컨트롤 클라이언트(1, 1')를 관리함으로써 관리의 편리성 및 통일성을 보장할 수 있는 장점이 있다.

[0061] 또한, 다른 실시예에 따르면, 보안 서버(8)의 개수는 복수개가 될 수 있다. 즉, 본 실시예는 백업용 또는 원격 수술 등의 목적으로 복수의 보안 서버(8)를 구비할 수 있으며, 각 보안 서버(8)는 다른 보안 서버(8)와 보안과 관련되는 정보인 보안 정보를 공유하거나 복제함으로써 참조할 수 있다. 예를 들면, 보안 서버(8)는 상술한 바와 같이 컨트롤 클라이언트(1, 1')로부터 식별자를 수신하여 컨트롤 클라이언트별(1, 1')로 인증을 수행하며, 보안과 관련된 보안 정보를 저장하는 제1 보안 서버(미도시)와, 제1 보안 서버와는 다른 형태(소프트웨어적인 형태 또는 유형의 하드웨어 형태)로 구현되어 제1 보안 서버에 저장된 보안 정보를 추출함으로써 보안 정보를 공유하거나 복제할 수 있는 제2 보안 서버(미도시)를 포함할 수 있다. 여기서, 보안 정보는 식별, 인증, 인가, 기밀성, 무결성, 감사 증적과 같은 기능을 수행하기 위해 상술한 다양한 정보를 포함하며, 저장부(87)에 저장되는 정보가 될 수 있다.

[0062] 또한, 제1 보안 서버와 제2 보안 서버 중 하나의 보안 서버(8)는 메인 보안 서버로 기능할 수도 있다. 예를 들면, 제1 보안 서버가 메인 보안 서버로 설정되는 경우 제1 보안 서버의 저장부(87)의 내용이 수정되면, 제2 보안 서버는 이를 제2 보안 서버의 저장부(87)에 복제함으로써 내용을 동기화시킬 수 있다. 이 경우 보안 정책이 변경되거나 또는 컨트롤 클라이언트(1, 1')별, 사용자별, 기능별 권한이 달라지는 경우 제1 보안 서버에 포함되는 저장부(87)의 해당 내용만 변경되면 다른 보안 서버의 내용도 변경된다. 따라서 본 실시예에 따르면, 보안 서버(8)의 관리 편리성이 증대되는 장점이 있다.

[0063] 또한, 다른 실시예에 따르면, 보안 서버(8)는 네트워크 자원에 대한 정보를 담고 있는 디렉토리를 이용하여 전체 망을 관리하는 디렉토리 서버(directory server)에 결합할 수 있다. 즉, 디렉토리 서버는 컨트롤 클라이언트(1, 1')에 대한 보안 정보를 디렉토리로 저장하며, 보안 서버(8)는 이러한 디렉토리 서버에 결합하여 관련 보안 정보를 추출 및 변경할 수 있다. 여기서, 디렉토리 서버는 다양하게 구현될 수 있으며, 예를 들면, X.500 디렉토리 서비스 또는 액티브 디렉토리와 같은 디렉토리 서버가 될 수 있다. 디렉토리 서버에 대한 기술은 당업자에게 널리 알려져 있으므로, 이에 대한 자세한 설명은 생략한다. 본 실시예에 따르면, 보안 서버(8)는 상술한 바와 같은 디렉토리 서버에 결합함으로써 컨트롤 클라이언트(1, 1')에 대해 총괄적으로 편리하게 보안 관리를 할 수 있는 장점이 있다.

[0064] 그 외 본 발명의 실시예에 따른 서버 클라이언트 방식의 수술용 로봇 시스템에 대한 임베디드 시스템, O/S 등의 공통 플랫폼 기술과 통신 프로토콜, I/O 인터페이스 등 인터페이스 표준화 기술 및 엑추에이터, 배터리, 카메라, 센서 등 부품 표준화 기술 등에 대한 구체적인 설명은 생략하기로 한다.

[0065] 상기한 바에서, 본 발명의 실시예에 따른 서버 클라이언트 방식의 수술용 로봇 시스템은 컨트롤 클라이언트(1, 1'), 서지컬 서버(2), 보안 서버(8)의 명칭, 개수, 구성, 연결 관계를 일 실시예에 따라 기술하였으나, 반드시 이에 한정될 필요는 없고, 명칭, 개수, 구성, 연결 관계가 달라지더라도 전체적인 작용 및 효과에는 차이가 없다면 이러한 다른 구성은 본 발명의 권리범위에 포함될 수 있으며, 해당 기술 분야에서 통상의 지식을 가진 자라면 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면의 간단한 설명

[0066] 도 1은 본 발명의 실시예에 따른 서버 클라이언트 방식의 수술용 로봇 시스템의 구성도.

[0067] 도 2는 본 발명의 실시예에 따른 서버 클라이언트 방식의 수술용 로봇 시스템의 컨트롤 클라이언트의 도면.

[0068] 도 3은 본 발명의 실시예에 따른 서버 클라이언트 방식의 수술용 로봇 시스템의 보안 서버의 블록 구성도.

[0069] <도면의 주요부분에 대한 부호의 설명>

[0070] 1, 1' : 컨트롤 클라이언트 2 : 서지컬 서버

[0071] 3 : 로봇 암 4, 4' : 컨트롤 인터페이스

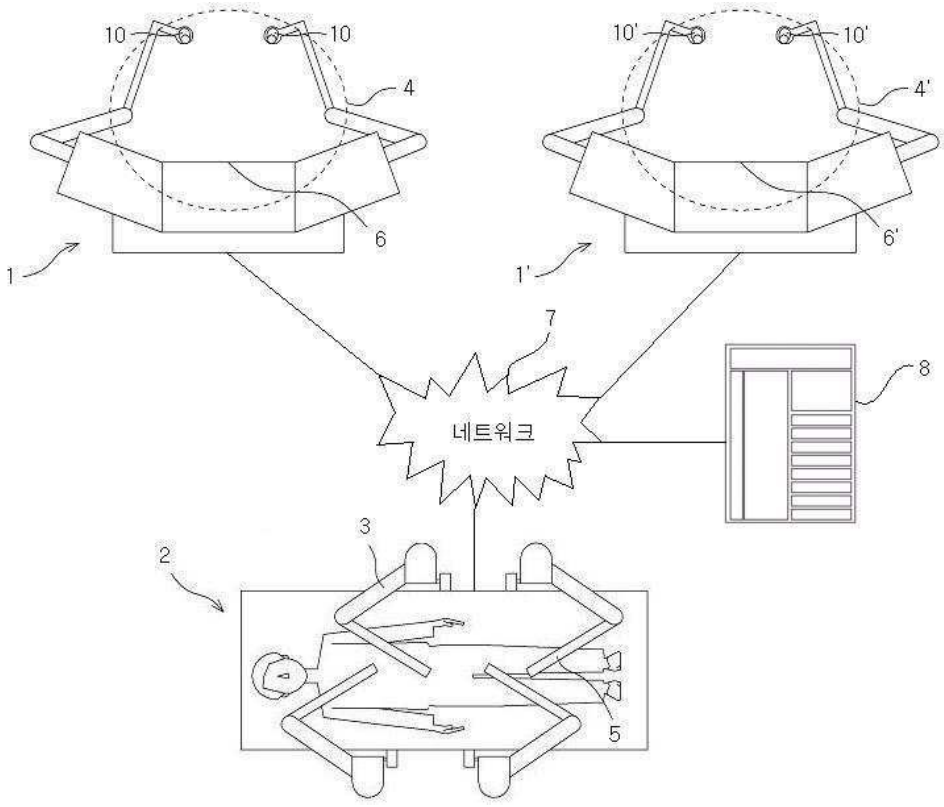
[0072] 5 : 복강경 6, 6' : 모니터

[0073] 8 : 보안 서버 10, 10' : 핸들

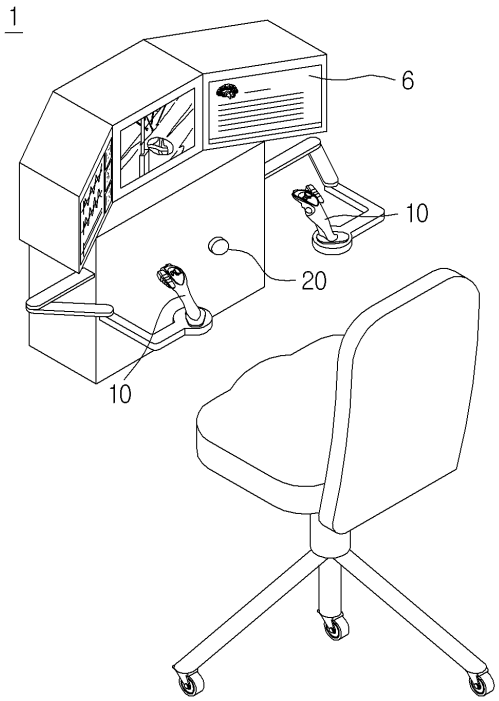
[0074]

도면

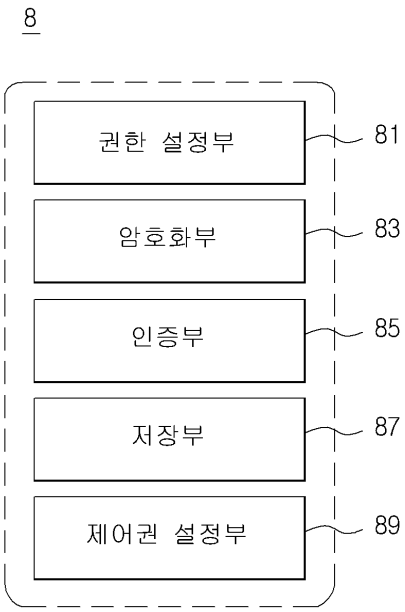
도면1



도면2



도면3



专利名称(译)	基于服务器的手术机器人系统		
公开(公告)号	KR1020100021395A	公开(公告)日	2010-02-24
申请号	KR1020090109480	申请日	2009-11-13
申请(专利权)人(译)	未来公司公司		
当前申请(专利权)人(译)	未来公司公司		
[标]发明人	CHOI SEUNG WOOK		
发明人	CHOI SEUNG WOOK		
IPC分类号	A61B17/00 A61B19/00		
外部链接	Espacenet		

摘要(译)

目的：提供一种服务器客户端方法的手术机器人系统，为机器人手术增加安全技术，进行安全手术。组成：服务器客户端方法的手术机器人系统包括：手术服务器（2），其组合到控制诸如腹腔镜，内窥镜，放大镜和反射器的设备的系统;操作手术服务器的多个控制客户端（1,1'）；控制接口（4,4'）包括信号处理器，控制台，监视器（6,6 '），操纵手柄和操作开关。控制界面是用于通过识别用户操纵来控制客户端来操作手术服务器的界面。