(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 564 787**

(51) Int. CI.:

G03H 1/04 (2006.01)
G03H 1/22 (2006.01)
G03H 1/18 (2006.01)
G11B 23/28 (2006.01)
B42D 25/328 (2014.01)
G03H 1/00 (2006.01)
G02B 5/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.04.2004 E 04759284 (5)**

(97) Fecha y número de publicación de la concesión europea: **09.12.2015 EP 1627261**

(54) Título: **Portadora de información insertada para datos ópticos**

(30) Prioridad:

10.04.2003 US 462566 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.03.2016

(73) Titular/es:

ERICKSON, RONALD R. (33.3%)
215 Berkeley Place
Brooklyn, NY 11217, US;
BOCK, JOEL N. (33.3%) y
SANDLER, ELIEZER D. (33.3%)

(72) Inventor/es:

ERICKSON, RONALD R.;
BOCK, JOEL N. y
SANDLER, ELIEZER D.

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Portadora de información insertada para datos ópticos

Reivindicación de prioridad

Esta solicitud reivindica la prioridad de la Solicitud de Patente de EE.UU. Nº de Serie 60/462.566, presentada el 10 de abril de 2003.

Campo de la invención

La presente invención se refiere a rasgos de seguridad holográficos, de difracción y variables ópticamente, métodos para crear tales rasgos de seguridad y aparatos, sistemas y métodos para verificación de tales rasgos de seguridad. Más específicamente, la presente invención se refiere a rasgos de seguridad variables ópticamente que tienen información de seguridad óptica insertada dentro de los mismos, incluyendo información de seguridad de múltiples capas y múltiples longitudes de onda, métodos para fabricar tales rasgos de seguridad que tienen información de seguridad óptica insertada y dispositivos, sistemas y métodos para lectura o verificación de la información de seguridad óptica insertada en tales rasgos de seguridad. La presente invención también se refiere a rasgos de seguridad que son no desmontables o se autodestruyen tras la retirada.

Antecedentes de la invención

Actualmente, hay una variedad de dispositivos ópticos para añadir un nivel de seguridad a artículos de valor o identificación, incluyendo documentos, moneda, tarjetas de identificación, pasaportes, software de ordenador, carnets de conducir, productos auténticos y tarjetas de crédito, por nombrar sólo unos pocos. Por ejemplo, casi todas las tarjetas de crédito incluyen actualmente un sello holográfico. Lo mismo es cierto para los nuevos Pasaportes de EE.UU., algunos valores de EE.UU., incluyendo el billete de veinte dólares y moneda extranjera, embalaje de software de ordenador y mercancía oficial de la liga mayor de beisbol, los cuales incluyen cada uno alguna forma de sello holográfico o rasgo de seguridad óptico. Debido a la relativa dificultad en el pasado de producir estos tipos de sellos holográficos y rasgos de seguridad ópticos, este rasgo añadido proporcionaba un aumento del nivel de seguridad y añadía un coste y esfuerzo significativo a aquellos que intentaban crear falsificaciones o artículos de imitación.

La Publicación Internacional Nº WO 92/09444 describe un holograma de seguridad que incluye múltiples patrones que parecen estar en diferentes planos (ver la Fig. 8, página 16, líneas 25-27 y 13-17). Un primer patrón que está en un primer plano parece estar en la parte delantera de y ocultando parte de un segundo patrón que está en un segundo plano (ver la Fig. 8, página 16, líneas 25-27 y 20-22).

La Patente Alemana Nº DE 101 06 105 A1 (Patente de EE.UU. Nº 7.126.729) describe un holograma que tiene un primer y segundo patrones de holograma separados físicamente uno de otro, que se pueden reproducir en diferentes planos (ver resumen). El primer patrón de holograma es un código legible por máquina cuya presencia no se puede detectar fácilmente (ver par. 0008) y el segundo patrón de holograma es un patrón que se puede registrar visualmente (ver par. 0009).

El documento FR 2785697 describe un aparato para verificación de información holográfica grabada.

El documento WO 01/95249 A2 describe un sistema de verificación y autenticación de producto que usa información codificada.

Durante los últimos dieciocho años los sellos holográficos se han usado con buenos resultados y poca preocupación. Durante este tiempo, no obstante, la tecnología de fabricación de hologramas ha llegado a ser más sofisticada y a estar más automatizada, dando a aquéllos que buscasen imitar o falsificar estos instrumentos herramientas nuevas y avanzadas para duplicar incluso los sellos holográficos más complejos y rasgos de seguridad ópticos usados en moneda, pasaportes, tarjetas de crédito y otros artículos.

El uso presente de sellos holográficos como rasgo de seguridad se ha visto comprometido por estas nuevas tecnologías de fabricación y algunos de los hologramas de falsificación son incluso de una calidad superior comparada con el artículo legítimo que está siendo fabricado y usado para propósitos de seguridad. Por ejemplo, el popular holograma de pájaro que está en uso en las tarjetas de crédito de la marca Visa® como un rasgo de seguridad, ahora se puede reproducir fácilmente por falsificadores con un mínimo coste. Esto es en parte resultado de la disponibilidad y bajo coste del equipo y tecnología necesarios para preparar las falsificaciones.

Como resultado, los sellos holográficos y rasgos de seguridad ópticos existentes tienen poco efecto disuasorio sobre los falsificadores e imitadores sofisticados. Las compañías de tarjetas de crédito y otras entidades de certificación se han visto forzadas a dar pasos alternativos y usar otros métodos para intentar proporcionar la seguridad y garantía de autenticidad necesarias.

De manera similar, como resultado de la disponibilidad de estas tecnologías de fabricación, el rasgo de holograma insertado en la nueva moneda de EE.UU. se ha visto comprometido conduciendo al éxito de falsificación de tal moneda.

Hay una significativa necesidad de rasgos de seguridad que proporcionen un efecto disuasorio para falsificación e imitación. También hay una necesidad de rasgos de seguridad que sean relativamente baratos comparado con el coste de crear un artículo de falsificación o imitación. También hay una necesidad de rasgos de seguridad que requieran una inversión significativamente mayor para la duplicación o copia no autorizada que el beneficio obtenido o ganancias derivadas del artículo de falsificación o imitación que se crea.

Compendio de la invención

La presente invención resuelve los problemas asociados con los rasgos de seguridad de la técnica anterior añadiendo niveles adicionales de seguridad y/o nuevos rasgos de seguridad que son extremadamente difíciles, caros y no son rentables de reproducir por un falsificador o imitador.

La presente invención enseña un dispositivo, esto es un holograma o sello holográfico de seguridad que proporciona rasgos de seguridad adicionales para propósitos de verificación de autenticidad como se expone en la reivindicación independiente 1 adjunta. Otros aspectos de la invención se exponen en las reivindicaciones dependientes adjuntas. Más específicamente, la presente invención proporciona un holograma o sello holográfico de seguridad que incluye información adicional que no se percibe o identifica fácilmente por un falsificador o un imitador. La información adicional proporcionada en el holograma o sello holográfico de seguridad puede incluir información de múltiples profundidades, información de múltiples imágenes, información fuera de banda, información binaria u otra información codificada adicional o cualquier combinación de estos diversos tipos de información.

La presente invención también enseña métodos de creación y fabricación de los hologramas y sellos holográficos de seguridad de la presente invención como se expone en la reivindicación 3 adjunta y un sistema para leer los hologramas y sellos holográficos de seguridad de la presente invención como se expone en la reivindicación 2 adjunta. Por ejemplo, el adhesivo que se usa para aplicar el sello de seguridad puede entremezclarse con el material al que se aplica creando una huella digital que es detectable usando, entre otras cosas, una longitud de onda de infrarrojos.

La presente invención también enseña un dispositivo, esto es un holograma o sello holográfico de seguridad que proporciona rasgos de seguridad adicionales para propósitos de verificación de autenticidad añadiendo información de identificación, por ejemplo, información relativa al portador, incluyendo entre otras cosas, información biométrica y personal.

Los hologramas de seguridad según la presente invención pueden incluir información óptica adicional, por ejemplo, información que puede funcionar como un dígito de comprobación o una serie de dígitos de comprobación para una serie en serie del objeto que se asegura, tal como, por ejemplo, una tarjeta de crédito o documento, como un repositorio de información seriada o información individualizada que está sometida a confirmación a través de una base de datos externa, como una indicación de tiempo o datos de ubicación con respecto a la creación del sello o el objeto que se asegura o como información adicional para propósitos de seguridad. La información óptica adicional puede estar en forma digital y puede ser legible mediante la presentación de luz de una longitud de onda predeterminada y/o luz a un ángulo predeterminado con respecto a la superficie del sello. La luz puede ser de cualquiera de las dos o tanto de longitudes de onda visibles como no visibles. La información óptica adicional puede proporcionar un valor único o múltiples valores al sistema de detector óptico o una gama de valores al sistema de detector óptico, uno de los cuales es el valor correcto para la ubicación individual en una matriz que se determina por valores de datos independientes puestos a disposición del lector de máquina a partir de otra información proporcionada por uno o más de una base de datos remota, el documento u objeto, un programa insertado e información biométrica u otra de o desde el portador.

Los hologramas de seguridad según la presente invención pueden incluir información de múltiples profundidades. Ésta incluye diferentes grupos de información que se proyectan en diferentes planos tridimensionales y/o diferentes grupos de información que se leen desde diferentes ubicaciones. Se podría diseñar una contraseña codificada en el holograma de seguridad con diferentes piezas del código incluidas en diferentes planos que se proyectan por el holograma de seguridad y/o legibles desde diferentes ubicaciones con respecto a la posición del holograma de seguridad. La división de la contraseña codificada en diferentes planos permite a la contraseña ser incorporada en una matriz, lo cual añade significativamente más niveles de complejidad y hace mucho más difícil de falsificar o imitar. La contraseña codificada puede constar de un único tipo de información o varios tipos de información. Por ejemplo, la información se puede codificar usando, por ejemplo, datos binarios, longitud de onda reflexiva, intensidad de reflexión, ángulo de reflexión o cualquier combinación de los mismos.

La técnica de insertado de información óptica puede usar, por ejemplo, técnicas de estampación actuales mejoradas por la adición de un número de puntos al campo de imagen del holograma que puede contener datos de seguridad o que puede bloquear datos, variando por ello los datos que se leen. Cada uno de los puntos es una ubicación de “dígito” y/o causa la ausencia de un punto de datos y el holograma de seguridad puede tener por encima de 1.000

de tales “dígitos”. Los dígitos particulares a ser usados para identificar un sello particular u objeto seriado se pueden determinar por la información contenida en la base de datos remota, por el objeto, por un programa insertado, la biometría del portador y/o información independiente proporcionada por el portador.

Adicional o alternativamente, cada una de las ubicaciones de “dígito”, partes del holograma de seguridad o el holograma de seguridad entero se pueden fabricar con una condición estructural, por ejemplo, con una parte posterior de lámina frágil, que frustraría la retirada para copiar. Tal proceso de lámina frágil podría reducir la copia proporcionando tras la laminación final un paso de postproducción que podría fracturar la lámina o dañar el holograma, usando un pulso láser, de manera que un dígito o serie de dígitos seleccionados no serían legibles en el objeto o documento finalizado. La selección de dígitos se puede hacer de cualquier forma y haría cada objeto o documento único dentro del sello holográfico. Estos avances harán el proceso de diseño mucho más complejo y harán el coste de imitación muy alto. Por ejemplo, debido a que tendrían que ser adquiridos varios cientos de tarjetas separadas en la misma serie y sometidas a análisis sofisticado antes de que un sello holográfico de imitación pudiera comenzar a ser fabricado para uso en más de una única cuenta. Las ubicaciones de dígitos, partes del holograma de seguridad o el holograma de seguridad entero se pueden fabricar usando un proceso químico de manera que tras la retirada o el intento de retirada del holograma de seguridad una reacción química destruirá o hará ilegible todo o partes del holograma de seguridad o las ubicaciones de dígitos. Este proceso químico puede ser algo, tal como, por ejemplo, un proceso de oxidación o agente oxidante.

Alternativamente, el holograma laminado entero se puede fabricar usando una base de “lámina frágil”. Un patrón de puntos, por ejemplo, agujeros, se escribe entonces en el holograma, por ejemplo, usando pulsos láser, lo cual seriaría el sello individual. Esto se puede conseguir como el último paso del proceso o en cualquier otro punto del proceso de producción del holograma. El sello se puede leer usando un lector que incorpora una matriz de detectores donde el patrón de puntos en el patrón óptico del holograma corresponde a los dígitos de comprobación necesarios para validar la tarjeta o documento individual. Las ubicaciones muestreadas por la matriz de detectores también se pueden controlar por un código predeterminado introducido en el detector usando un número pin o contraseña conocido solamente por el titular de la tarjeta o fuente del documento. Sin tal código el lector no será capaz de leer la información en el holograma y con el código erróneo, el lector leerá la información errónea. Debido a la significativa dificultad de duplicación, una infracción de seguridad o robo de una tarjeta permitirá a un imitador y solamente uno que sea altamente sofisticado y entendido en técnicas holográficas, en el mejor de los casos, un periodo de tiempo limitado de acceso a la cuenta asociada con la tarjeta robada.

Otra opción es imponer defectos de superficie en un patrón estructurado dentro del holograma o sello holográfico de seguridad de manera que se puedan oscurecer ciertos datos, los cuales representarían la información que se modifica para propósitos de efectuar un cambio de código. Esta información se podría leer por detectores colocados en una cualquiera o más de una variedad ubicaciones y la decodificación dependería de la ubicación. El patrón que se crearía sería aleatorio singularmente de manera que el desgaste y otro daño al holograma o sello holográfico de seguridad no sería capaz de replicar realistamente tal patrón.

El holograma o sello holográfico de seguridad también puede incorporar información acerca del portador del artículo. Por ejemplo, el sello incorporado en una tarjeta de identificación, tal como, por ejemplo, un carnet de conducir o pasaporte, podría incluir información digital suficiente para generar una fotografía o vídeo del portador en un visualizador o en una copia impresa. Debido a la dificultad de reproducir el sello incorporando la información digital acerca del portador en el sello, la sustitución de tal información requerirá la reproducción del sello entero incluyendo toda la información codificada. De esta manera, la alteración sustituyendo la información de identificación del portador será mucho más difícil con respecto a la presente invención que la simple sustitución de la fotografía del portador como es posible actualmente con tarjetas de identificación y pasaportes convencionales. Adicional o alternativamente, el holograma o sello holográfico de seguridad puede incluir un código pin o de paso, información biométrica y/u otra información de identificación relativa al portador. Tal información se podría comparar con datos en tiempo real obtenidos desde el portador tras la presentación de la tarjeta de identificación.

En una aplicación de muy alta seguridad, el sistema podría proporcionar un nivel mayor de seguridad añadiendo un elemento de modificación. El sistema tras cada validación de un holograma o sello holográfico de seguridad modificaría inmediatamente después o concurrentemente, el sello holográfico u holograma de seguridad para proporcionar un código de seguridad diferente. El sistema entonces modificaría la base de datos de datos de verificación en consecuencia. Por ejemplo, el patrón de puntos en un holograma de lámina frágil se modificaría tras cada uso de la tarjeta de identificación para cambiar el código de seguridad, usando un láser pulsado, con la base de datos de información de seguridad que se actualiza en consecuencia. Por ejemplo, el láser pulsado podría quemar uno o más puntos o sacar uno o más pedacitos del patrón o se podría usar un dispositivo para cambiar el ángulo de reflexión modificando por ello el patrón y la información contenida dentro del mismo. La base de datos se modificaría en consecuencia para incluir el nuevo patrón o información de manera que tras la siguiente decodificación se podría lograr una coincidencia correcta. Este proceso continuaría durante cada uso hasta que no quede allí ningún elemento modificable adicional en el patrón. Con este tipo de disposición, la tarjeta de seguridad necesitaría sustitución después de un número finito de usos, por ejemplo, mil usos. Este sistema no proporcionaría la existencia de una tarjeta de seguridad duplicada para un individuo dado que se denegaría el acceso a menos que se use la tarjeta modificada. En el caso de que se haga con éxito una falsificación de la tarjeta de seguridad, el falsificador tendría que usar la tarjeta de seguridad falsificada antes de que se use de nuevo la tarjeta de seguridad

real. Si después del punto que se hace la falsificación, se utiliza primero la tarjeta de seguridad real, la tarjeta falsificada se reconocería como está fuera de secuencia y no se permitiría el acceso al portador de la tarjeta falsificada. Si el falsificador utiliza la tarjeta primero entonces se denegará el acceso al sistema al portador de la tarjeta original y puede aconsejar al departamento de seguridad en consecuencia. Tras una detección de una tarjeta de seguridad incorrecta, el sistema puede activar automáticamente una alarma o función de notificación, indicando que se ha intentado un uso no autorizado de la tarjeta de seguridad y que se debería iniciar un bloqueo de seguridad. El sistema puede requerir el uso de la tarjeta de seguridad tanto para la entrada como para la salida, añadiendo por ello un nivel de seguridad mayor. El sistema puede incluir el requisito de un código pin o de paso, información biométrica y/o verificación de información de identificación de portador además de una tarjeta de seguridad.

Debido a que la luz de longitudes de onda de IR y UV tienen necesidades muy diferentes en un holograma laminado "espejo", los sellos holográficos u hologramas de seguridad no necesitan portar una imagen visible al ojo humano, sino que en su lugar pueden incluir una imagen que es no visible, pero que es capaz de ser leída usando detectores de IR y/o UV. La imagen en el sello u holograma de seguridad se genera usando luz IR y/o UV. La lectura de la información insertada se consigue usando una fuente de luz IR y/o UV y la luz reflejada se lee usando un detector o detectores de IR y/o UV. El sello holográfico se puede insertar en cualquier ubicación en la cara de la tarjeta de seguridad. Tal ubicación puede ser la primera serie de seriación de la tarjeta de seguridad. Los dígitos de comprobación en el sello holográfico pueden ser la segunda serie de seriación en la tarjeta de seguridad. La seriación personalizada, única para la tarjeta individual puede ser, por ejemplo, la longitud de onda, respuesta, ubicación o los puntos de dígitos binarios.

Las tarjetas de seguridad se pueden implementar como un sello que tiene información insertada legible por máquina. Estos sellos se pueden usar en conjunto con tarjetas de crédito existentes o seriadas para producir el efecto de un número de serie extendido. La información del sello puede operar en conjunto con la seriación existente. Por ejemplo, el número de cuenta del dígito 15 o 16 en una tarjeta de crédito se aumenta ahora por el número de "Serie" que se incorpora en la tarjeta de crédito (pero no en la Información de la Banda Magnética) para producir un número de cuenta de 18 a 20 dígitos. El sello añadiría dígitos adicionales a la seriación existente para cada cuenta, incluso aunque hubiera un número fijo de dígitos en todos los sellos proporcionados.

Las tarjetas de seguridad se pueden implementar incorporando una función de sustracción de datos. Bajo este método, se incluye en el sello fabricado un número grande de puntos de datos activos. Tras la activación o uso de la tarjeta o documento, se retira un conjunto o conjuntos únicos de puntos de datos (puntos de datos "retirados después") para proporcionar los datos en serie únicos dentro del sello para añadir una capa de seguridad adicional o para individualización de cada sello. Esta información de punto de datos junto con otros datos en serie en la misma u otras modalidades en la tarjeta, documento u otro objeto se pueden introducir en una base de datos maestra para confirmación en tiempo real, casi en tiempo real o retardada.

Alternativamente, la información incluida en el sello puede tener ya una serie de puntos de datos retirados (puntos de datos "retirados insertados"), por ejemplo, con el ángulo de reflexión o refracción variado a partir de los puntos de datos retirados después en cuanto a diferenciar los datos codificados añadidos a un punto posterior en el tiempo a partir de los datos estáticos que son preexistentes en el sello. La diferencia entre los puntos de datos retirados insertados y los puntos de datos retirados después puede proporcionar la información de seguridad de identificación o individualización.

El holograma de seguridad puede incorporar ángulos de reflexión variables en las ubicaciones de dígitos. Cada ubicación de dígito podría incorporar un ángulo de reflexión predeterminado de manera que cada bit del código único se reflejaría en un ángulo particular a ser leído por un detector particular. Cada ubicación de dígito del código único sería capaz de representar más que unos y ceros binarios, pero puede representar cualquier número de dígitos dependiendo del número de detectores usados. Por ejemplo, si se usan cinco detectores o bien ninguno o bien uno cualquiera de los cinco detectores puede detectar un dígito tras la iluminación de las ubicaciones de dígitos. Los cinco detectores, por ejemplo, se pueden situar cada uno en una posición particular con respecto al holograma de seguridad. Tras la iluminación, cada ubicación de dígito individual se reflejaría a una ubicación particular a ser detectada por un detector en la posición correspondiente, proporcionando por ello un número mayor de códigos únicos que utilizan menos ubicaciones de dígitos. Un código de ocho dígitos incorporado en el holograma de seguridad contendría seis veces tanta información como un código binario de ocho dígitos que utiliza un único detector sin diferenciación angular. Tal holograma de seguridad es mucho más difícil de reproducir debido a los ángulos de reflexión específicos y definidos requeridos para los dígitos en el holograma de seguridad para permitir una lectura precisa del código.

Alternativamente o además, se pueden incorporar en el holograma o sello holográfico de seguridad ángulos de datos señuelo que proyectarían información a una ubicación particular pero que no incluiría la información codificada, sino que en su lugar incluiría información señuelo. Esto puede ser además de o en lugar de los puntos de datos señuelo.

El holograma de seguridad también o alternativamente puede utilizar información fuera de banda. Por ejemplo, la señal reflejada puede incluir una longitud de onda pico primaria y una longitud de onda pico secundaria. El sistema según la presente invención puede utilizar el pico secundario como la señal detectada para el propósito de

codificación de la información de identificación o el sistema puede usar cualquier combinación de los picos primario, secundario y cualquier otro para propósitos de codificación de la información de identificación.

El holograma de seguridad puede incluir puntos de datos de múltiples capas que refuerzan la señal de datos solamente en ángulos predeterminados, produciendo por ello diferencias de amplitud en la información presentada al lector sin la necesidad de fabricación altamente precisa del holograma de seguridad.

El lector puede incorporar software que contiene uno o más algoritmos que pueden estar basados en tiempo y ser volátiles y, dependiendo del tiempo (día, semana, mes, hora), puede descifrar la información de seguridad en el sello u holograma de seguridad a un código diferente. Tal código entonces se descifraría en base a uno o más de los algoritmos en el software.

La información de seguridad en el sello u holograma de seguridad se puede estructurar como una matriz tridimensional, por ejemplo, 20x20x20 bit o byte. La información contenida en la matriz tridimensional se puede leer usando una matriz de detectores dispuestos en una configuración tridimensional o en una configuración bidimensional correspondiente o se puede leer usando uno o más grupos de configuraciones bidimensionales o tridimensionales de detectores. El orden en el que se leen los detectores se puede controlar por un primer algoritmo y la información leída por los detectores se puede decodificar usando un segundo algoritmo. Los algoritmos específicos que se usan son no críticos y, de hecho, cualquier algoritmo desde el más simple al más complejo se puede usar para propósitos de leer, codificar y/o decodificar la información de seguridad insertada en el sello u holograma de seguridad. Los detectores se pueden alternar, controlar o disponer para proporcionar una variedad de configuraciones para detección y/o decodificación de información almacenada en el sello u holograma de seguridad y puede ser adaptable a variaciones o cambios en los algoritmos o información de control para propósitos de verificación. Por ejemplo, si ha habido una infracción verificada o supuesta de la base de datos, robo de una tarjeta de seguridad y/o descifrado del algoritmo y/o de los códigos, el sistema se puede poner en el modo de infracción por lo cual se utiliza una nueva matriz para decodificación. Ésta se puede basar en un algoritmo almacenado en una ubicación de seguridad diferente y puede utilizar información alternativa almacenada en el sello u holograma de seguridad, diferentes ángulos o diferentes longitudes de onda de luz, tales como, por ejemplo, información fuera de banda, información de múltiples profundidades y/o información de múltiples imágenes, para propósitos de decodificación y verificación.

En la configuración donde los detectores se sitúan en un único plano, el sello u holograma de seguridad se puede leer linealmente (deslizando) o de forma paralela (insertando). Los detectores se pueden situar en diferentes posiciones en un único plano. Cada detector representa un decimal, de manera que se usaría un único detector donde la información codificada se representa en formato binario, se usarían siete detectores donde la información codificada se representa en formato octal, etc. Cuanto mayor es el número de detectores, mayor es la dificultad de generar y copiar el sello u holograma de seguridad, debido a la criticidad de obtener los ángulos de reflexión correctos de la luz requerida para la lectura adecuada de la información almacenada en el sello u holograma de seguridad.

La información de seguridad o algún otro código o códigos de acceso se puede programar sobre la cinta magnética en una tarjeta de seguridad u otra forma de identificación usando holografía, como se enseña por las Patentes de EE.UU. Nº 4.547.002, 4.597.814, 4.684.871, 5.336.871, 5.634.669 y 6.086.708. La información de seguridad se puede leer deslizando la tarjeta a través del lector de tarjeta. El lector puede incluir detectores para leer la información de seguridad u otro código de acceso que se pueda colocar en un ángulo predeterminado, en un ángulo diferente para cada detector o cualquier combinación de ángulos. Para cada ángulo en el que se dispone un detector, se puede detectar un código diferente. Usando los detectores dispuestos en diferentes ángulos se puede usar un algoritmo para controlar la lectura o procesamiento de información de seguridad, proporcionar un orden particular de detección y/o leer la información detectada en varias secuencias. Esto puede producir un código diferente dependiendo de la hora, día o algún factor temporal.

La información de seguridad se puede procesar en o cerca de la ubicación de verificación del sello u holograma de seguridad, por ejemplo, en el mostrador de pago de la tienda. La información de seguridad también se puede procesar enviando los datos en bruto a una ubicación remota donde se puede decodificar la matriz. La decodificación puede incluir, por ejemplo, utilización de un algoritmo o una comparación con información personal o información biométrica. Una capa o rasgo de seguridad adicional incluye la adición de una segunda capa de información de seguridad, por ejemplo, añadir un número pin que cuando se introduce por el portador fija el algoritmo para propósitos de codificación. Un nuevo número pin se puede lanzar al portador tras la aceptación o terminación de la transacción.

Una base de datos remota o local que contiene información del portador se puede utilizar para propósitos de verificación de la información de seguridad en el sello u holograma de seguridad y puede incluir diversa información, incluyendo, por ejemplo, una imagen del portador, información física o información histórica, tal como, por ejemplo, fecha de nacimiento, lugar de nacimiento, nombre de soltera de la madre, etc.

También se pueden proporcionar diferentes niveles de seguridad en el lado de lectura. Por ejemplo, el lector se puede controlar por software, un código, un dispositivo remoto o alguna otra entrada automática o manual que

determina el algoritmo a aplicar para propósitos de decodificación de la información almacenada en el sello u holograma de seguridad o que controla los detectores o capas de detectores que se activarán o desactivarán para propósitos de lectura de la información contenida en el sello u holograma de seguridad. Se pueden usar diversas combinaciones de estos rasgos de seguridad para propósitos de control de acceso a la información en el sello u holograma de seguridad y para asegurar la lectura adecuada de la información almacenada.

Se pueden implementar niveles de seguridad añadidos. Por ejemplo, un rasgo de seguridad basado en el uso de un transpondedor u otra portadora de información insertada dentro del portador adecuado del sello u holograma de seguridad se puede incluir en el sistema según la presente invención. Esta portadora de información se puede activar tras entrar en la ubicación segura y se puede requerir al portador para salir de tal ubicación. La portadora de información se puede activar por un código o algoritmo específico y, por lo tanto, puede no ser detectable hasta que ocurre tal activación. Tras la salida adecuada de la ubicación segura, la portadora de información se puede desactivar por el mismo o diferente código o algoritmo específico. Alternativamente, la portadora de información puede estar activa continuamente o activar durante periodos de tiempo predeterminados. Por ejemplo, la portadora de información puede estar activa anterior a entrar en la ubicación segura y se puede requerir para propósitos de verificación de la información del portador en el sello u holograma de seguridad. Si la información de portador contenida en la portadora de información coincide con la información de portador en el sello u holograma de seguridad, entonces se pude permitir acceso a la ubicación asegurada.

El transpondedor se puede usar independientemente de una tarjeta de identificación. El transpondedor puede contener un código de identificación que representa al portador que se puede usar para obtener información de identificación acerca del portador desde una base de datos local o remota. La información de identificación se puede usar en conjunto con un sistema de evaluación biométrico y/o mostrar en un dispositivo de visualización para verificación visual. El sistema de evaluación biométrico puede comparar la información de identificación recuperada de la base de datos con información obtenida del portador. El dispositivo de visualización permite una comparación visual a ser hecha entre la información de identificación obtenida de la base de datos y del portador. El transpondedor puede estar en un modo desactivado hasta que reciba una señal de activación desde el transceptor y se puede desactivar de nuevo tras la verificación o en cualquier otro momento.

Breve descripción de los dibujos

La Figura 1 muestra un holograma de seguridad según una primera realización ejemplar de la presente invención.

La Figura 2 muestra una secuencia y ubicación para colocación de puntos de datos en una matriz según una realización ejemplar de la presente invención.

La Figura 3 muestra el holograma de seguridad de la Figura 1 que incluye información adicional acerca del portador según una realización ejemplar de la presente invención.

La Figura 4 muestra el holograma de seguridad de la Figura 1 que incluye información adicional que es legible solamente usando luz ultravioleta según una realización ejemplar de la presente invención.

La Figura 5 muestra un holograma de seguridad que tiene una estructura modificable para variar el código de seguridad después de cada lectura del holograma de seguridad según una realización ejemplar de la presente invención.

La Figura 6 muestra un holograma de seguridad que incluye una imagen que es legible solamente usando una longitud de onda de UV según una realización ejemplar de la presente invención.

La Figura 7 muestra el holograma de seguridad de la Figura 5 implementado utilizando una función de sustracción de datos según una realización ejemplar de la presente invención.

La Figura 8 muestra un holograma de seguridad que utiliza una pluralidad de ángulos de reflexión según una realización ejemplar de la presente invención.

La Figura 9 muestra un diagrama de reflexión del holograma de seguridad de la Figura 8.

La Figura 10 muestra un holograma de seguridad que tiene una condición estructural que frustraría la retirada o manipulación según una realización ejemplar de la presente invención.

La Figura 11 muestra un lector que se usa para leer la información codificada almacenada en un holograma de seguridad según una primera realización ejemplar de la presente invención.

La Figura 12 muestra un lector que se usa para leer la información codificada almacenada en un holograma de seguridad según una segunda realización ejemplar de la presente invención.

La Figura 13 muestra un lector que se usa para leer la información codificada almacenada en un holograma de seguridad según una tercera realización ejemplar de la presente invención.

La Figura 14 muestra un sistema de transpondedor según una primera realización ejemplar de la presente invención.

La Figura 15 muestra un sistema de transpondedor según una segunda realización ejemplar de la presente invención.

Descripción detallada

Como se muestra en la Figura 1, el holograma de seguridad 1 incluye información que cuando se ve o lee para propósitos de verificación, se presenta como una imagen tridimensional 3. La imagen 3 incluye información codificada 5 en un patrón predeterminado. Esta información codificada 5 se dispone en un patrón predeterminado que permitirá niveles de seguridad variables. El patrón predeterminado de la información codificada 5 se dispone como una matriz tridimensional 9. La matriz tridimensional 9 incluye información que abarca tres planos discretos cada uno situado a una distancia predeterminada del plano del holograma de seguridad 1. El primer plano 11 de la matriz tridimensional 9 se sitúa aproximadamente a tres milímetros de la superficie del holograma de seguridad 1. Este primer plano 11 incluye solamente una primera parte 13 de la información codificada 5 almacenada en el holograma de seguridad 1 y solo es insuficiente para establecer una confirmación con éxito de verificación de identidad de autorización de seguridad. El segundo plano 15 se sitúa aproximadamente a seis milímetros de la superficie del holograma de seguridad 1 e incluye solamente una segunda parte 17 de la información codificada 5 almacenada en el holograma de seguridad e incluso junto con la primera parte 15 es insuficiente para establecer una confirmación con éxito de verificación de identidad de autorización de seguridad. El tercer plano 19 se sitúa aproximadamente a nueve milímetros de la superficie del holograma de seguridad 1 e incluye una tercera parte 21 de la información codificada 5, el resto de la información codificada 5 necesaria para establecer una confirmación con éxito de verificación de identidad de autorización de seguridad. No solamente es la información codificada 5 almacenada en tres planos separados de una matriz tridimensional 9, cada uno a una distancia diferente del holograma de seguridad 1, sino que la información almacenada en los tres planos se codifica según un algoritmo único que determina la secuencia según la cual la información se lee en los diversos planos para reproducir la información codificada 5. El algoritmo puede ser el mismo para cada plano o puede ser diferente para uno o más de los planos.

Como se muestra en la Figura 2, se puede conseguir procesar la información codificada usando un algoritmo o algoritmos predeterminados que determinan la secuencia y ubicación de la información a ser colocada en la matriz y el orden en el que se debería leer tal información cuando se intenta una confirmación de la información de seguridad. La matriz usada en este ejemplo es una matriz 12 x 12 x 3 22 y el código de seguridad es una palabra de doce bits 23. En este caso el algoritmo proporciona la colocación de los bits en la matriz como se muestra. El primer bit 24 se sitúa en la posición [3, 1, 1] de la matriz. El segundo bit 25 se sitúa en la posición [6, 6, 1] de la matriz. El tercer bit 26 se sitúa en la posición [9, 11, 2] de la matriz. El cuarto bit 27 se sitúa en la posición [12, 4, 2]. El quinto bit 28 se sitúa en la posición [2, 9, 3] de la matriz. El sexto bit 29 se sitúa en la posición [5, 2, 3] de la matriz. El séptimo bit 30 se sitúa en la posición [8, 7, 3] de la matriz. El octavo bit 31 se sitúa en la posición [11, 12, 3] de la matriz. El noveno bit 32 se sitúa en la posición [1, 5, 1] de la matriz. El décimo bit 33 se sitúa en la posición [4, 10, 2] de la matriz. El undécimo bit 34 se sitúa en la posición [7, 3, 1] de la matriz y el duodécimo bit 35 se sitúa en la posición [10, 8, 2] de la matriz.

Este ejemplo, usa un algoritmo simple donde el primer elemento sigue un patrón de progresión en incrementos de tres dígitos comenzando con la posición tres y dando vueltas a través de doce posiciones y después de cada cuatro progresiones disminuyendo la siguiente progresión a dos dígitos y entonces continuando las siguientes cuatro progresiones en incrementos de tres dígitos. El segundo elemento sigue una progresión continua de incrementos de cinco dígitos dando vueltas a través de doce posiciones. El tercer elemento depende del primer y segundo elemento. Donde la suma del primer elemento y el segundo elemento es un número positivo por debajo de doce, el tercer elemento es un uno. Donde la suma del primer elemento y el segundo elemento es un número positivo por encima de doce, el tercer elemento es un dos. Donde la suma del primer elemento y el segundo elemento es un número negativo, el tercer elemento es un tres.

Como se muestra en la Figura 3, el holograma de seguridad 1 de la Figura 1 incluye información adicional acerca de la emisión, tal como, por ejemplo, una imagen de la emisión 40 y/u otra información de identificación personal. La imagen de la emisión 40 se puede incluir como una imagen holográfica fácilmente visible por un observador bajo condiciones de iluminación natural o legible solamente mediante un lector especial utilizando condiciones de iluminación especializadas. La imagen de la emisión 40 se puede comparar con información de imagen almacenada en una base de datos remota, en o dentro del lector o disponible para un operador. La imagen de la emisión 40 se puede comparar manualmente, electrónicamente, visualmente o por cualquier otro método con la información de la imagen almacenada o disponible acerca de la emisión y/o a una imagen de o el portador real del holograma de seguridad 1. Alternativamente la imagen de la emisión 40 se puede generar como una imagen fotográfica o de vídeo a partir de la información digital almacenada en el holograma de seguridad 1.

La Figura 4 muestra el holograma de seguridad 1 de la Figura 1 que incluye la información digitalizada adicional 44 que es legible solamente usando luz ultravioleta 43 presentada en un ángulo de 45 grados al holograma de seguridad 1. La información digitalizada adicional 44 se puede representar por puntos 46 dispuestos en un patrón, con cada punto 46 que representa un dígito o bit de información. La información digitalizada adicional 44 indica a un

lector la hora y fecha de creación del holograma de seguridad 1. La información digitalizada adicional 44 se puede codificar o insertar en una parte de luz visible del holograma de seguridad 1. La información digitalizada adicional 44 se puede usar como un rasgo de seguridad extra para confirmar la autenticidad del holograma de seguridad 1. La información digitalizada adicional 44 se puede verificar mediante comparación con datos almacenados en una base de datos remota, en o dentro del lector o disponible para un operador.

La Figura 5 muestra un holograma de seguridad que tiene una estructura modificable para variar el código de seguridad después de cada lectura del holograma de seguridad. El holograma de seguridad 50 se fabrica usando un material alterable 52, tal como, por ejemplo, una lámina frágil, que se puede modificar usando un láser pulsado 54. El holograma de seguridad 50 se fabrica con un código de seguridad particular representado por un patrón de puntos 56. Tras un primer uso verificado del holograma de seguridad 50 el sistema de verificación 58 modifica el código de seguridad utilizando el láser pulsado 54 para quemar uno o más puntos adicionales 60 en el patrón de puntos 56. Para cada modificación del código de seguridad, el sistema de verificación actualiza una base de datos con el nuevo código de seguridad para propósitos de la siguiente verificación. Este proceso puede continuar durante un número de usos finito, es decir, 200, de manera que el holograma de seguridad 50 necesitaría ser sustituido cada pocos meses, suponiendo un número de usos por día. En caso de que la tarjeta de identificación que incorpora el holograma de seguridad 50 sea falsificada, si la tarjeta falsificada se utiliza en primer lugar, entonces tras el uso por el portador real, se denegará el acceso y se proporcionará una notificación automática de una infracción de seguridad o se sugerirá tal denegación de acceso del portador real para informar de una infracción de seguridad. Si la tarjeta falsificada se utiliza en segundo lugar, entonces tras tal uso se detectará inmediatamente la falsificación y se podría designar al sistema iniciar una alarma, notificación o condición de seguridad. El sistema de verificación 58 se puede diseñar de manera que la tarjeta de identificación necesita ser presentada tanto tras la entrada como tras la salida. Adicionalmente, el portador se puede dotar con el rasgo de seguridad adicional de un código que se debe introducir tras el uso, información biométrica acerca del portador correcto u otra información que se almacenaría en una base de datos y verificar la identidad del portador.

La Figura 6 muestra un holograma de seguridad que no porta una imagen visible sino que en su lugar porta una imagen que es legible usando una longitud de onda de UV. El holograma de seguridad 70 se crea usando luz UV y el holograma de seguridad 70 se puede situar en cualquier parte de la tarjeta de identificación 72, en el ejemplo mostrado se sitúa en el cuadrante superior izquierdo 73. El holograma de seguridad se puede leer usando una fuente de luz UV 74 en conjunto con un detector de UV 76. La fuente de luz UV 74 se coloca para proyectar luz UV sobre el holograma de seguridad 70 con la luz reflejada desde el holograma de seguridad 70 que se lee por el detector de UV 76. Alternativamente, la tarjeta de identificación 72 puede incluir el holograma de seguridad 70 y uno o más hologramas de seguridad señuelo 78 situados en diferentes posiciones en la tarjeta de identificación 72, con la ubicación del holograma de seguridad 70 que se determina por el código asignado al portador, información biométrica acerca del portador correcto u otra información. El holograma de seguridad 70 se puede generar de manera que la información almacenada en el mismo se pueda leer solamente usando luz reflejada en un ángulo predeterminado o por el detector de UV 76 colocado en un ángulo o distancia particular desde el holograma de seguridad 70.

Como se muestra en la Figura 7, un holograma de seguridad como se describe con respecto a la Figura 5 se puede implementar usando una función de sustracción de datos. En esta realización un gran número de puntos de datos 80 se incorporan en el espacio en blanco del holograma de seguridad 82 usado en la tarjeta de identificación 84. Tras la activación de la tarjeta de identificación 84 un conjunto único de puntos de datos 86 se retiran usando un láser pulsado 88 para proporcionar un código único dentro del espacio en blanco del holograma de seguridad 82. Este código único se puede introducir en una base de datos 90 para verificación de autenticidad o identidad en tiempo real, casi en tiempo real o retardada.

La Figura 8 muestra un holograma de seguridad que utiliza una pluralidad de ángulos de reflexión según otra realización de la presente invención. El holograma de seguridad 100 se genera incorporando ángulos de reflexión variables 104 en las ubicaciones de dígitos. Cada ubicación de dígito 102 incorpora un ángulo de reflexión predeterminado de manera que cada bit del código único se reflejará en un ángulo particular para ser leído por un detector particular 106. Cada ubicación de dígito 102 del código único es capaz de representar más que unos y ceros binarios, sino que puede representar cualquier número de dígitos dependiendo del número de detectores 106. En este ejemplo, hay 5 detectores 106, cada uno en una ubicación particular con respecto al holograma de seguridad 100. Cada ubicación de dígito individual 102 se reflejará a un detector particular 106 proporcionando por ello un gran número de códigos únicos utilizando menos ubicaciones de dígitos. Como se muestra en la Figura 9, tras la iluminación del holograma de seguridad 50 por el haz de luz 109, la primera ubicación de dígito 110 se refleja al primer detector 112. La segunda ubicación de dígito 114 se refleja al quinto detector 116, la tercera ubicación de dígito 118 se refleja al segundo detector 120, la cuarta ubicación de dígito 122 se refleja al primer detector 112, la quinta ubicación de dígito 124 se refleja al cuarto detector 126, la sexta ubicación de dígito 128 se refleja al segundo detector 120, la séptima ubicación de dígito 130 se refleja al tercer detector 132 y la octava ubicación de dígito 134 se refleja al primer detector 112. El código de ocho dígitos incorporado en este holograma de seguridad contendrá seis veces tanta información como un código binario de ocho dígitos que utiliza un único detector sin diferenciación angular y el holograma de seguridad será mucho más difícil de reproducir debido a los ángulos de reflexión específicos y definidos requeridos para los dígitos en el holograma de seguridad para permitir una lectura precisa del código.

En la Figura 10 se muestra un holograma de seguridad que tiene una condición estructural que frustraría la retirada o manipulación. Las ubicaciones de dígitos 140 o ubicaciones donde se almacena información en el holograma de seguridad 142 se fabrican usando una parte posterior de lámina frágil 144. La parte posterior de lámina frágil 144 se diseña de manera que cualquier intento de retirar el holograma de seguridad 142 de la tarjeta de identificación 146 para propósitos de reproducir el holograma destruiría las partes del, si no el holograma de seguridad 142 entero. La parte posterior de lámina de frágil 144 llegaría a ser eficaz para evitar la manipulación con el holograma de seguridad 142 como resultado de un proceso de laminación u otro proceso de postproducción por el cual la parte posterior de lámina frágil se puede insertar parcialmente en o adherir a un adhesivo u otro material. Tras la retirada del holograma de seguridad 142 de la tarjeta de identificación 146 se afectaría a la parte posterior de lámina frágil 144, con partes restantes en el holograma de seguridad 142 y partes restantes en la tarjeta de identificación 146.

En la Figura 11 se muestra un lector que se usa para leer la información codificada almacenada en un holograma de seguridad. El lector 200 incluye un alojamiento 201 que tiene una ranura 202 para inserción de una tarjeta de identificación 204. La ranura 202 permite la inserción de aproximadamente ¾ de la longitud de la tarjeta de identificación 204 en el lector 200. El holograma de seguridad 206 se debería colocar por lo tanto dentro de los límites 208 formados por un borde 210 de la tarjeta que pasa a lo largo de su anchura y que se mueve en una dirección hacia la línea central 212 de la tarjeta, a lo largo. En esta realización, el holograma de seguridad 206 se coloca en el lado derecho de la tarjeta de identificación 204. El lector 200 incluye una fuente de luz 213. El lector 200 también incluye una matriz de detectores 214 colocados dentro del alojamiento 201 y configurados en tres planos x-y que se encuentran paralelos al plano del holograma de seguridad 206 cuando se inserta en la ranura 202. Un primer conjunto de detectores 216 se colocan en un primer plano 218 más cercano al holograma de seguridad 206. Un segundo conjunto de detectores 220 se colocan en un segundo plano 222 en el lado alejado del primer conjunto de detectores 216 con respecto al holograma de seguridad 206 (en la dirección z) y se sitúan en posiciones en el plano que corresponde a las posiciones de detectores desde el primer conjunto de detectores 216, pero ligeramente desplazados en una dirección (x) del primer conjunto de detectores 216. Un tercer conjunto de detectores 224 se colocan en un tercer plano 226 en el lado alejado del segundo conjunto de detectores 220 con respecto al holograma de seguridad 206 (en la dirección z) y se sitúan en posiciones en el plano que corresponde a las posiciones de detectores desde el primer conjunto de detectores 216 y el segundo conjunto de detectores 220, pero ligeramente desplazados en una dirección (x) del segundo conjunto de detectores 220. Alternativamente, el primer conjunto de detectores 216, el segundo conjunto de detectores 220 y el tercer conjunto de detectores 224 cada uno puede constar de una formación de detectores. El primer conjunto de detectores 216, el segundo conjunto de detectores 220 y el tercer conjunto de detectores se acoplan cada uno a un microprocesador 228 y a un decodificador 230. El microprocesador 228 se puede programar para activar ciertos de los detectores dependiendo de la fecha y/u hora. El microprocesador 228 puede procesar la información decodificada desde el decodificador 230 y verificar la autenticidad del holograma de seguridad 206.

Como se muestra en la Figura 12, el lector 200 puede incluir un teclado 232 para entrada por el portador de la tarjeta de un código pin u otra información de verificación. Tal información se puede usar para seleccionar los detectores a ser activados para leer el holograma de seguridad 206 o el algoritmo a ser usado para decodificar la información almacenada en el holograma de seguridad 206. El lector 200 también puede incluir un visualizador 234 para ver la imagen del portador almacenada en el holograma de seguridad 206 o para ver una imagen del portador almacenada en una base de datos local o remota 236. El visualizador 234 también se puede usar para ver y/o comparar la información biométrica del portador con la almacenada en el holograma de seguridad 206 y/o una base de datos local o remota 236.

Alternativamente, como se muestra en la Figura 13, el lector 200 puede incluir una hendidura 240 en lugar de la ranura 202. La hendidura 240 permite al portador deslizar la tarjeta de identificación 243 a lo largo de la hendidura 240 que a su vez permite a los detectores leer la información desde el holograma de seguridad 241. Los detectores se pueden colocar como se describe con respecto a la Figura 11, con el holograma de seguridad que se lee de manera en serie en lugar de en paralelo. Una lectura en serie del holograma de seguridad 241 usando el lector 200 de la Figura 13 puede incluir un punto de destello 242 en una posición aleatoria en el holograma de seguridad 241 que se lee durante un golpe fuerte de la tarjeta de identificación 243 a través de la hendidura 240. En el punto de destello 242 todos los dígitos que corresponden a los detectores a ser activados por la información codificada se leen provocando una activación colectiva de todos los detectores pertinentes. Este punto de destello 242 se puede decodificar por el microprocesador 228 y usar como una verificación adicional de la autenticidad del holograma de seguridad 241.

Como se muestra en la Figura 14, se puede incorporar un nivel de seguridad añadido en el sistema según la presente invención a través del uso de un transpondedor insertado en el portador. Un transpondedor 250 se inserta bajo la piel del portador 252 en la región abdominal 254. El transpondedor 250 no transmite ninguna señal hasta que recibe una señal de activación codificada desde un transceptor 256 en el punto de entrada del área segura tras la exploración de la tarjeta de identificación 262 por un lector 264. Tras recibir la señal de activación el transpondedor 250 comienza emitiendo una señal que coincide con el código en el holograma de seguridad 266 en la tarjeta de identificación 262. Tras la verificación de la información de verificación en el holograma de seguridad 266 o tras la salida del portador 252 de la ubicación segura el código de seguridad en el holograma de seguridad 266 se puede modificar por el lector 264 o un dispositivo de modificación de código independiente y el código de seguridad en el transpondedor 250 se puede modificar por el transceptor 256 o por el dispositivo de modificación de código

independiente. Tras la verificación de la información de identificación en el holograma de seguridad 266 y/o tras la salida del portador 252 de la ubicación segura el transpondedor se puede desactivar por el transceptor 256 o el dispositivo de modificación de código independiente.

El transpondedor 250 se puede usar independientemente de una tarjeta de identificación como se muestra en la Figura 15. El transpondedor 250 puede contener un código de identificación que representa el portador 252. El transceptor 256 repite el código de identificación a una base de datos 270 que contiene información de identificación acerca del portador 252. La información de identificación se puede cargar en un sistema de evaluación biométrico 272 y/o mostrar en un dispositivo de visualización 274 para evaluación visual. El sistema de evaluación biométrico 272 compara la información de identificación recuperada desde la base de datos 270 con información obtenida en tiempo real desde el portador 252. El dispositivo de visualización 274 permite una comparación visual a ser hecha entre la información de identificación obtenida desde la base de datos 270 y el portador 252. El transpondedor 250 puede estar en un modo desactivado hasta que recibe una señal de activación desde el receptor 256 y se puede desactivar de nuevo tras la acreditación del portador 252.

REIVINDICACIONES

1. Un dispositivo para limitar la reproducibilidad de información, que comprende: un sustrato; y un elemento holográfico (1) acoplado al sustrato, el elemento holográfico (1) que incluye un primer conjunto de información óptica (21) percibida tras la iluminación en una primera área plana (19) y un segundo conjunto de información óptica en un patrón codificado de manera que tras la iluminación el patrón codificado se puede percibir en una pluralidad de áreas planas sin hacer el segundo conjunto de información óptica fácilmente identificable por un observador, en donde una primera parte del patrón codificado (17) se percibe tras iluminación en una segunda área plana (15) y una segunda parte del patrón codificado (13) se percibe tras la iluminación en una tercera área plana (11) y en donde la segunda área plana (15) está desplazada de la tercera área plana (11) en una distancia predeterminada y en donde al menos una de la primera parte y la segunda parte del patrón codificado se oscurece de la inspección visual desde un punto de vista predeterminado por el primer conjunto de información óptica (21).

2. Un sistema para autenticación de información, que comprende: un elemento holográfico (1), el elemento holográfico (1) que incluye un primer conjunto de información óptica (21) percibida tras la iluminación en una primera área plana (19) y un segundo conjunto de información óptica en un patrón codificado de manera que tras la iluminación el patrón codificado se puede percibir en una pluralidad de áreas planas sin hacer el segundo conjunto de información óptica fácilmente identificable por el observador, en donde una primera parte del patrón codificado (17) se sitúa en una segunda área plana (15) y una segunda parte del patrón codificado (13) se sitúa en una tercera área plana (11) y en donde la segunda área plana (15) está desplazada de la tercera área plana (11) en una distancia predeterminada y en donde al menos una de la primera parte del patrón codificado (17) y la segunda parte del patrón codificado (13) se oscurece de la inspección visual desde un punto de vista predeterminado por el primer conjunto de información óptica (21); y un lector (201), que incluye una abertura (202), la abertura que define una primera área respecto a la cual el lector puede conseguir una lectura del elemento holográfico que depende de la ubicación del elemento holográfico respecto a la abertura, una fuente de luz (213), un detector colocado en una primera ubicación (214) respecto a la abertura (202) cuando el elemento holográfico se coloca en una segunda ubicación respecto a la abertura (202).

3. Un método para limitar la reproducibilidad de información, que comprende: escribir un primer conjunto de información óptica (21) sobre un elemento holográfico (1), en donde el primer conjunto de información óptica (21) se percibe tras la iluminación en una primera área plana (19); escribir un segundo conjunto de información óptica en un patrón codificado sobre el elemento holográfico (1), en donde el segundo conjunto de información óptica es de manera que tras la iluminación el patrón codificado se puede percibir en una pluralidad de áreas planas sin hacer el segundo conjunto de información óptica fácilmente identificable por el observador y en donde una primera parte del patrón codificado (17) se sitúa en una segunda área plana (15) y una segunda parte del patrón codificado (13) se sitúa en una tercera área plana (11) y en donde la segunda área plana (15) está desplazada de la tercera área plana (11) en una distancia predeterminada; obscurecer al menos una de la primera parte del patrón codificado (17) y la segunda parte del patrón codificado (13) de la inspección visual desde un punto de vista predeterminado por el primer conjunto de información óptica (19).

4. El dispositivo según la reivindicación 1 o sistema según la reivindicación 2 o método según la reivindicación 3, en donde el patrón codificado se basa en uno o más algoritmos.

5. El dispositivo según la reivindicación 1 o sistema según la reivindicación 2 o método según la reivindicación 3, en donde el patrón codificado es un primer patrón codificado y el primer conjunto de información óptica (21) se proporciona en un segundo patrón codificado.

6. El dispositivo según la reivindicación 5 o sistema según la reivindicación 2 o método según la reivindicación 3, en donde el primer patrón codificado y el segundo patrón codificado se basan en algoritmos independientes.

7. El dispositivo según la reivindicación 1 o sistema según la reivindicación 2 o método según la reivindicación 3, en donde el patrón codificado se percibe tras la iluminación a través de inspección visual asistida.

8. El dispositivo según la reivindicación 1 o sistema según la reivindicación 2 o método según la reivindicación 3, en donde una parte del patrón codificado se oscurece parcialmente de la inspección visual desde un punto de vista predeterminado por el primer conjunto de información óptica (21).

9. El dispositivo según la reivindicación 1 o sistema según la reivindicación 2 o método según la reivindicación 3, que además comprende un tercer conjunto de información óptica (40) que incluye el patrón codificado o escribir un tercer conjunto de información óptica en un patrón codificado sobre el elemento holográfico, en donde el tercer conjunto de información óptica (40) se dispersa en una disposición predeterminada entre al menos la primera área plana (19) y la segunda área plana (15).

10. El dispositivo según la reivindicación 1 o sistema según la reivindicación 2 o método según la reivindicación 3, que además comprende un tercer conjunto de información óptica (40) que incluye el patrón codificado o escribir un tercer conjunto de información óptica en un patrón codificado sobre el elemento holográfico, en donde el tercer conjunto de información óptica (40) se dispersa en una disposición predeterminada entre al menos la primera área

plana (19) y la segunda área plana (15) y en donde el tercer conjunto de información óptica (40) incluye además al menos uno de dígitos de comprobación e información de señuelo.

11. El dispositivo según la reivindicación 1 o sistema según la reivindicación 2 o método según la reivindicación 3, en donde la primera área plana (19), la segunda área plana (15) y la tercera área plana (11) se incluyen dentro de una matriz tridimensional y en donde la matriz tridimensional incluye una primera parte del patrón codificado (17) situada dentro de una primera área volumétrica y la segunda parte del patrón codificado (13) situada dentro de una segunda área volumétrica.

12. El sistema según la reivindicación 2, en donde el lector (201) además incluye un microprocesador acoplado a la fuente de luz (213) y el detector y en donde el detector está compuesto de un detector, una pluralidad de detectores o una formación de detectores (214).

13. El sistema según la reivindicación 2, en donde la fuente de luz (213) saca luz visible y luz no visible.

14. El sistema según la reivindicación 2, en donde la fuente de luz (213) es una primera fuente de luz y que además comprende una segunda fuente de luz (43) y en donde la primera fuente de luz y la segunda fuente de luz proporcionan diferentes longitudes de onda de luz.

15. El sistema según la reivindicación 2, que además comprende un segundo detector colocado en una tercera ubicación respecto al elemento holográfico cuando el elemento holográfico está en la primera ubicación.

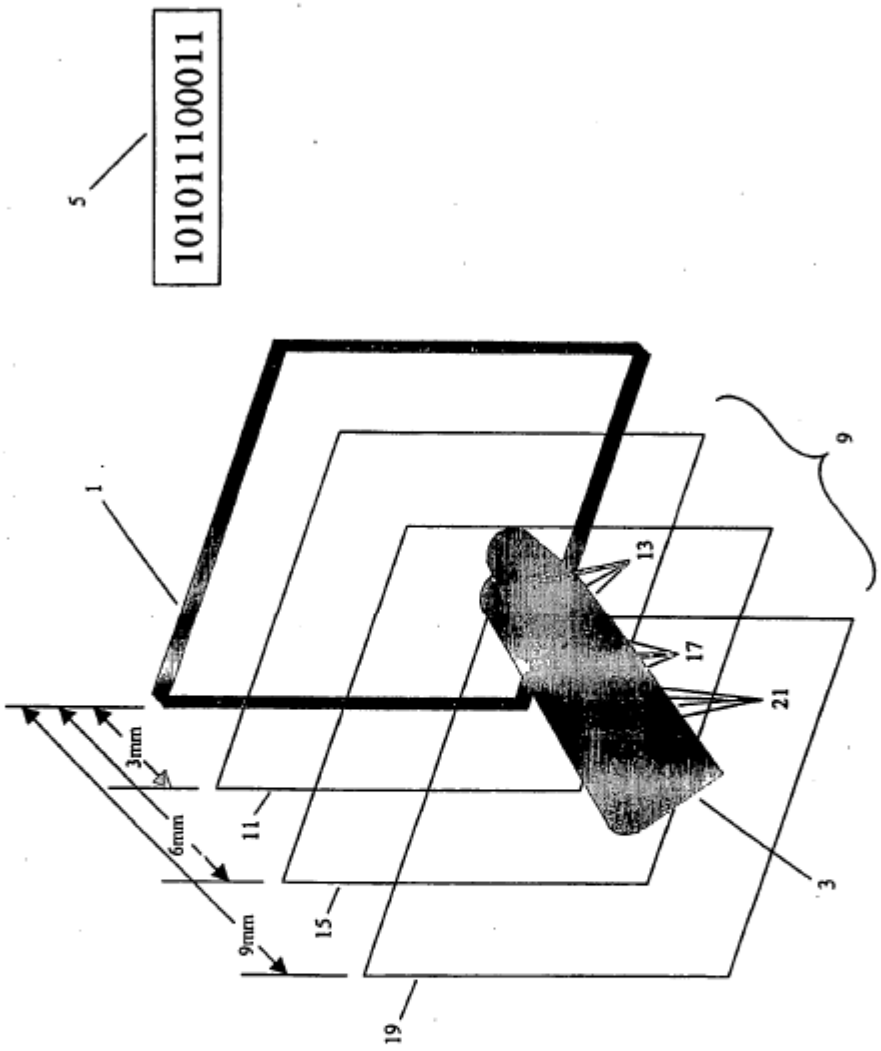

Figura 1

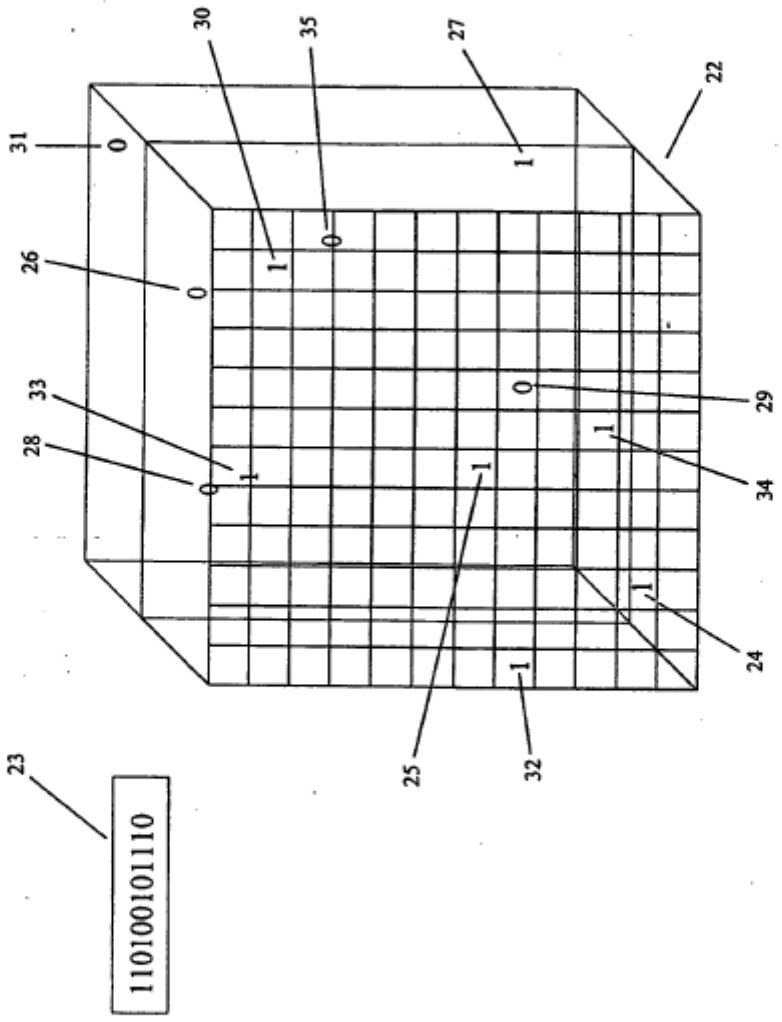
30
35
27
22
31
0
1
0
26
0
1
0
33
0
29
28
0
1
1
34
1
1
24
1
25
32
23
11010010110

Figura 2

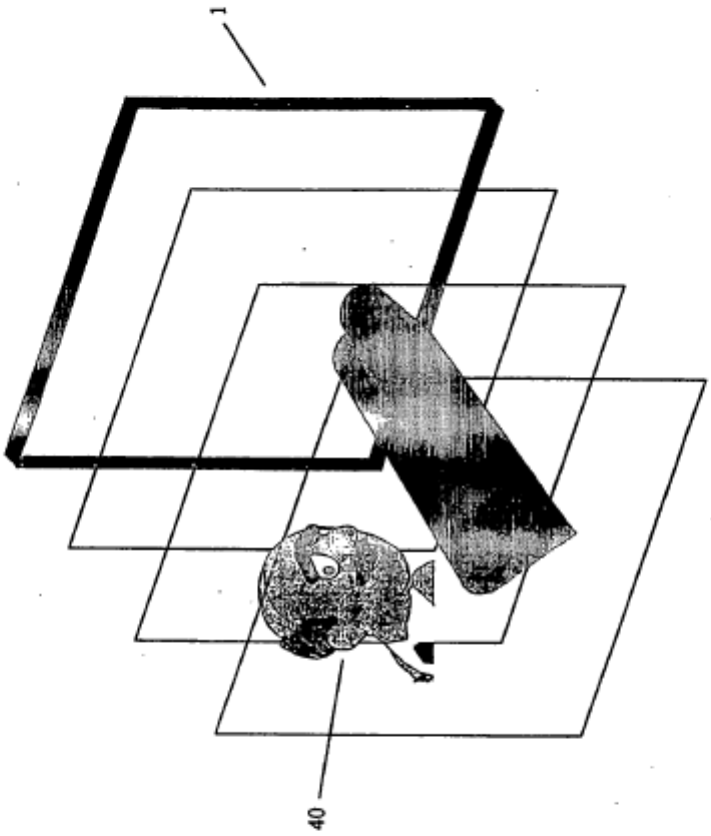

Figura 3

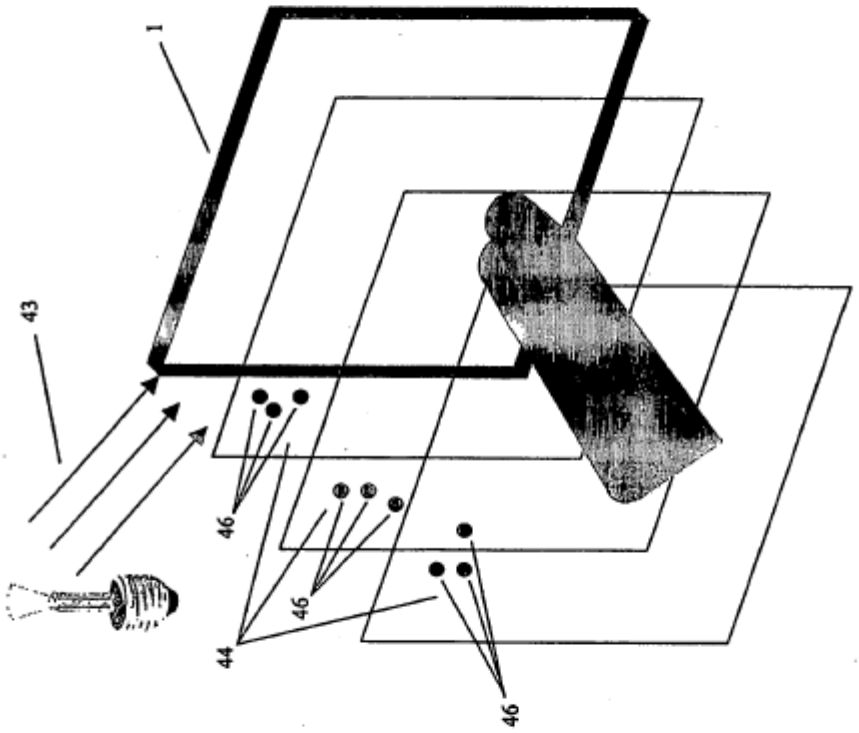

Figura 4

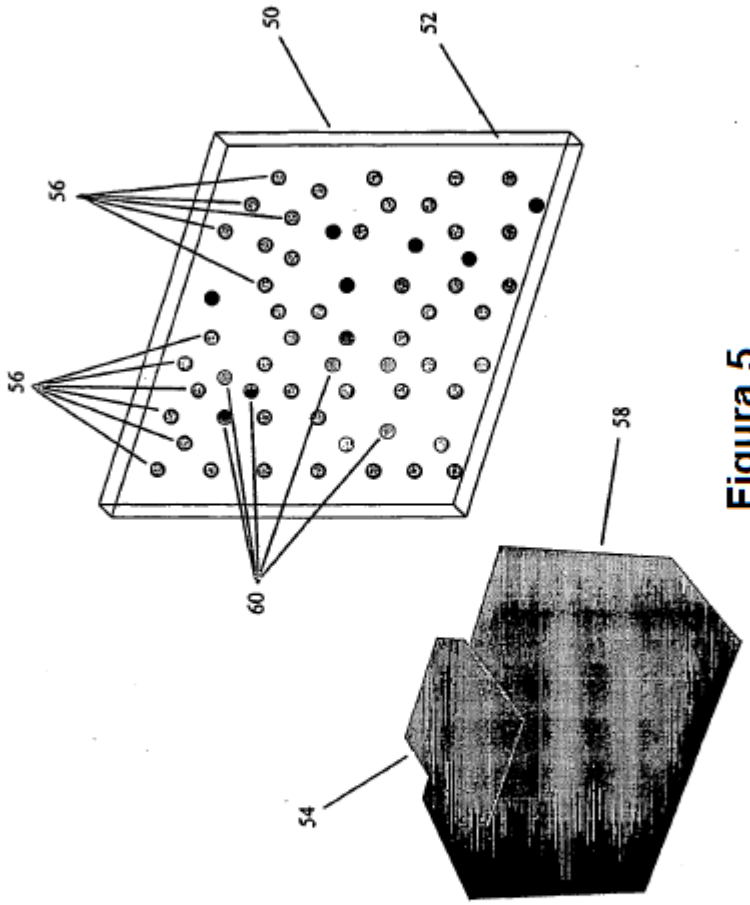

Figura 5

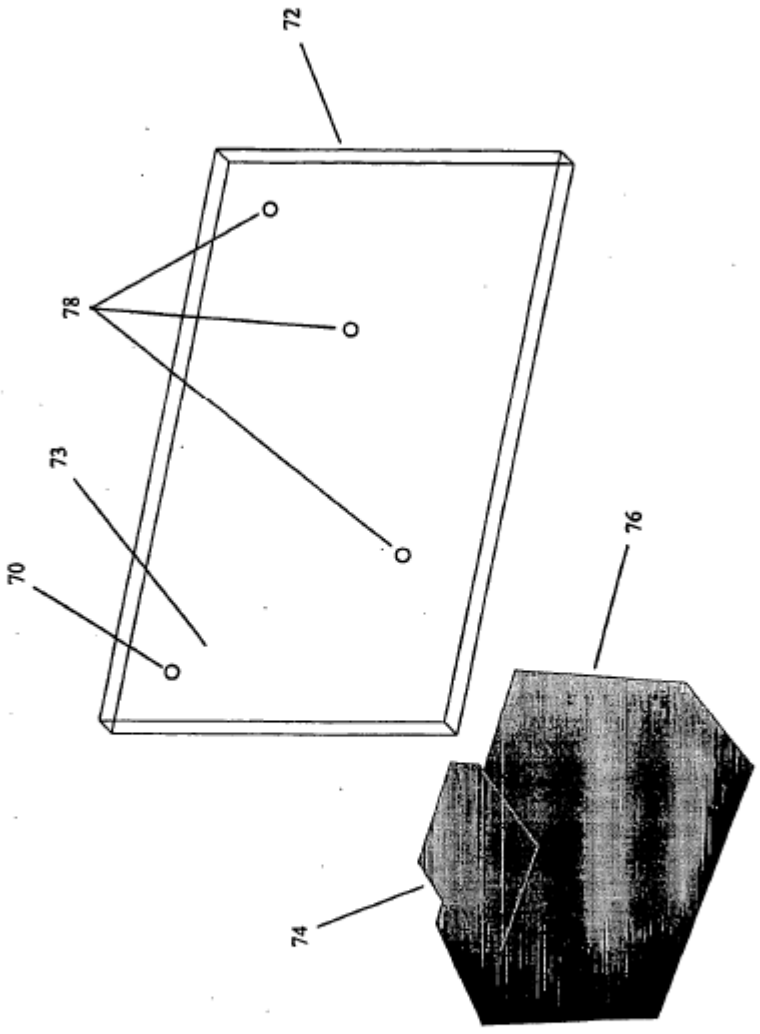

Figura 6

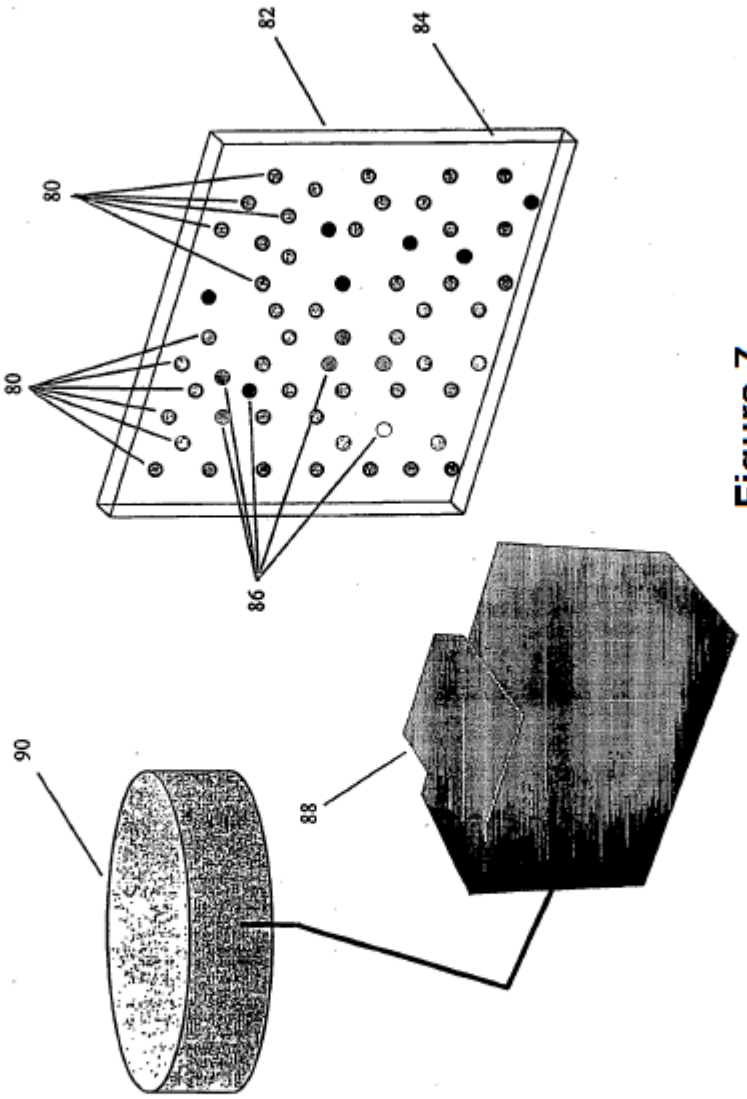

Figura 7

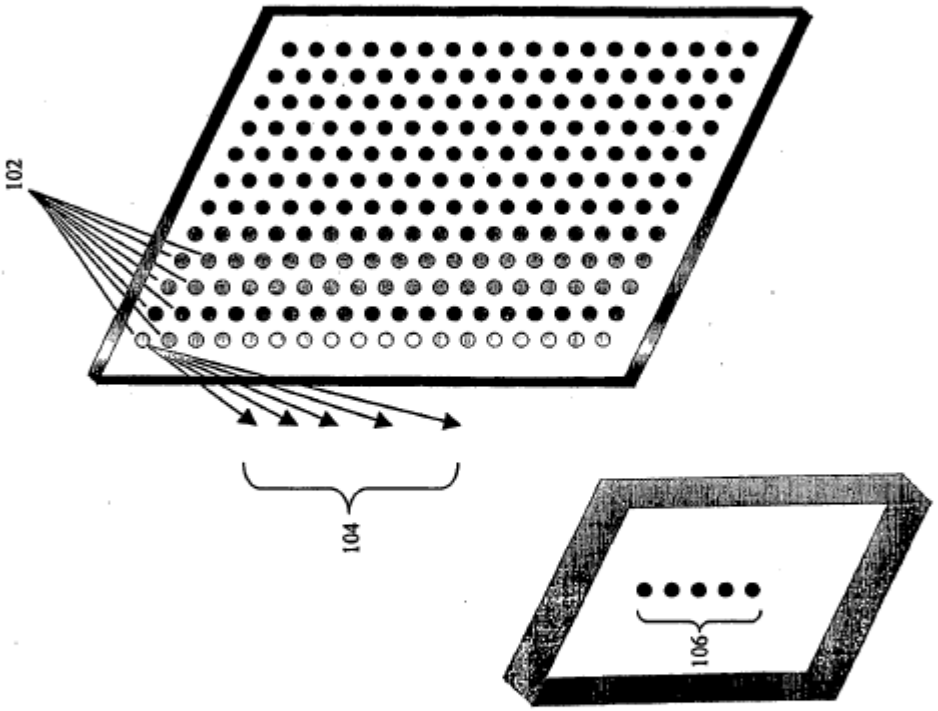

Figura 8

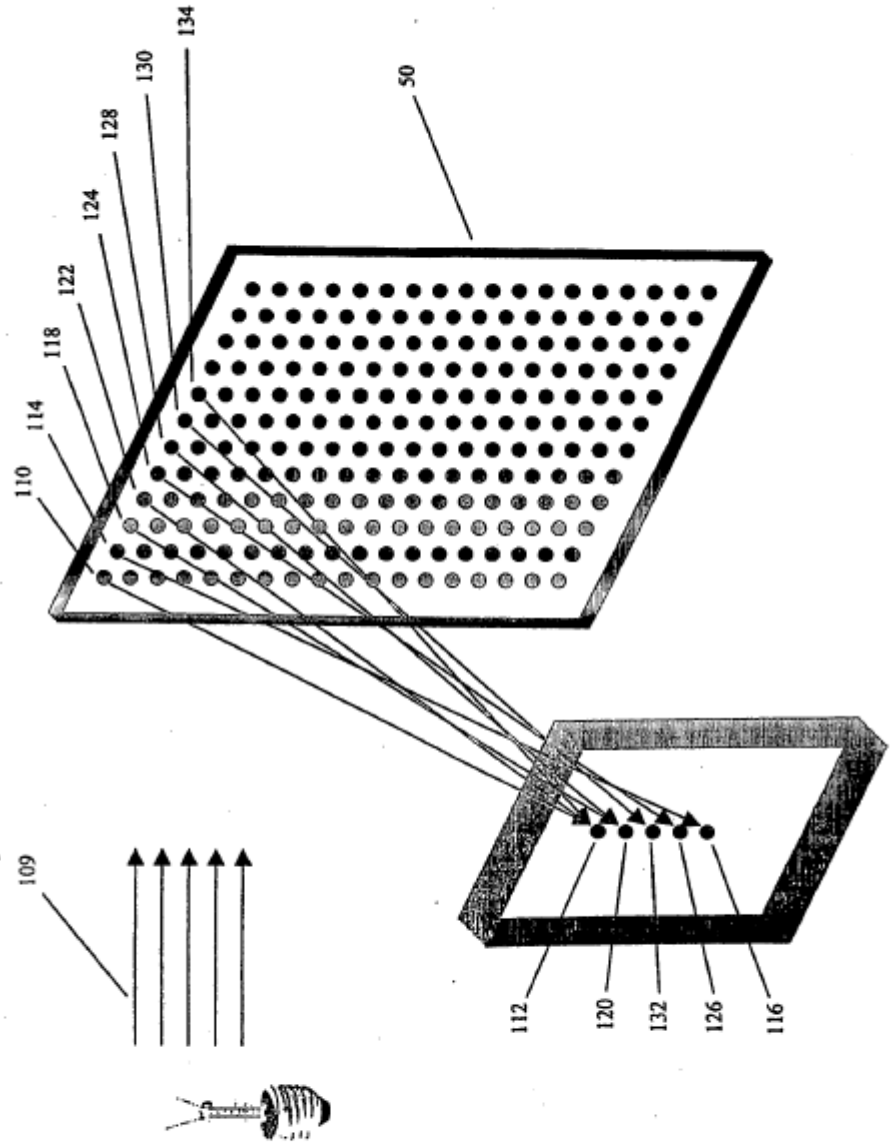

Figura 9

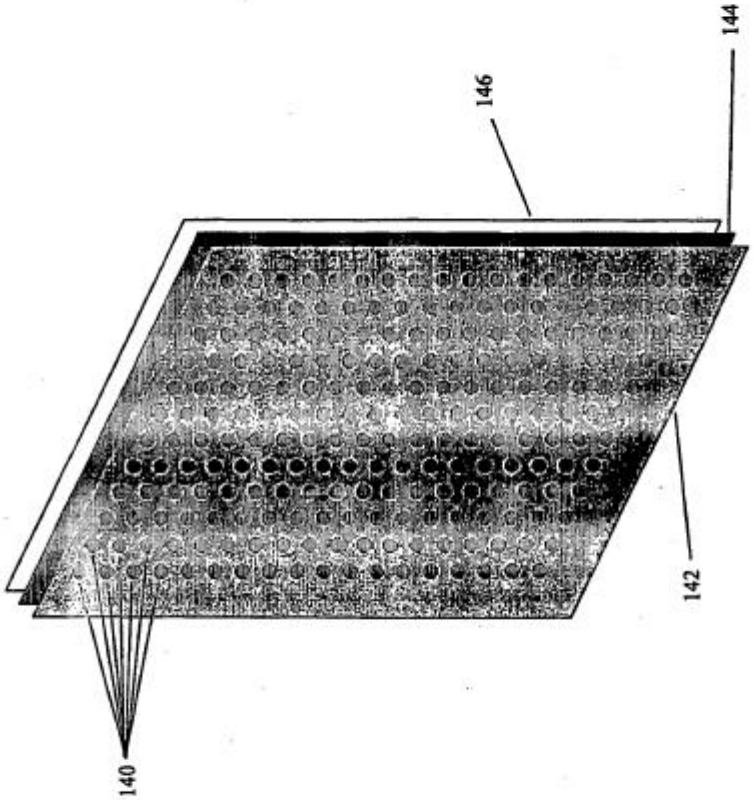

Figura 10

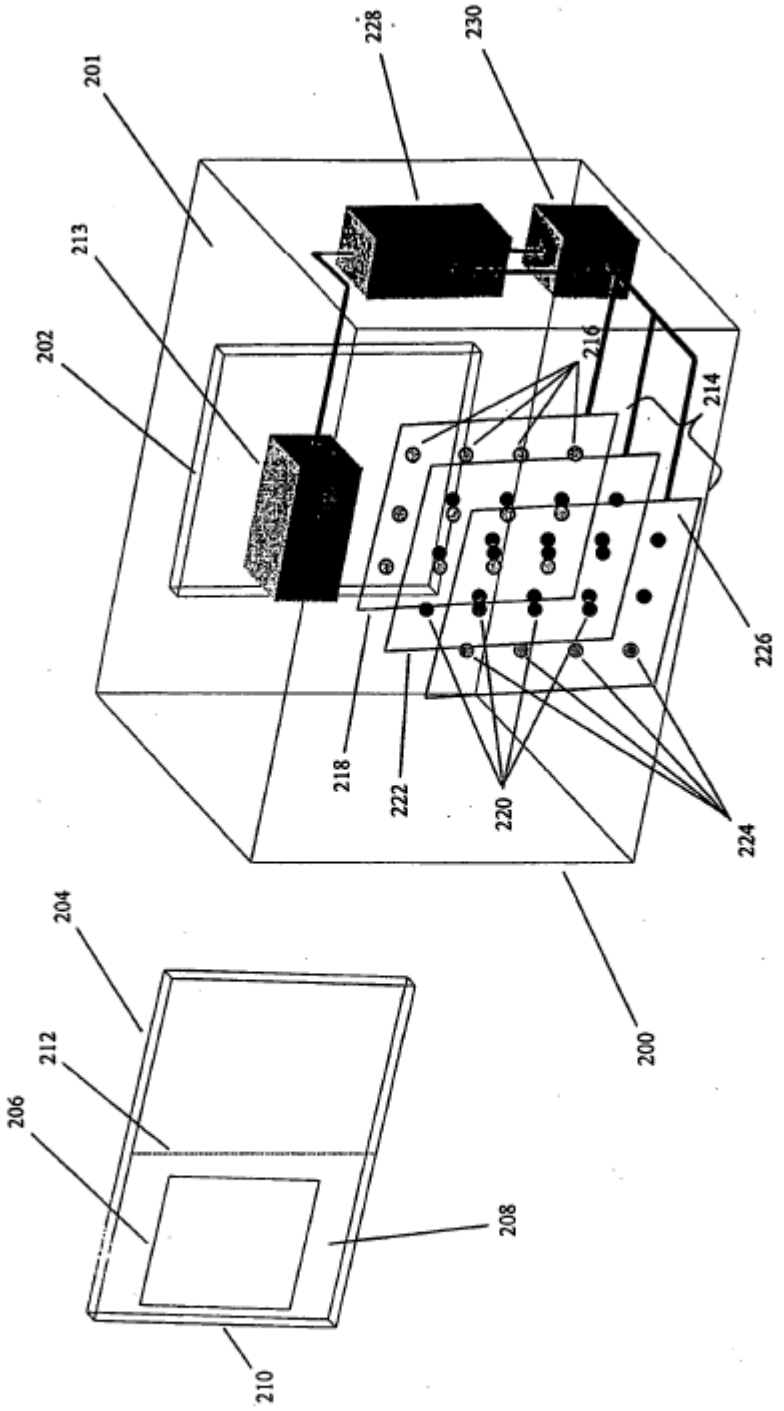
201
228
230
213
202
216
214
226
218
222
220
224
200
204
212
206
208
210

Figura 11

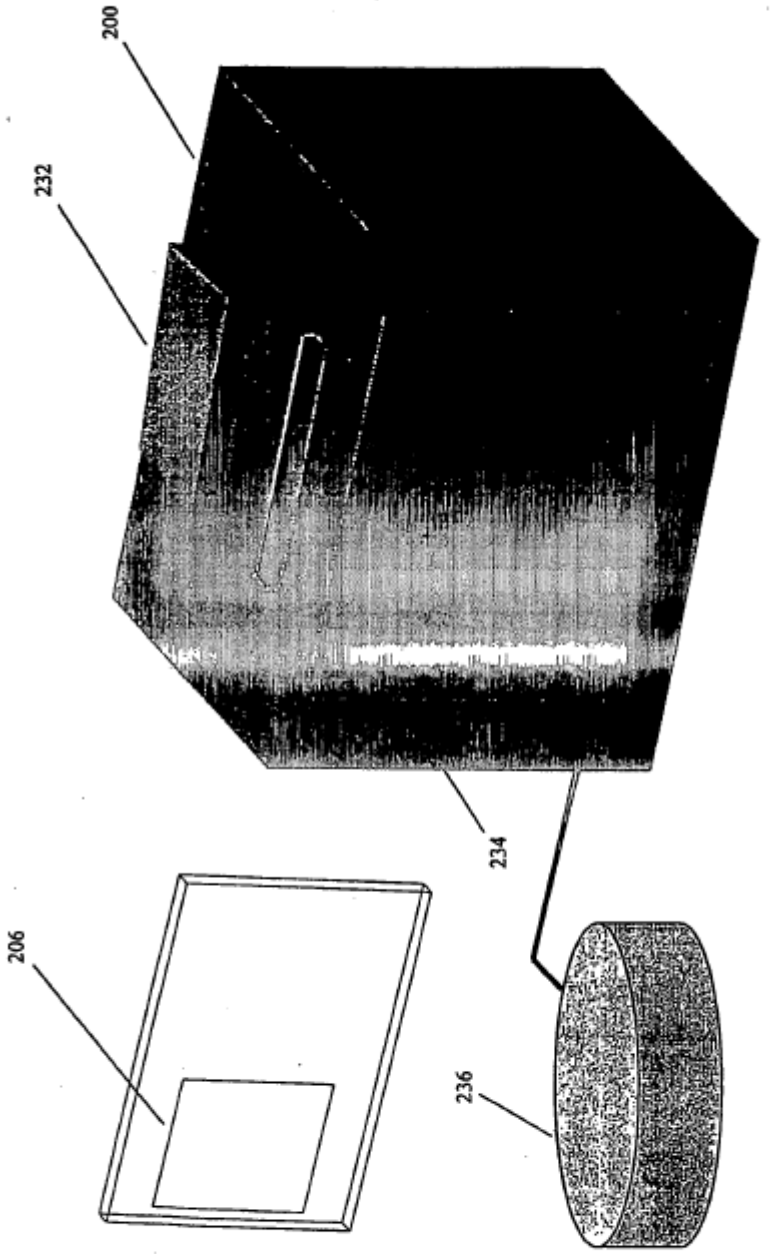

Figura 12

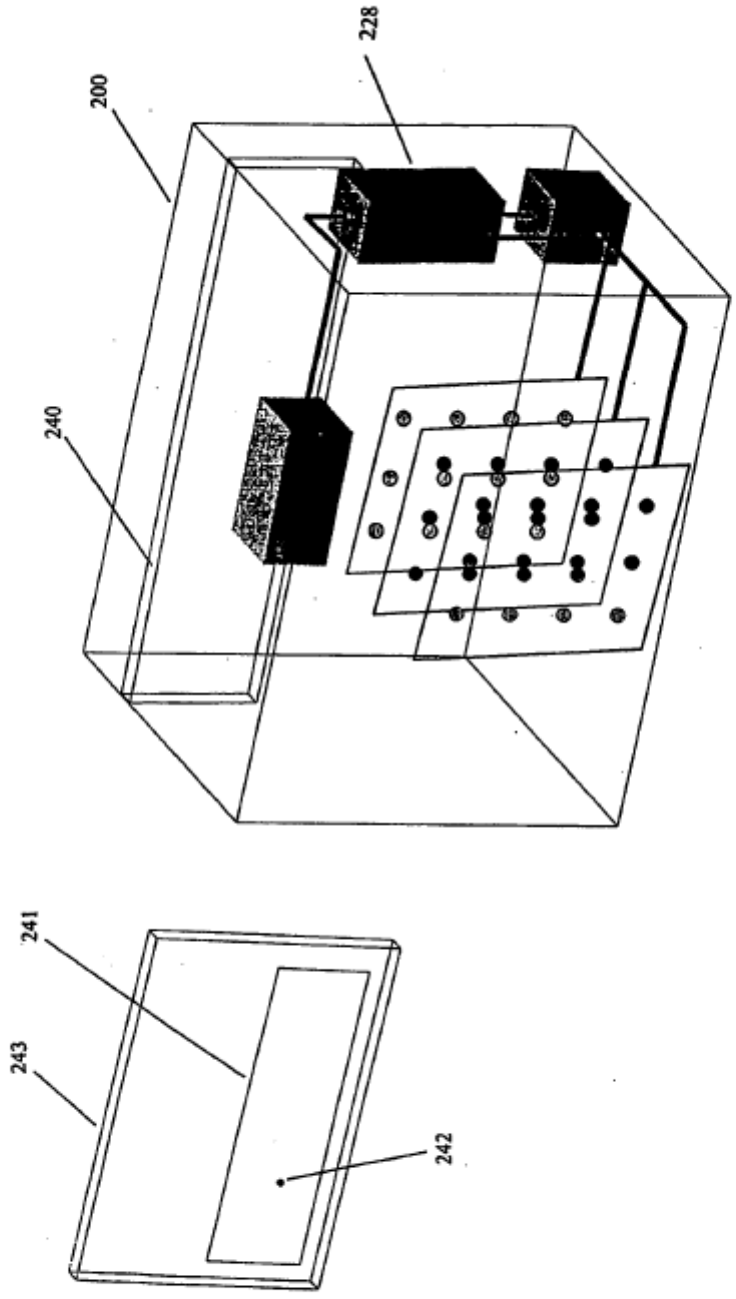

Figura 13

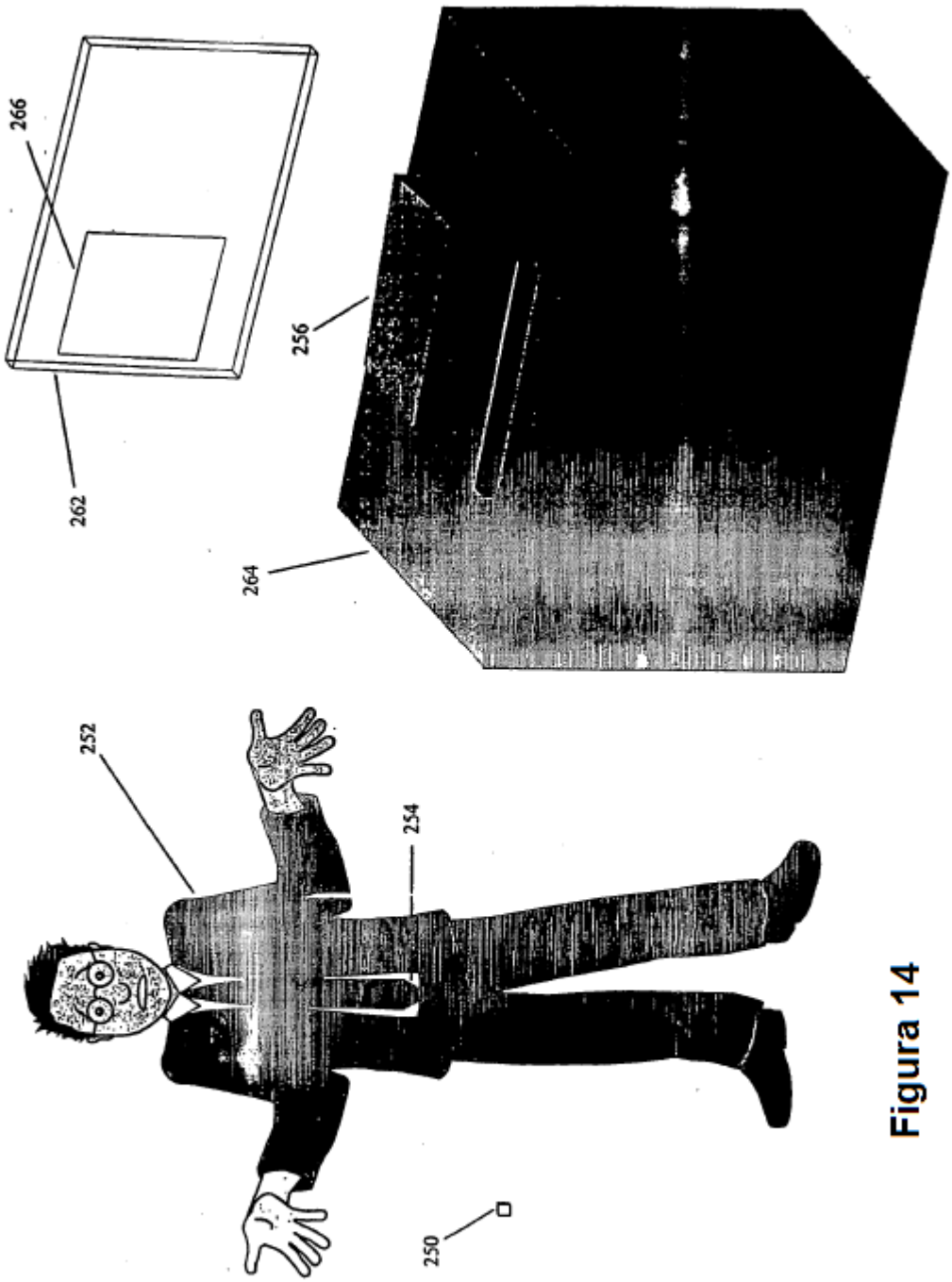

Figura 14

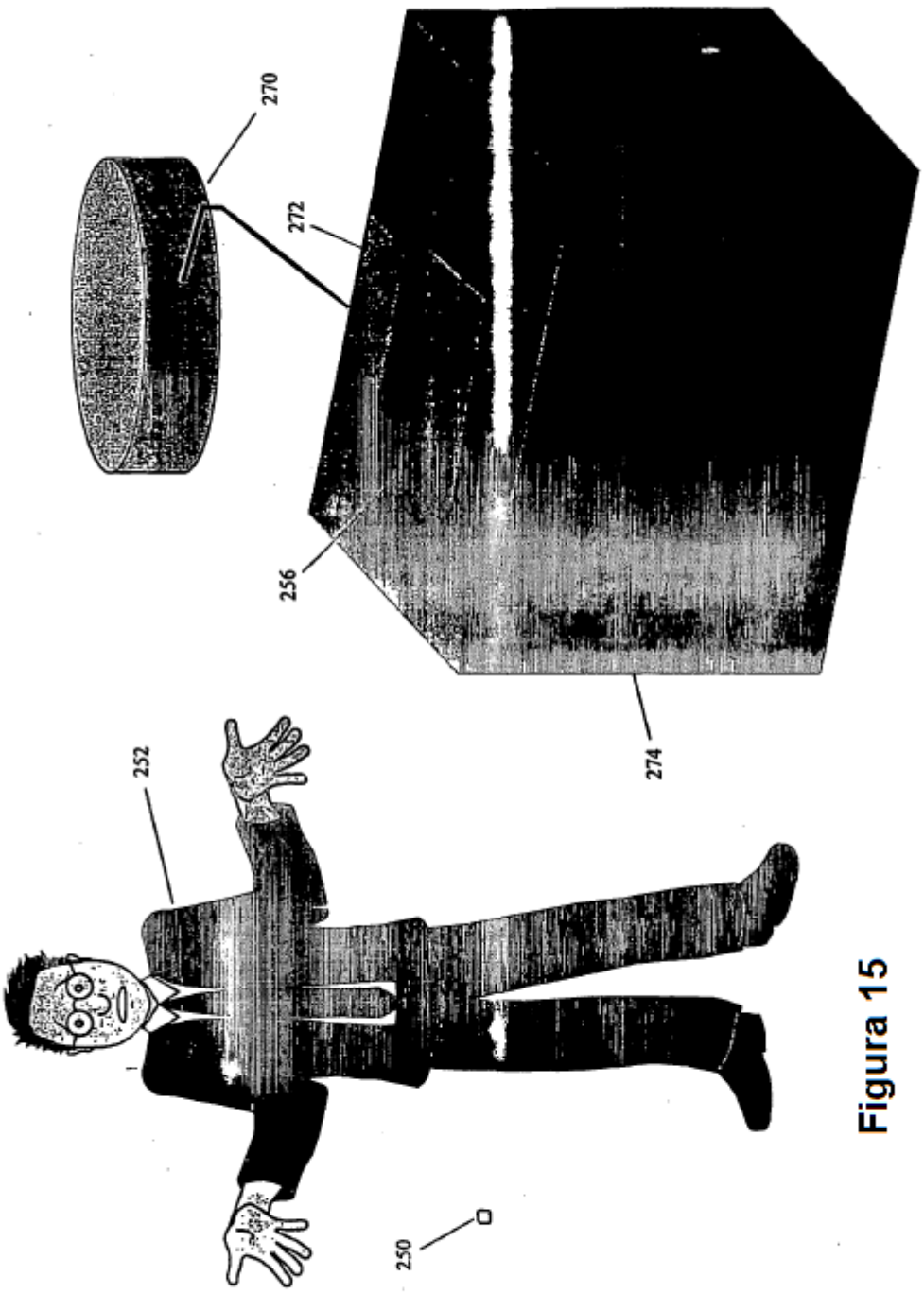

Figura 15