(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 549 506**

(51) Int. CI.:

G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.03.2010 E 10847122 (8)**

(97) Fecha y número de publicación de la concesión europea: **15.07.2015 EP 2542744**

(54) Título: **Sistema de autenticación sin discontinuidad**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.10.2015

(73) Titular/es:

UTC FIRE & SECURITY CORPORATION (100.0%)
Nine Farm Springs Road
Farmington, Connecticut 06034, US

(72) Inventor/es:

LAKAMRAJU, VIJAYA RAMARAJU;
SOLDNER, NICHOLAS CHARLES y
BAJEKAL, SANJAY

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Sistema de autenticación sin discontinuidad

ANTECEDENTES

La presente invención se refiere a sistemas de comunicación y, más concretamente, a un sistema de seguridad que proporciona acceso a o desde un espacio controlado.

Hay muchos sistemas de seguridad o control de acceso para bloquear y desbloquear puertas o portales, tales como aquellos usados para entrar o salir de edificios comerciales, edificios residenciales y vehículos a motor. Los sistemas de seguridad electrónicos típicamente emplean una credencial en forma de una tarjeta en combinación con un lector de tarjeta de banda magnética o un lector de tarjeta inteligente de bajo alcance (generalmente menor que 10 cm). Se puede emplear un teclado numérico que requiera al usuario introducir un código pin en combinación con la tarjeta/lector o como una medida de seguridad independiente.

El lector de tarjeta típicamente se monta en la pared cerca de la puerta o es parte de la cerradura de la puerta y la credencial se transporta por el usuario. En tal disposición, el lector se puede alimentar o bien por línea o bien por batería y la credencial generalmente es pasiva (sin batería). También existen sistemas de seguridad con funcionalidad similar que utilizan credenciales activas.

Los sistemas de seguridad convencionales que emplean credenciales pasivas o activas típicamente sufren de diversos inconvenientes o rasgos indeseables. Por ejemplo, los sistemas de seguridad con credenciales activas son caros y tienen vida limitada debido al uso de baterías primarias o secundarias. Adicionalmente, la mayoría de los sistemas de seguridad requieren acciones “sin valor añadido” por el usuario para abrir una puerta asegurada. Como consecuencia de estas acciones sin valor añadido, el usuario no puede abrir la puerta asegurada en un movimiento suave, natural simplemente girando la manilla de la puerta (como si la puerta estuviera desbloqueada) o entrando en contacto con un área específica de la puerta. En su lugar, el usuario debe situar físicamente la credencial y colocarla o bien en o bien cerca del lector de tarjeta o, alternativamente, introducir un código pin. Estas acciones sin valor añadido pueden ralentizar en gran medida la entrada o salida del usuario.

El documento EP 0770749 A2 describe un sistema que tiene los rasgos del preámbulo de la reivindicación 1. El documento US 2001/0052839 A1 describe un sistema de control de puerto de vehículo que comprende un sensor capaciflexivo, un puerto, un cierre que asegura el puerto y una unidad de control. El documento US 2007/0176437 describe un conjunto de manilla para una cerradura con un pestillo para permitir acceso a usuarios autenticados.

COMPENDIO

La presente invención proporciona un sistema para proporcionar acceso a o desde un espacio controlado según la reivindicación 1.

Un sistema para proporcionar acceso a o desde un espacio controlado incluye una credencial, un módulo lector, un sensor de infrarrojos pasivo y un controlador. La credencial envía y recibe señales y está configurada para ser usada o transportada por un usuario. El módulo lector envía y recibe señales para detectar la credencial. El sensor de infrarrojos pasivo está adaptado para detectar la presencia del usuario adyacente a una entrada a o salida del espacio controlado. El controlador es sensible al sensor de infrarrojos pasivo para dirigir las señales del módulo lector hacia el usuario.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La FIG. 1A es una vista esquemática de un usuario que se aproxima a una puerta que utiliza una primera realización de un sistema de control de acceso.

Las FIG. 1B y 1C son una vista esquemática del usuario de la FIG. 1A que abre la puerta que utiliza el sistema de control de acceso.

La FIG. 2A es una vista delantera de un mecanismo de cierre de puerta con un sensor capaciflexivo y un lector de huella dactilar utilizado con el sistema de control de acceso.

La FIG. 2B es una vista de despiece del sensor capaciflexivo de la FIG. 2A.

La FIG. 2C es un circuito que emplea el sensor capaciflexivo de la FIG. 2A.

La FIG. 3A es una vista esquemática de un usuario que se aproxima a una puerta que utiliza otra realización de un sistema de control de acceso.

La FIG. 3B es una vista esquemática del usuario de la FIG. 3A que intenta acceder a la puerta que utiliza el sistema de control de acceso de la FIG. 3A.

La FIG. 4A es un diagrama de flujo de un método usado para determinar si un usuario puede acceder al espacio controlado.

La FIG. 4B es un diagrama de flujo de otra realización del sistema de control de acceso que permite al usuario acceder al espacio de control.

DESCRIPCIÓN DETALLADA

La presente solicitud se refiere a un sistema que permite a un usuario acceder de manera sin discontinuidad a un espacio controlado. En particular, las realizaciones del sistema descrito permiten al usuario obtener acceso a o desde el espacio controlado sin tener que alcanzar y presentar una credencial a un lector. El sistema está configurado para reducir el consumo de potencia y extender la vida de la batería utilizando dispositivos, circuitos y algoritmos que averiguan la intención del usuario antes o después de detectar y autenticar una o más credenciales que se pueden transportar por o son biométricas al usuario. El sistema también se pueda adaptar para detectar y autenticar credenciales así como determinar la intención del usuario en un área predefinida adyacente al punto de entrada a o punto de salida del espacio controlado. De esta manera, los usuarios autorizados casuales que meramente pasan por la entrada/salida no serán detectados, evitando por ello la entrada a o salida no autorizada del espacio controlado. Estos y otros rasgos permiten al sistema reducir el consumo de potencia, mejorar la comodidad del usuario y mejorar la seguridad del sistema.

Las FIG. 1A a 1C ilustran un usuario 10 que se aproxima y que abre una puerta 12 equipado con un sistema de control de acceso 14A. El sistema de control de acceso 14A incluye una credencial 16A, un dispositivo de detección 18A, un controlador 20 y un sensor 22A dispuesto dentro o adyacente a una manilla 24 de un mecanismo de cierre 26. El dispositivo de detección 18A produce un patrón de haz o patrón de señal 28 que se centra en una región adyacente a la puerta 12. En otras realizaciones, el sistema de control 14A incluye sistemas en los que el dispositivo lector 18A y el controlador 20 están integrados en la cerradura 26 y/o sistemas en los que el sensor 22A es parte del dispositivo lector 18A.

Tras la aproximación de un usuario autorizado 10 adyacente a la puerta 12, el sistema de control de acceso 14A permite al usuario 10 entrar en o salir de un espacio controlado sin discontinuidad sin tener que presentar la credencial 16A al dispositivo de detección 18A. En particular, cuando la credencial 16A se lleva a una posición adyacente al dispositivo de detección 18A en un intento del usuario 10 de entrar o salir de la puerta 12, la credencial 16A y el dispositivo de detección 18A están configurados para enviar y recibir señales que se procesan por el controlador 20 para autenticar al usuario 10 y desbloquear el mecanismos de cierre 26 para conceder al usuario 10 acceso al espacio controlado a través de la puerta 12. El sistema de control de acceso 14A opera sin discontinuidad debido a que el controlador 20 es sensible a un intento del usuario (que se determina por el sensor 22A) y el dispositivo de detección 18A para tomar una decisión de acceso (para permitir o denegar al usuario 10 entrar al espacio controlado) dentro de un periodo de tiempo corto que es menor que el periodo de tiempo que tendría el usuario 10 para alcanzar, agarrar y girar la manilla 24. En la mayoría de las realizaciones, el periodo de tiempo entre la detección del intento del usuario, la autenticación y la decisión de acceso es menor de alrededor de 100 milisegundos.

En una realización, la autenticación ocurre después de que el usuario 10 expresa la intención del usuario de entrar/salir del espacio controlado a través de la puerta 12. En esta realización, el intento del usuario se detecta por uno o más sensores 22A que están adaptados para detectar la presencia de la mano del usuario 10 adyacente a la manilla 24. En la realización ilustrada en las FIG. 1A a 1C, el sensor 22A está dispuesto adyacente a la manilla 24 en el mecanismo de cierre 26. El sensor 22A se puede configurar para detectar o bien el contacto (toque) entre el usuario 10 y la manilla 24 o bien la presencia de la mano del usuario 10 dentro de alrededor de 10 centímetros de la manilla 24. En la FIG. 1B, los datos detectados con respecto a la presencia del usuario 10 (indicativa de la intención del usuario) se envía al controlador 20 que entonces activa el dispositivo de detección 18A desde un modo de potencia reducida para producir el patrón de señal 28 en la región adyacente a la puerta 12. Si el dispositivo de detección 18A detecta la presencia de la credencial 16A dentro de esta región, el controlador 20 entonces realiza el proceso de autenticación para tomar la decisión de acceso para o bien conceder o bien denegar al usuario 10 la entrada a o salida del espacio controlado. Como se muestra en la FIG. 1B, la determinación de la intención del usuario, el proceso de autenticación (y el desbloqueo del mecanismo de cierre 26) ocurre tan rápidamente que son completamente anteriores a un intento por el usuario 10 de girar la manilla 24 o tirar de la puerta 12 abierta. De esta manera, el controlador 20 es sensible tanto al dispositivo de detección 18A como al sensor 22A para tomar la decisión de acceso anterior a un intento (ilustrado en la FIG. 1C) por el usuario de entrar o salir del espacio controlado. La capacidad del sistema de control de acceso 14A permite al usuario 10 entrar o salir del espacio controlado sin tener que presentar la credencial 16A al dispositivo de detección 18A.

Como se ilustra en la FIG. 1A, el usuario 10 está ampliamente definido y puede incluir un activo tal como un ordenador portátil, cartera, maletín, teléfono celular, carpeta de archivos o cualquier otro equipo usado en un ambiente de trabajo o de ocio. De manera similar, la credencial 16A puede ser cualquier dispositivo capaz de recibir y/o transmitir señales electromagnéticas o podría ser una credencial biométrica tal como la cara (para detección facial), voz, retina o huella dactilar de una persona. Ejemplos de dispositivos capaces de recibir y/o transmitir señales electromagnéticas incluyen: dispositivos de mano, teléfonos celulares, teléfonos inalámbricos, auriculares,

dispositivos de comunicación de muñeca, tarjetas de crédito, ordenadores personales o buscapersonas. Alternativamente, la credencial 16A podría ser distinta del activo y se podría unir virtualmente a cualquier artículo incluyendo la ropa de una persona.

En la realización mostrada en las FIG. 1A a 1C, la credencial 16A comprende un distintivo de alta o ultra alta radiofrecuencia (RF) que tiene un transmisor de RF que está configurado para enviar y recibir señales de radiofrecuencia de campo lejano. La credencial 16A también tiene un microprocesador y otro medio de procesamiento de señal que la permite procesar y enviar y recibir señales de datos. En otras realizaciones, la credencial puede soportar otros medios de autenticación, por ejemplo podría actuar como un lector de huella dactilar. Para minimizar el consumo de potencia del sistema de control de acceso 14A, el distintivo de RF mostrado es una credencial pasiva que se alimenta y que tiene su contenido de memoria leído y/o escrito cuando se sitúa adyacente al dispositivo de detección 18A.

En la realización ilustrada en las FIG. 1A a 1C, el dispositivo de detección 18A comprende un módulo lector de RF con un transceptor y un conjunto de antena. La antena puede comprender una antena de tamaño mini disponible comercialmente para uso en la banda de UHF (902-928). Una antena tal se vende al por menor por Snyder Antenna Systems, Inc de Altadena, California como la referencia ANT-UHF-4x4-CP. La antena ANT-UHF-4x4-CP está polarizada circularmente y se especifica con una ganancia de 6 decibelios circular isotrópica (dBiC).

El módulo lector transmite y recibe radiofrecuencias de campo lejano para detectar la credencial 16A. La antena dentro del módulo lector se puede diseñar para producir el patrón de señal 28 que se enfoca en una forma predefinida tal como la forma cónica ilustrada. Este patrón de señal u orientación de haz se puede consumar por métodos conocidos tales como una disposición de antenas en fase, múltiples antenas de haz o conmutando elementos de antena. El patrón de señal cónico 28 permite la detección de la credencial 16A dentro de alrededor de 1 metro del módulo lector montado adyacente a la puerta 12. Enfocando el patrón de señal 28 a una región predeterminada adyacente a la puerta 12, se minimiza el uso de energía y los usuarios 10 con credenciales casuales que meramente pasan por la puerta 12 a una distancia no se detectarán. En otras realizaciones, el dispositivo de detección 18A puede alojar el controlador 20 y/o un segundo dispositivo de detección tal como un lector de huella dactilar o teclado. Aún en otra realización, la manilla 20 puede alojar un segundo dispositivo de detección tal como un lector de huella dactilar o de geometría de la mano. Aunque no se ilustra en la realización mostrada, el dispositivo de detección 18A también se puede configurar para alojar uno o más sensores tales como el sensor 22A para identificar la intención del usuario.

El controlador 20 se configura para comunicar tanto con el dispositivo de detección 18A como con el sensor 22A y accionar los componentes del mecanismo de cierre 26. El controlador 20 es sensible tanto al dispositivo de detección 18A como al sensor 22A para tomar la decisión de acceso que puede desbloquear el mecanismo de cierre 26 anterior a un intento (ilustrado en la FIG. 1C) por el usuario de entrar o salir del espacio controlado. El controlador 20 puede comprender, por ejemplo, un microprocesador, un microcontrolador o cualquier hardware capaz de procesar señales de entrada, tomando una decisión de acceso y controlando el mecanismo de cierre 26 y otros componentes. El controlador 20 se puede integrar con tecnología de sistemas de información para hacer el seguimiento del movimiento del usuario 10, incluyendo el movimiento de los activos mencionados anteriormente, en todo un lugar de trabajo, compañía u organización.

Las FIG. 2A a 2C ilustran una realización del sensor 22A y un segundo dispositivo de detección. La FIG. 2A muestra el sensor 22A como un sensor capaciflexivo 30 que está montado en o sobre el mecanismo de cierre 26 adyacente a la manilla 24. Un segundo dispositivo de detección se ilustra como un lector de huella dactilar de conformación 31 integrado en la manilla 24. La FIG. 2B muestra una vista de despiece del sensor capaciflexivo 30 que incluye elementos conductivos 32A, 32B, 32C y 32D, aisladores 34A y 34B, placa de protección 36 y placa de tierra 38. En la FIG. 2C, el sensor capaciflexivo 30 está integrado en un circuito sensor 40 que incluye el resistor 42 y amplificador operacional 44.

El sensor 22A puede comprender o bien un sensor táctil capacitivo o bien capaciflexivo 30 tal como el ilustrado en las FIG. 2A a 2C. El sensor capaciflexivo 30 es capaz de detectar la presencia de un objeto a una distancia del mismo. Los sensores “táctiles” capacitivos requieren contacto físico a fin de detectar la presencia de un objeto. Tales sensores son bien conocidos en la técnica y se pueden utilizar en el sistema de control de acceso 14A (FIG. 1A-1C). El sistema de control de acceso 14A también puede utilizar un sensor capaciflexivo 30 que permite que un objeto tal como una mano sea detectado a una distancia predeterminada X alejada del sensor. Los sensores capaciflexivos tales como el sensor 30 son conocidos en la técnica. Ejemplos de sensores capaciflexivos capaces de ser usados en sistemas de control de acceso se pueden encontrar en la Solicitud de Patente de Estados Unidos 6.825.752 de Nahata et al., la Publicación de Solicitud de Patente de Estados Unidos 2007/0281614 de Oliver et al. y la Publicación de Solicitud de Patente de Estados Unidos 2008/0024312 de Richter.

Las FIG. 2A a 2C ilustran un sensor capaciflexivo 30 ejemplar. El sensor capaciflexivo 30 está montado adyacente al mecanismo de cierre 26 cerca de la manilla 24 en la FIG. 2A. En otras realizaciones, el sensor capaciflexivo 30 se puede disponer dentro de la manilla 24 o un pomo de puerta o adyacente a la puerta 12 (FIG. 1A a 1C).

La FIG. 2B muestra una vista de despiece del sensor capaciflexivo 30. En la FIG. 2B, el sensor capaciflexivo 30 tiene cuatro elementos conductivos detectores 32A, 32B, 32C y 32D. Cada elemento 32A, 32B, 32C y 32D comprende un sensor que forma una porción exterior del sensor capaciflexivo 20. Los elementos conductivos 32A, 32B, 32C y 32D se disponen en una porción exterior del sensor capaciflexivo 30 para hacer de interfaz con la manilla 24. Los elementos conductivos 32A, 32B, 32C y 32D se construyen de materiales conductivos tales como metal o materiales compuestos de metal/polímero. Los elementos 32A, 32B, 32C y 32D están aislados eléctricamente unos de otros para crear cuarto señales discretas que se sacan al controlador 20 (FIG. 1A a 1C). Los elementos conductivos 32A, 32B, 32C y 32D se cargan para crear una diferencia de voltaje entre ellos y la placa de tierra 38. Los aisladores 34A y 34B que comprenden un material dieléctrico, tal como un polímero, aire u otro material aislante, se disponen entre los elementos conductivos 32A, 32B, 32C y 32D y la placa de protección 36 y entre la placa de protección 36 y la placa de tierra 38, respectivamente. La placa de protección 36 comprende una capa apantallada activamente colocada entre los aisladores 34A y 34B. La placa de protección 36 es un conductor que tiene un voltaje alrededor del mismo que el voltaje de los elementos conductivos 32A, 32B, 32C y 32D. Debido a esta realización, la placa protectora 36 hace al campo eléctrico generado por el diferencial de voltaje extenderse desde los elementos conductivos 32A, 32B, 32C y 32D, alrededor de la placa de protección 36, en última instancia a la placa de tierra 38. Los objetos en este campo eléctrico (tales como una mano humana que alcanza la manilla 24 ilustrada en la FIG. 1B) cambiarán el campo, causando un cambio en la constante dieléctrica y la capacitancia, que se lee como la presencia del objeto.

La FIG. 2C ilustra el sensor capaciflexivo 30 integrado en el circuito detector 40. El sensor capaciflexivo 30 está conectado al resistor 42 y el amplificador operacional 44. El amplificador operacional 44 es parte del circuito detector 40 para mantener alrededor del mismo voltaje entre un elemento 32A, 32B, 32C y 32D y la placa de protección 36 cuando un objeto no está presente dentro del alcance de detección del sensor capaciflexivo 30. Juntos el sensor capaciflexivo 30 y el resistor 42 forman un circuito RC con una frecuencia de 1/RC. La frecuencia 1/RC cambia con el cambio en la capacitancia que es causada por un objeto dentro del alcance de detección. El amplificador operacional 44 saca una señal, que tiene una frecuencia relacionada con 1/RC que se comunica al controlador 20. En la realización mostrada, cuatro señales de cuatro circuitos 40 serían sacadas al controlador 20 como cuatro canales. El controlador 20 compara las frecuencias detectadas de los circuitos 40 con una frecuencia umbral predeterminada. En particular, el software cuenta el número de ondas cada unidad de tiempo y compara las frecuencias detectadas con la frecuencia umbral predeterminada. Cuando la frecuencia detectada desde uno o más canales se mueve por debajo de la frecuencia umbral predeterminada, el controlador 20 responde activando el dispositivo de detección 18A o tomando la decisión de acceso que puede desbloquear el mecanismo de cierre 26 anterior a un intento (ilustrado en la FIG. 1C) por el usuario de entrar o salir del espacio controlado. La frecuencia umbral predeterminada se puede fijar en software y, de ahí, se puede cambiar para hacer el alcance de detección ajustable desde un valor máximo a un valor mínimo que puede ser un toque por la mano del usuario 10. Una vez que se detecta la presencia del usuario 10 y se procesa, el controlador 20 puede activar el dispositivo de detección 18A o puede accionar el dispositivo de detección 18A para detectar la credencial 16A para autenticación y entonces tomar la decisión de acceso.

La FIG. 3A muestra al usuario 10 aproximándose a la puerta 12 que utiliza otra realización de un sistema de control de acceso 14B. La FIG. 3B muestra al usuario 10 accediendo a la puerta 12 que utiliza el sistema de control de acceso 14B. Además de la primera credencial 16A y el primer dispositivo de detección 18A, la realización del sistema de control de acceso 14B incluye una segunda credencial 16B (incluye identidad biométrica tal como la cara del usuario 10), un segundo dispositivo de detección 18B, un sensor 22B, un primer patrón de señal 28A, un segundo patrón de señal 28B, una primera región de detección 46A y una segunda región de detección 46B.

En el sistema de control de acceso 14B, el sensor 22B comprende un sensor de infrarrojos pasivo (PIR) que es capaz de detectar la presencia del usuario 10 adyacente a la puerta 12. El sensor 22B pasa la información de detección al controlador 20. El controlador 20 es sensible a la información de detección del sensor PIR 22B para activar y dirigir el primer dispositivo de detección 18A, que comprende el módulo lector de RF que saca una señal de RF, hacia el usuario 10 para leer la primera credencial 16A. La dirección u orientación de la señal de RF se puede consumar usando métodos conocidos en la técnica tales como una disposición de antenas en fase, múltiples antenas de haz o conmutando elementos de antena. Cuando el sensor de PIR 22B detecta la aproximación del usuario en la primera región de detección 46A, la antena de RF saca el primer patrón de señal 28A dirigido en la misma dirección general que la primera región de detección 46A hacia el usuario 10 para leer la credencial 16A. De esta manera, se reduce el consumo de energía del módulo lector de RF. Adicionalmente, la precisión de las comunicaciones entre el módulo lector de RF y la credencial 16A se mejora en la medida que las señales de RF están más centradas, transfiriendo por ello más energía a la credencial 16A. El controlador 20 también está adaptado para dirigir al receptor de RF para hacer el seguimiento con el movimiento del usuario 10 (a medida que se detecta por el sensor de PIR 22B) una vez que la presencia del usuario 10 se ha detectado adyacente a la puerta 12. Por ejemplo, a medida que el usuario 10 se mueve a otra posición, ilustrada en la FIG. 3B, el usuario 10 entra en la segunda región de detección 46B y el controlador 20 dirige al módulo lector de RF para producir el segundo patrón de señal 28B que se dirige hacia el usuario 10 para leer la credencial 16A. Esta configuración mejora la sensibilidad del camino de retorno permitiendo al módulo lector de RF recibir mejor las señales desde la credencial 16A.

El sensor de PIR 22B es de construcción convencional y se adapta para recibir y medir luz de infrarrojos que se radia desde objetos en su campo de vista. Los sensores de PIR son conocidos en la técnica y se usan comúnmente como detectores de movimiento. Los sensores de PIR emplean comúnmente un circuito integrado de sensor piroeléctrico que puede sacar una señal al controlador 20, que se configura para interpretar la señal de salida. El sensor de PIR 22B puede emplear lentes tales como una lente de Fresnel o espejos tales como espejos parabólicos segmentados para enfocar la recepción de infrarrojos a regiones tales como la primera región de detección 46A y la segunda región de detección 46B. La primera y segunda regiones de detección 46A y 46B se extienden adyacentes a la puerta 12 como se ilustra en la FIG. 3. El sistema de control de acceso 14B puede incluir una pluralidad de regiones de detección además de la primera región de detección 46A y la segunda región de detección 46B. Una vez que la presencia del usuario 10 (indicativa de la intención del usuario) se detecta adyacente a la puerta 12 por el sensor de PIR, el sistema de control de acceso 14B autentica al usuario como se trató previamente salvo por la adición del segundo dispositivo de detección 18B y la segunda credencial 16B.

Para completar la autenticación y permitir al usuario 10 acceder al espacio controlado, el segundo dispositivo de detección 18B debe detectar la segunda credencial 16B. En la realización ilustrada en la FIG. 3, la segunda credencial 16B comprende la cara del usuario 10. De esta manera, la segunda credencial 16B es una credencial biométrica. El segundo dispositivo de detección 18B es una cámara de video configurada para capturar imágenes del usuario 10 y en particular la cara del usuario 10, a medida que el usuario 10 se aproxima a la puerta 12. La cámara de video saca una señal al controlador 20, que está configurado con software de reconocimiento facial para interpretar la señal de salida y averiguar si el usuario 10 está autorizado o no para acceder al espacio controlado. La autenticación de la segunda credencial 16B puede ocurrir en cualquier orden con respecto a la detección/autenticación de la primera credencial 16B y la detección por el sensor 22B. Por ejemplo, aproximando a la puerta 12 la cara del usuario 10 se puede reconocer como autorizada por el controlador 20 que ejecuta el software de reconocimiento facial. De esta manera, aproximando meramente a la puerta 12 o llegando dentro del alcance de la cámara, el usuario 10 completa un paso del proceso de autenticación. La autenticación facial puede ocurrir antes de que se detecte al usuario 10 por el sensor de PIR y antes de que el primer dispositivo de detección 18A (en este caso el lector de RF) detecte la primera credencial 16A. No obstante, la autenticación y detección de la intención del usuario debería ocurrir anterior a un intento por el usuario de girar la manilla y tirar de la puerta abierta para hacer el proceso de entrada sin discontinuidad para el usuario 10. De esta manera, el controlador 20 es sensible a ambos dispositivos de detección 18A y 18B y el sensor 22B para tomar la decisión de acceso anterior a un intento por el usuario de entrar o salir del espacio controlado.

La FIG. 4A muestra un diagrama de flujo de un método 100A usado para determinar si el usuario puede acceder al espacio controlado. El método 100A comienza en el bloque 102 y pasa al bloque de estado 104. En el bloque de estado 104, el primer sensor está en un modo de baja potencia, generalmente entre el 1 y el 10 por ciento del ciclo de trabajo. El mecanismo de cierre está en un estado bloqueado de operación que no permite el acceso a o desde el espacio controlado. Desde el bloque de estado 104, el método 100A se mueve al bloque de consulta 106. El bloque de consulta 106 determina si el usuario está presente utilizando uno o más sensores. La presencia del usuario detectada es indicativa de la intención del usuario de acceder al espacio controlado. Criterios indicativos de la presencia o uso además del mismo se pueden usar en el bloque de consulta 106 para averiguar si el usuario ha expresado suficiente claramente la intención de entrar al espacio controlado. Los criterios indicativos pueden incluir: un tiempo que gasta el usuario intentando acceder al espacio controlado, un movimiento o serie de movimientos del usuario que se detectan por el sensor, el número de frecuencias que caen por debajo de la frecuencia predeterminada que se trató previamente con respecto al sensor capaciflexivo mostrado en las FIG. 2A a 2C, un contacto o alcance entre el sensor y el usuario, una dirección o ángulo o aproximación hacia el sensor por el usuario, una identidad del usuario (tal como rasgos de identificación biológicos como la cara o huella dactilar del usuario), la aplicación del sistema se utiliza en o el nivel de seguridad del sistema se fija para, una ubicación del sensor dentro de una estructura tal como un edificio o una vibración causada por el usuario. Si se determina un intento del usuario suficiente para entrar al espacio controlado, el método 100A pasa desde el bloque de consulta 106 al bloque de estado 108. En el bloque de estado 108, el segundo sensor está activo y comienza a detectar. De manera similar, el detector está activo y comienza a detectar. En otras realizaciones sin segundo sensor, solamente está activo el detector o está activa una pluralidad de detectores en el bloque de estado 108. Desde el bloque de estado 108 el método 100A se mueve al bloque de consulta 110. El bloque de consulta 110 determina si ha trascurrido más de un periodo de tiempo predeterminado desde que el método 100A entró en el bloque de estado 108. En una realización este periodo de tiempo es de alrededor de 10 segundos. Si aún no ha trascurrido el periodo de tiempo predeterminado, el método 100A permanece en el bloque de estado 108. Si se ha excedido el tiempo predeterminado, el método 100A pasa al bloque de consulta 112. El bloque de consulta 112 averigua si han ocurrido menos de un número predeterminado de intentos para acceder al espacio controlado desde que se activó el sensor o detector. En una realización, el número predeterminado de intentos es tres. En otras realizaciones, el bloque de consulta 112 puede averiguar si está ocurriendo una vibración excesiva para bloquear el mecanismo. Similar a exceder el número predeterminado de intentos para acceder al espacio controlado, una vibración excesiva puede ser determinante de un intento malicioso para poder entrar al espacio controlado. En el método 100A mostrado en la FIG. 4A, si ocurre más del número predeterminado de intentos para acceder al espacio de control, el método 100A se mueve al bloque de estado 114. El bloque de estado 114 comprende un modo de nivel de seguridad aumentada. En este modo, la potencia para el(los) sensor(es) o detector(es) se puede reducir sustancialmente o eliminar a la de un modo de apagado. Desde el bloque de estado 114 el método 100A pasa al bloque de consulta 116 que averigua

si ha trascurrido menos de un tiempo predeterminado desde que el método 100A entró al bloque de estado 114. Si ha trascurrido menos del tiempo predeterminado, el método 100A permanece en al modo de apagado. Si ha trascurrido más del tiempo predeterminado, el método 100A pasa desde el bloque de consulta 116 al bloque de estado 104.

Si han ocurrido menos del número predeterminado de intentos para acceder al espacio controlado, método 100A se mueve desde el bloque de consulta 112 al bloque de consulta 118. El bloque de consulta 118 averigua si se detecta la presencia del usuario con el segundo sensor, activado en el bloque de estado 108. Alternativamente, el bloque de consulta 118 puede averiguar si se detecta una primera credencial por el primer detector. Si no se detecta la presencia del usuario, el método 100A pasa desde el bloque de consulta 118 de vuelta al bloque de estado 104. Si se detecta la presencia del usuario, el método 100A pasa al bloque de consulta 120 que averigua si se detecta una credencial por el primer detector o en algunos casos si se detecta una segunda credencial por un segundo detector. Desde el bloque de consulta 120, el método 100A se mueve al bloque de estado 122, que comprende un estado desbloqueado. En el estado desbloqueado, el usuario puede acceder libremente al espacio de control a través de la puerta o portal similar. El bloque de consulta 124 determina si ha trascurrido menos de un periodo de tiempo predeterminado desde que el método 100A entró en el bloque de estado 122. En una realización, el periodo de tiempo predeterminado comprende alrededor de 5 segundos. Una vez que ha trascurrido el periodo de tiempo predeterminado, el método 100A se mueve al bloque 126 que devuelve el método al bloque 102.

La FIG. 4B muestra un método alternativo 100B usado para determinar si el usuario puede acceder al espacio controlado. El método 100B es idéntico al método 100A con la excepción de que se ha añadido el bloque de consulta 105. El bloque de consulta 105 determina si está presente la primera credencial. En una realización, esta credencial es la cara del usuario para propósitos de reconocimiento facial. El método 100B entonces pasa al bloque de consulta 106, que determina la intención del usuario en base a detectar la presencia del usuario con uno o más sensores. Si se detecta la presencia del usuario, el método 100B pasa desde el bloque de consulta 106 al bloque de estado 108. En el bloque de estado 108, un segundo sensor o un segundo detector (o ambos) se activan y comienzan a detectar. El método 100B continúa avanzando de una manera similar que la del método 100A.

Aunque la presente invención se ha descrito con referencia a las realizaciones preferidas, los expertos en la técnica reconocerán que se pueden hacer cambios en la forma y detalle sin apartarse del alcance de la invención que se define por las siguientes reivindicaciones.

REIVINDICACIONES

1. Un sistema (14A) para proporcionar acceso a o desde un espacio controlado, que comprende:

una credencial (16A) que envía y recibe señales y está configurada para ser usada o transportada por un usuario (10);

un módulo lector (18A) que envía y recibe señales para detectar la credencial (16A);

un sensor de infrarrojos pasivo (22A) adaptado para detectar la presencia del usuario (10) adyacente a una entrada a o salida del espacio controlado; y

un controlador (20) sensible tanto al sensor de infrarrojos pasivo (22A) como al módulo lector (18A) para tomar una decisión de acceso anterior a un intento por el usuario (10) de entrar o salir del espacio controlado,

caracterizado por que: el controlador es sensible al sensor de infrarrojos pasivo (22A) para dirigir las señales del módulo lector (18A) hacia el usuario (10).

2. El sistema (14A) de la reivindicación 1 y que además comprende un segundo sensor (22B) adaptado para detectar la presencia de un usuario (10) adyacente a una entrada a o salida del espacio controlado o una segunda credencial (16B) capaz de ser detectada por un segundo dispositivo (18B).

3. El sistema (14A) de la reivindicación 1, en donde la credencial (16A) es una tarjeta de radiofrecuencia que envía y recibe señales y está configurada para ser usada o transportada por el usuario (10) del sistema.

4. El sistema (14A) de la reivindicación 3, en donde la credencial (16A) comprende una credencial biométrica o una credencial pasiva.

5. El sistema (14A) de la reivindicación 3, en donde el módulo lector (18A) comprende un módulo lector de radiofrecuencia que envía y recibe señales para detectar la credencial (16A).

FIG. 1A

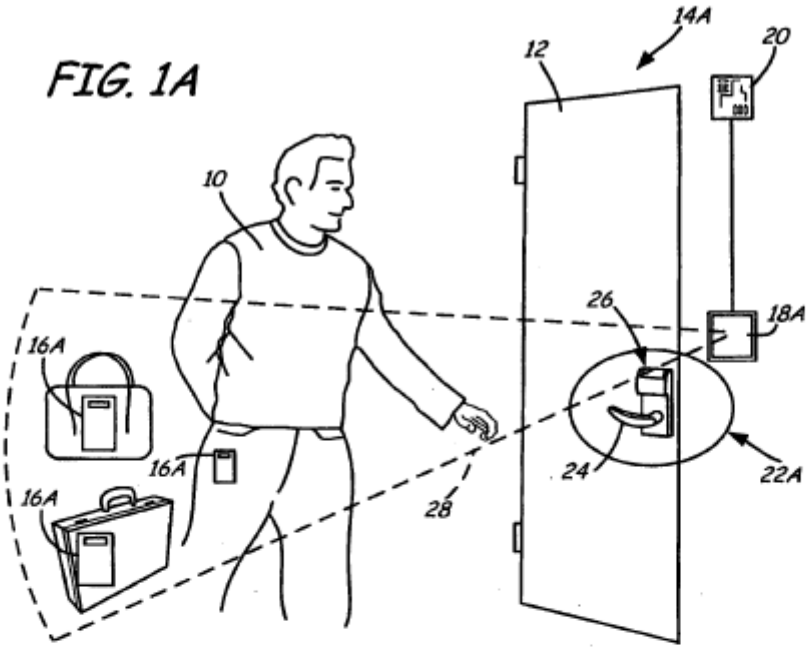
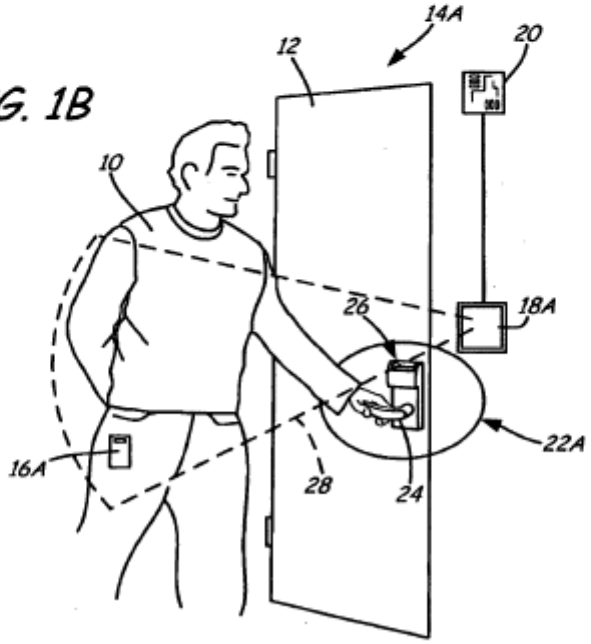

14A
12
20
10
26
18A
16A
16A
16A
24
22A
28

FIG. 1B


14A
12
20
10
26
18A
22A
16A
28
24

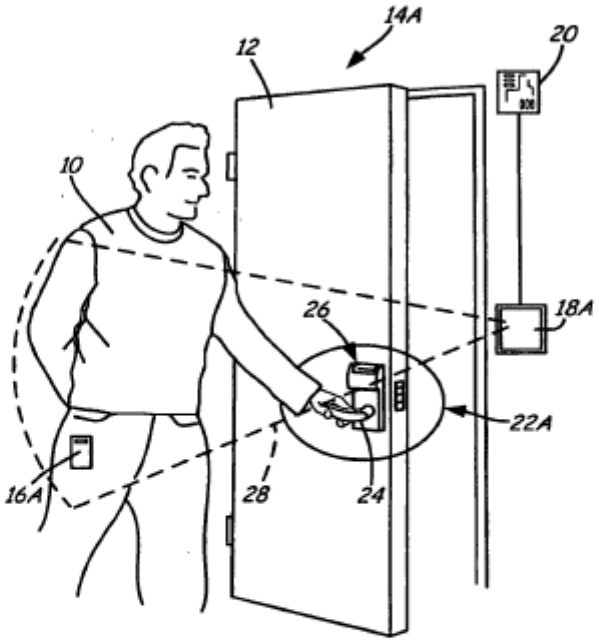


FIG. 1C

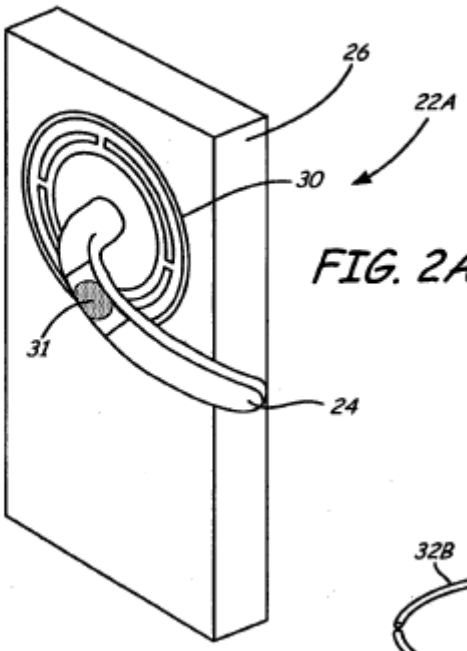
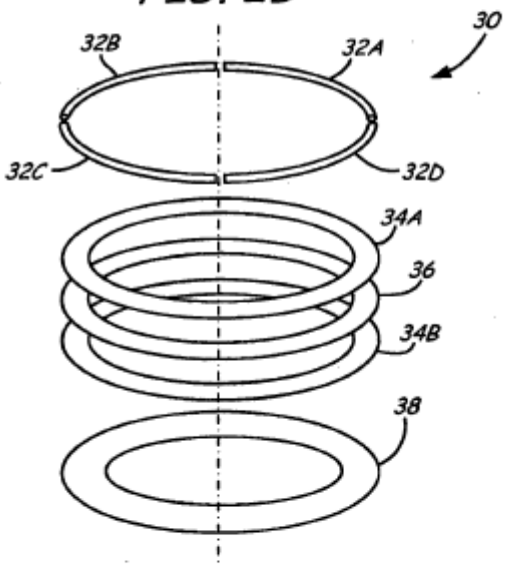


FIG. 2A

FIG. 2B



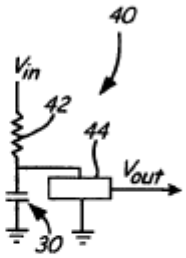


FIG. 2C

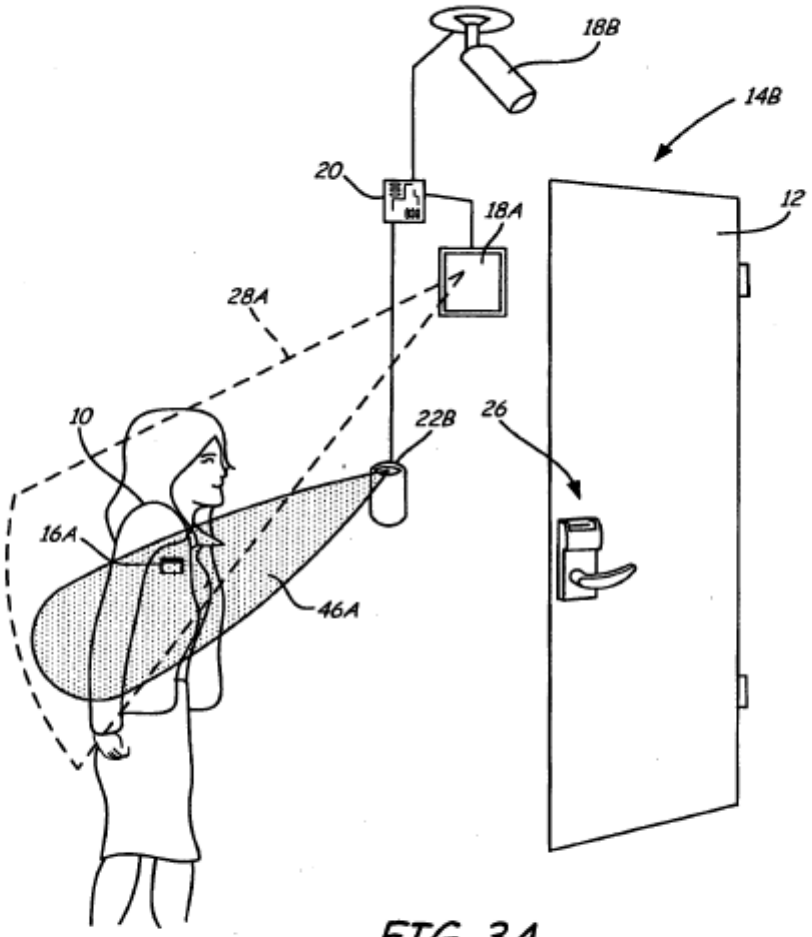


FIG. 3A

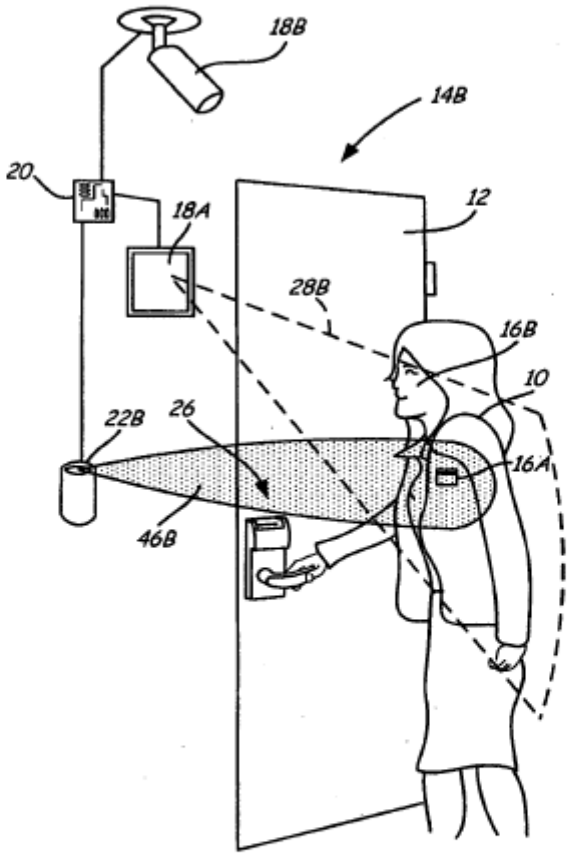


FIG. 3B

FIG. 4A

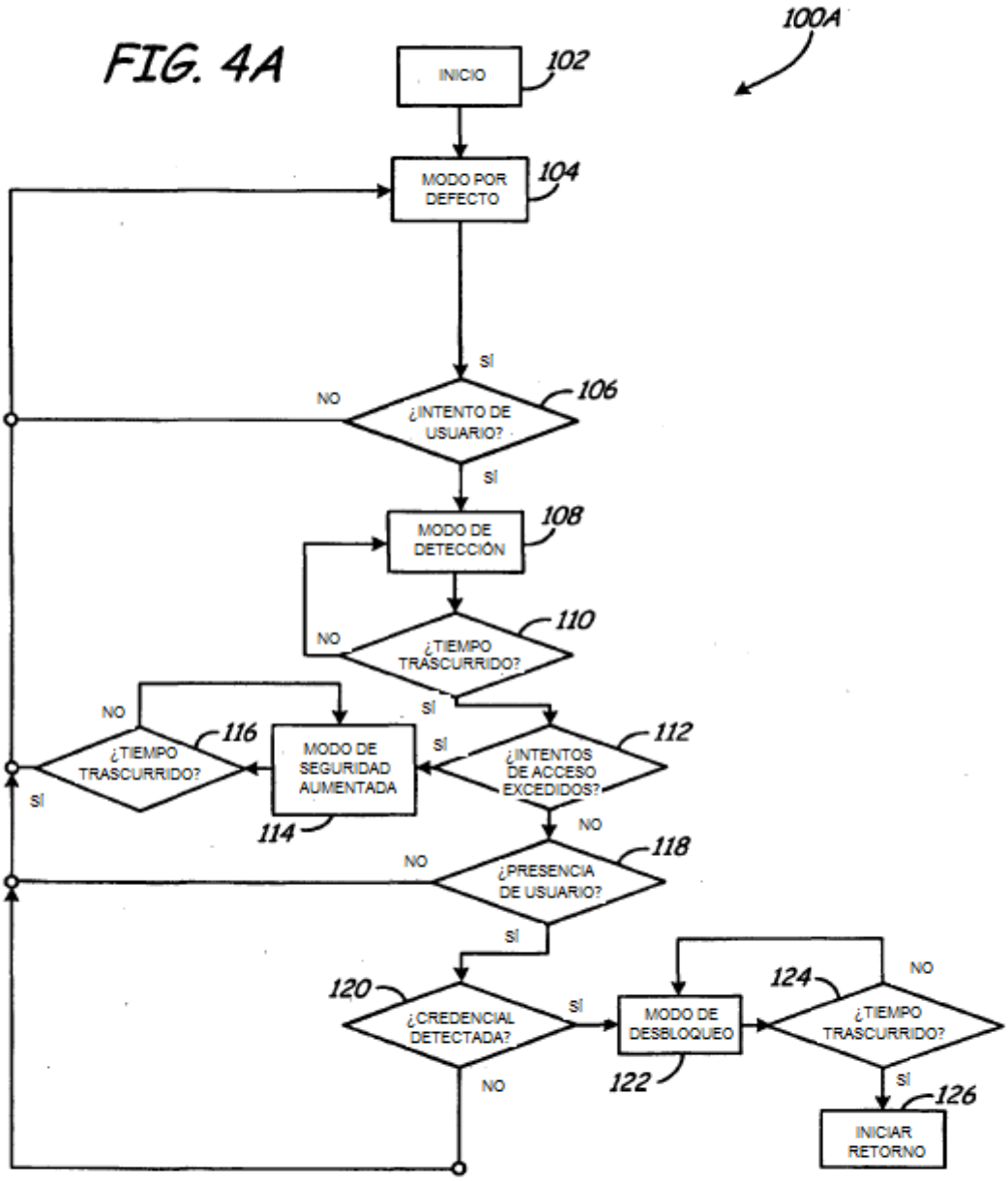
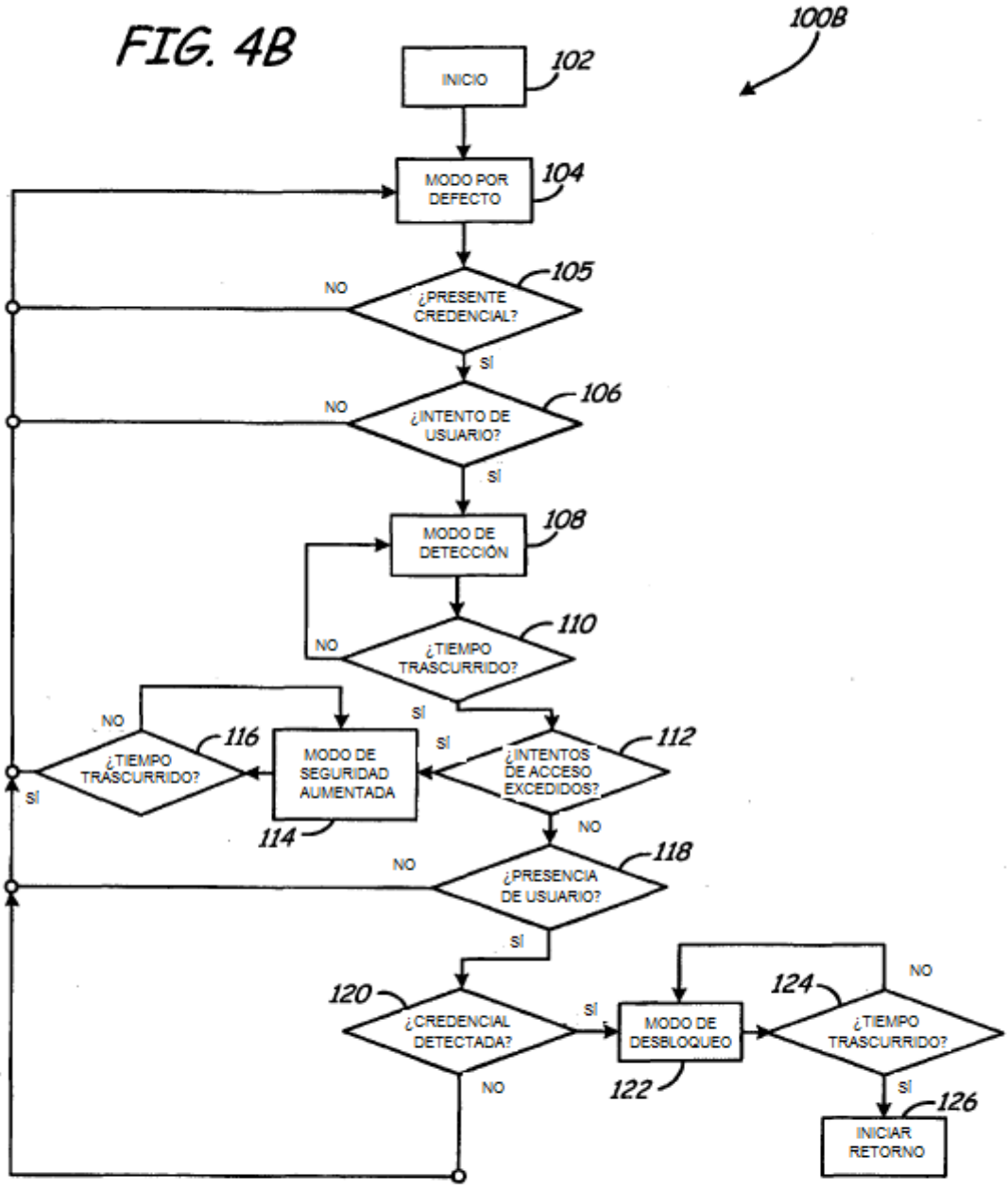

100A
INICIO
102
MODO POR DEFECTO
104
SÍ
NO
¿INTENTO DE USUARIO?
106
SÍ
MODO DE DETECCIÓN
108
NO
¿TIEMPO TRASCURRIDO?
110
SÍ
NO
¿TIEMPO TRASCURRIDO?
116
MODO DE SEGURIDAD AUMENTADA
114
SÍ
¿INTENTOS DE ACCESO EXCEDIDOS?
112
SÍ
NO
NO
¿PRESENCIA DE USUARIO?
118
SÍ
120
¿CREDENCIAL DETECTADA?
SÍ
NO
MODO DE DESBLOQUEO
122
124
NO
¿TIEMPO TRASCURRIDO?
SÍ
126
INICIAR RETORNO

FIG. 4B


100B
INICIO
102
MODO POR DEFECTO
104
¿PRESENTE CREDENCIAL?
105
NO
SÍ
¿INTENTO DE USUARIO?
106
NO
SÍ
MODO DE DETECCIÓN
108
¿TIEMPO TRASCURRIDO?
110
NO
SÍ
¿INTENTOS DE ACCESO EXCEDIDOS?
112
SÍ
MODO DE SEGURIDAD AUMENTADA
114
¿TIEMPO TRASCURRIDO?
116
NO
SÍ
NO
¿PRESENCIA DE USUARIO?
118
NO
SÍ
¿CREDENCIAL DETECTADA?
120
SÍ
NO
MODO DE DESBLOQUEO
122
¿TIEMPO TRASCURRIDO?
124
NO
SÍ
INICIAR RETORNO
126