(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 679 286**

(51) Int. CI.:

G06F 21/60 (2013.01)
H04L 29/06 (2006.01)
G06F 21/31 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **07.02.2012 PCT/IB2012/050551**

(87) Fecha y número de publicación internacional: **16.08.2012 WO12107879**

(96) Fecha de presentación y número de la solicitud europea: **07.02.2012 E 12744330 (7)**

(97) Fecha y número de publicación de la concesión europea: **25.04.2018 EP 2673708**

(54) Título: **Distinguir usuarios válidos de robots, OCR y solucionadores de terceras partes cuando se presenta CAPTCHA**

(30) Prioridad:

10.02.2011 US 201161441630 P
05.04.2011 US 201161472114 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.08.2018

(73) Titular/es:

FIREBLADE HOLDINGS, LLC (100.0%)
2021 McKinney Avenue, Suite 1100
Dallas, TX 75201, US

(72) Inventor/es:

RAPAPORT, SHAY;
AZARIA, EREZ y
SCHWARTZ, OMRI

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Distinguir usuarios válidos de robots, OCR y solucionadores de terceras partes cuando se presenta CAPTCHA

Campo técnico

La presente invención se refiere a retos CAPTCHA destinados a evitar la navegación de internet robótica y presentación de formularios y en particular a formas de detección de medios comunes usados para superar los retos CAPTCHA.

Análisis de la técnica relacionada

CAPTCHA son pruebas generadas por ordenador que, en la mayoría de las circunstancias, no pasará un sistema informático y son fácilmente resueltas por los humanos. La implementación típica es una imagen generada por ordenador de caracteres y dígitos que pueden estar distorsionados y contener algún "ruido" de fondo visual. Se pide al usuario que teclee la cadena que se muestra en la imagen, suponiendo el procedimiento que los humanos pueden leer estas imágenes mientras que los ordenadores no pueden. Estas pruebas están destinadas para validad la presencia de un usuario final humano en interacciones efectuándose a través de una red informática.

En la Internet se ha vuelto una práctica común usar herramientas de automatización, conocidas como "robots", para realizar tareas repetitivas y manipular las aplicaciones web. Las tareas repetitivas pueden incluir presentaciones de formularios y peticiones de páginas repetitivas, y se diseñan para crear cuentas de usuarios, para iniciar sesión en cuentas, presentar contenido en formularios web, recoger datos de sitios web y generalmente para manipular plataformas y recursos de sistema. Estas actividades crean valor comercial a los que realizan las mismas, mientras en muchos aspectos alteran gravemente los sistemas y los negocios que manipulan. Las CAPTCHA se desarrollaron para evitar estas manipulaciones, estableciendo si el usuario final es humano o una máquina. Se han convertido en la práctica común que usan los sitios web para evitar la manipulación automatizada, tal como correo basura y otros.

Sin embargo, ya que las CAPTCHA son tan comunes, son el objetivo de creadores de correo basura, empresas e individuos que desean superar o sortear CAPTCHA, para realizar sus fechorías. Existen dos formas conocidas de superar o sortear un reto CAPTCHA. El primero es usando un sistema de Reconocimiento Óptico de Caracteres (OCR) avanzado. Los OCR pueden programarse para identificar los caracteres distorsionados que se usan en ciertas CAPTCHA. Una rutina automatizada ("robot") que utiliza un OCR dejará que el OCR descifre la CAPTCHA y a continuación rellena la cadena en el formulario web, en el que el valor de CAPTCHA debería teclearse.

El segundo procedimiento es retransmitiendo la CAPTCHA a un solucionador humano de tercera parte. Una tercera parte significa una entidad que no es el cliente que interactúa con el servidor web. Compañías de resolución de CAPTCHA comerciales (conocidas como "granjas de CAPTCHA") cobran tan poco como 0,50 $ por resolver 1.000 CAPTCHA. Cuando un robot se encuentra un CAPTCHA, habitualmente capturará la imagen CAPTCHA y enviará la misma a la granja de CAPTCHA (en ocasiones a través de una Interfaz de Programación de Aplicación), en la que un solucionador humano descifrará la imagen, enviando la cadena resultante de vuelta al robot, para rellenar y pasar la prueba. En algunos casos, sitios con tráfico alto, tal como índices de números de serie de software y contenido para adultos, se usan para atraer usuarios inocentes, a los que se les pide que resuelvan un CAPTCHA para conseguir el contenido que estaban buscando. La CAPTCHA realmente se reenvía desde un robot que manipula otra plataforma, siendo ayudado por estos usuarios.

Típicamente, los sitios web que se dan cuenta de actividad automatizada que supera sus CAPTCHA cambiarán a otra variante de CAPTCHA. Esto obstruirá a los OCR, al menos durante un tiempo, porque dependen de las características visuales de la CAPTCHA para resolver la misma. Sin embargo, esto no ayudará contra solucionadores humanos de terceras partes, ya que les da lo mismo el tipo de CAPTCHA: siempre que un usuario humano puede resolver el mismo, ellos pueden. Esto también indica por qué las granjas de CAPTCHA se están volviendo más y más populares, a pesar del hecho de que cuestan dinero y por qué los OCR se están convirtiendo en menos favorables para los creadores de correo basura.

Deseando evitar la superación de CAPTCHA basada en OCR, los retos CAPTCHA se han vuelto más y más difíciles. Los caracteres habitualmente se desenfocan, se tuercen y solapan entre sí en muchos casos. Finalmente, muchas CAPTCHA se ha vuelto muy difíciles incluso para los humanos. Distorsionan la experiencia de usuario y en algunos casos incluso espantan a los usuarios. Estas CAPTCHA difíciles, resistentes a OCR, fallan en detener la resolución de humanos de terceras partes (es decir, una retransmisión) y por lo tanto se comprometen y se superan, por un coste muy bajo, por creadores de correo basura.

Breve resumen

Realizaciones ilustrativas de la presente técnica desvelan un procedimiento y sistemas para proporcionar una prueba de Turing pública automatizada a un sistema de visualización cliente. El procedimiento incluye proporcionar una imagen que tiene una pluralidad de caracteres aleatorios, así como proporcionar un código de navegador al cliente, con lo que el código de navegador se adapta para restingar la visualización de la imagen a únicamente una

porción predeterminada de la imagen. El procedimiento incluye adicionalmente detectar una respuesta de cliente a la recepción de la porción predeterminada de dicha imagen.

Otras realizaciones ilustrativas de la presente técnica incluyen adicionalmente un procedimiento de retar selectivamente a un usuario con una prueba de Turing pública automatizada a un usuario en respuesta a una comunicación del usuario. El procedimiento incluye comprobar la existencia de un identificador de usuario. El procedimiento incluye adicionalmente verificar que el identificador de usuario devuelto no es un identificador robado si se devuelve el identificador de usuario. Si no se devuelve el identificador de usuario, entonces el procedimiento asigna un identificador de usuario al usuario. Además, el procedimiento incluye presentar la prueba de Turing pública automatizada al usuario a no ser que se cumpla un criterio predeterminado. Además, el procedimiento incluye obtener y almacenar un análisis de la respuesta del usuario a la prueba de Turing pública automatizada. Ejemplos del estado de la técnica en el presente campo técnico se desvelan en los documentos US2009/113294 A1 y WO2010/111169 A1. La invención se define mediante las reivindicaciones independientes. Realizaciones adicionales se definen mediante las reivindicaciones dependientes.

Breve descripción de los dibujos

Para un mejor entendimiento de las realizaciones de la invención y para mostrar cómo la misma puede llevarse a efecto, se hará ahora referencia, simplemente a modo de ejemplo, a los dibujos adjuntos en los que números similares designan elementos o secciones correspondientes por todos ellos.

En los dibujos adjuntos:

La Figura 1 es un diagrama de flujo que ilustra las interacciones funcionales entre un usuario final, un servidor web y un servidor dedicado a la provisión del servicio CAPTCHA, de acuerdo con un aspecto de la presente técnica.
La Figura 2 es un diagrama de flujo de un Conjunto de Reglas de Análisis de CAPTCHA, de acuerdo con un aspecto de la presente invención.
La Figura 3 es un diagrama de flujo, de acuerdo con un aspecto de la presente invención.
La Figura 4 es un sistema de red de acuerdo con una realización ilustrativa de la presente invención.

Descripción detallada

Con referencia específica ahora a los dibujos en detalle, se hace hincapié que los particulares mostrados son únicamente a modo de ejemplo y para fines de descripción ilustrativa de las realizaciones preferidas de la presente invención, y se presentan con el motivo de proporcionar lo que se cree que es la descripción más útil y fácilmente entendible de los principios y aspectos conceptuales de la invención. En este sentido, no se hace ningún intento de mostrar detalles estructurales de la invención en más detalle de lo que es necesario para un entendimiento fundamental de la invención, la descripción tomada con los dibujos que hace evidente a los expertos en la materia cómo pueden incorporarse en la práctica varias formas de la invención.

Antes de explicar al menos una realización de la invención en detalle, se ha de entender que la invención no se limita en su aplicación a los detalles de construcción y la disposición de los componentes expuestos en la siguiente descripción o ilustrados en los dibujos. La invención es aplicable a otras realizaciones o de practicarse o efectuarse de diversas formas. También, se ha de entender que la fraseología y terminología empleadas en el presente documento es para el fin de descripción y no deberían considerarse como limitantes.

La Figura 1 es un diagrama de flujo 10 que ilustra operación general de los procedimientos desvelados descritos en mayor detalle a continuación, proporcionando el diagrama 10 de flujos una vista general de las interacciones funcionales entre un usuario final, un servidor web y un servidor dedicado a la provisión del servicio CAPTCHA (en lo sucesivo "Máquina de Servicio"), funcionando los componentes de sistema de acuerdo con la presente invención.

Una sesión de CAPTCHA se inicia en el servidor web o aplicación web, en la etapa 12. La Máquina de Servicio devuelve un ID de transacción y un código al servidor web o aplicación web, en la etapa 14. El servidor web o aplicación web emite una rutina al usuario, en la etapa 16. El usuario final recibe la rutina, en la etapa 18, y consigue una página con un código embebido, y crea un Iframe. La Máquina de Servicio recibe una transmisión desde el usuario final y consigue una etiqueta de usuario o aplica una etiqueta de usuario, en la etapa 20. La Máquina de Servicio también consigue los atributos del dispositivo de usuario, en la etapa 22, y genera imágenes y código, en la etapa 24.

En la etapa 26, la Máquina de Servicio envía el código de CAPTCHA al usuario final. El usuario final obtiene el código de CAPTCHA, en la etapa 28, envía una etiqueta y solicita una imagen de CAPTCHA. La Máquina de Servicio recibe la petición de usuario y envía la imagen de CAPTCHA al usuario final, en la etapa 30. El dispositivo de usuario final muestra una imagen parcial, registra eventos y envía el formulario al servidor web o aplicación web, en la etapa 32. El servidor web o aplicación web obtiene las entradas del formulario, incluyendo los campos de CAPTCHA, en la etapa 34. El servidor web o aplicación web a continuación consulta a la Máquina de Servicio para validar la CAPTCHA, en la etapa 36.

La Máquina de Servicio obtiene la CAPTCHA y los eventos de dispositivo de usuario, en la etapa 38. La Máquina de Servicio a continuación genera un análisis de entradas de usuario, en la etapa 40, un análisis de eventos de dispositivo de usuario, en la etapa 42, y un análisis de historial de dispositivo de usuario, en la etapa 44. Los resultados y alertas de prueba de CAPTCHA resultantes se devuelven al dispositivo de usuario final por la Máquina de Servicio, en la etapa 46. El dispositivo de usuario final recibe los resultados y alertas de prueba de CAPTCHA desde la Máquina de Servicio, en la etapa 48, y reacciona en consecuencia, en la etapa 50, como se describe en mayor detalle a continuación.

En una realización ilustrativa de la presente invención, puede generarse una imagen que comprende una cadena aleatoria, convertida en un mapa de bits, por un servidor, ya sea el servidor web sirviendo el sitio que se navega o un servidor dedicado a la provisión de la Máquina de Servicio. La imagen puede ser animada, tal como usando GIF animado, para "dificultar" el descifrado de la cadena con un OCR. Una animación puede ser, sin limitación, (i) una línea vertical gruesa de píxeles que da vueltas horizontalmente en la cadena de texto, de modo que en cada minuto dado al menos un carácter estará al menos parcialmente oculto detrás de los píxeles en círculo, o (ii) una línea horizontal dando vueltas arriba y abajo de la imagen para ocultar una porción de todos los caracteres en cualquier momento dado.

En una realización ilustrativa, únicamente se mostrará al usuario final una parte predeterminada de la imagen de CAPTCHA generada por la Máquina de Servicio. Para este fin, la Máquina de Servicio decidirá primero, aleatoriamente, qué parte de la imagen completa debe mostrarse (por ejemplo, caracteres 4-9 de una imagen de CAPTCHA de 12 caracteres). La Máquina de Servicio calculará la cantidad de píxeles que necesitan ocultarse en ambos bordes de la imagen de CAPTCHA completa, y almacenará todos los valores generados, incluyendo; (i) la cadena de CAPTCHA completa, (ii) la cadena parcial a mostrar y (iii) el número de píxeles que necesitan ocultarse en ambos lados de la imagen de CAPTCHA completa.

En una realización ilustrativa, para el fin del cálculo de la anchura de las partes de la imagen de CAPTCHA completa que necesitan ocultarse, un procedimiento puede funcionar para crear tanto la imagen de CAPTCHA completa como crear una imagen o imágenes de las partes de la cadena completa que no se conciben para mostrarse. Por ejemplo, si la cadena completa es "abcdefgh12345" y únicamente la cadena "fgh123" se concibe para mostrarse al usuario final, el servidor creará una imagen de "abcdefgh123" y a continuación dos imágenes temporales, una imagen de la cadena "abcde" y una imagen de "45", usando el mismo tipo de fuente y tamaño. Las últimas dos imágenes se usarán para medir su anchura, que puede consultarse fácilmente después de que se hayan producido, y almacenar los valores del número de píxeles a ocultar en cada lado de la imagen completa.

En una realización ilustrativa, para el fin de ocultar partes de la CAPTCHA completa y mostrar únicamente los caracteres seleccionados, la Máquina de Servicio genera un código de lado de cliente (habitualmente HTML, Javascript y CSS), que se servirá en el navegador del cliente final y encapsulará la imagen. El número de píxeles a ocultar en ambos lados pueden pasarse a esta rutina, como un valor numérico o como una función o numerosas funciones que generan este valor. La rutina, cuando se representa en un explorador web, mostrará la imagen, pero ocultará los caracteres que no están destinados a mostrarse. Tal rutina puede, sin desear ser limitante, generar una etiqueta de iFrame, con atributos que hacen la misma más corta en longitud que la imagen creada para el reto. La imagen puede presentarse en el marco, y puede concebirse para la derecha o la izquierda mediante el número de píxeles precalculado que hará visible exactamente la parte deseada. Por ejemplo y sin desear ser limitante, el sangrado de la imagen a la derecha o a la izquierda puede hacerse con atributos de estilo, tal como atributos de CSS "izquierda" o "derecha", o añadiendo otras imágenes generadas con la anchura precalculada a la izquierda o la derecha de la imagen de CAPTCHA completa.

En otra realización ilustrativa, cuando el usuario envía la CAPTCHA, las entradas del usuario se transferirán a la Máquina de Servicio, ya sea directa o indirectamente (tal como mediante una llamada de servicio web que contiene un ID de transacción). La Máquina de Servicio realizará un Análisis de Entrada del Usuario que se concibe para concluir si la CAPTCHA se tecleó correctamente y si existe una indicación de retransmisión o fraude de automatización. El resultado de Análisis de Entrada del Usuario puede almacenarse finalmente como un único valor, o dos valores separados - un valor indicando en análisis de coincidencia de cadena y un valor indicando si se ha detectado un fraude en el rellenado de la CAPTCHA. Por claridad de explicación, cuando se usan dos tales valores separados, el primer valor se identifica mediante la etiqueta stringMatch y el segundo valor se identifica mediante la etiqueta fraudDetected.

Para realizar el Análisis de Entrada del Usuario, la Máquina de Servicio puede comparar la cadena de entrada del usuario tanto a la cadena parcial que se concibió para mostrarse y a la completa generada para la actual transacción de CAPTCHA, de acuerdo con un Conjunto de Reglas para la Toma de Decisiones, funcionando el Conjunto de Reglas de acuerdo con un diagrama 60 de flujo, mostrado en la Figura 2. Si la cadena de entrada del usuario coincide con la cadena parcial, en el bloque 62 de decisión, significa que el usuario tecleó la parte visible de la imagen de CAPTCHA completa y pasó la prueba correctamente. En tal caso el valor de stringMatch se establecería a "Pasada," en la etapa 64. Si la cadena no coincide con ninguna de las cadenas almacenadas, es decir, ni una cadena almacenada completa ni una cadena parcial almacenada generada para esta transacción, significa que el usuario falló la prueba de CAPTCHA y el valor de stringMatch se establecerá a "Fallada," en el bloque 65 y el procedimiento se mueve al bloque 66 de decisión. Si, en el bloque 66 de decisión, la cadena de entrada del usuario

coincide con la cadena completa (que comprende la imagen completa, incluyendo los caracteres ocultos) esto significa que tuvo lugar un procedimiento de retransmisión, en la etapa 68, ya que el usuario no debería ver las partes ocultas de la imagen de CAPTCHA completa. Esto indica que la imagen completa se transmitió a una máquina de tercera parte, en la que un usuario humano vio la misma sin las capas cubriendo porciones de la misma, y por lo tanto rellenando toda la cadena. En tales casos, el valor de stringMatch permanecerá como "Fallada," en la etapa 70, y el valor de fraudDetected se establecerá de su valor por defecto de "OK" a "Retransmisión."

Al final del Análisis de Entrada del Usuario, la Máquina de Servicio puede almacenar el resultado (Pasada/Fallada, Retransmisión/OK) con los datos de usuario y datos de usuario. La Máquina de Servicio puede responder a la aplicación web con el resultado de Análisis de Entrada del Usuario o realizar análisis adicionales como se explica adicionalmente antes del almacenamiento de los resultados y la respuesta a la aplicación web. En aún otra realización ilustrativa, la presente invención incluye medios adicionales para identificar casos de retransmisión. Ya que se usan rutinas de lado de cliente tal como HTML/CSS/Javascript para cubrir partes de la imagen, los creadores de correo basura pueden intentar transmitir todo el código pertinente con la imagen a un solucionador humano de tercera parte, para establecer una situación en la que la misma parte de la imagen se oculta o muestra en la pantalla del solucionador.

Si se usa una iFrame para mostrar la CAPTCHA, puede embeberse un Javascript dentro del documento de iFrame, para detectar la presencia de una iFrame y un documento padre, y/o para examinar el tamaño de iFrame y estar seguro que es del mismo tamaño que originalmente se insertó en el código y/o para consultar el URL de la iFrame y su documento padre y ver si ambos aparecen en los URL correctos de la aplicación web o para abrir aún otro marco de documento e intentar consultar el mismo a través de rutina de lado de cliente, para estar seguros se permiten rutinas cruzadas y se establece que la CAPTCHA y aplicación web se muestren en el mismo dominio. URL incorrectos, una falta de iFrame, relaciones incorrectas de documentos padre/hijo o incapacidad de alcanzar otro URL en el dominio de la aplicación web a través de rutina, pueden indicar retransmisión. En caso de tal retransmisión, el valor de fraudDetected se establecerá desde su valor por defecto de "OK" a "Retransmisión".

En aún otra realización ilustrativa, la presente invención puede incluir más medios para detectar retransmisión. La aplicación web puede incluir un código que comprobará las direcciones IP de usuario durante sus sesiones y enviará las mismas a la Máquina de Servicio al comienzo de una sesión de servicio CAPTCHA. La Máquina de Servicio puede comparar adicionalmente la dirección IP o direcciones con la usada para rellenar la CAPTCHA. Si la página que presenta la CAPTCHA se lee desde una dirección IP diferente de la que realiza la sesión de usuario, y no dentro del mismo intervalo de IP o geolocalización, o mismo ID de organización (tomada desde la consulta 'whois' de IP), esto también es una evidencia de un procedimiento de retransmisión. En caso de tal retransmisión, el valor de fraudDetected se establecerá desde su valor por defecto de "OK" a "Retransmisión."

En otra realización ilustrativa, la presente invención puede incluir Análisis de Eventos de Usuario para detectar intentos automatizados o fraudulentos para enviar datos y superar la CAPTCHA. Para el fin de recoger datos para el Análisis de Eventos de Usuario, el código de lado de cliente puede incluir escuchadores de eventos, que probarán si el usuario: (i) realmente enfocó en el campo de texto de CAPTCHA u otros campos de formulario (evento de "onFocus" en Javascript), (ii) si hubo o bien un clic de ratón, un movimiento de ratón o bien una pulsación de tecla para moverse entre campos y (iii) si se usaron eventos de pulsaciones de teclas correlativas para teclear los datos y si se usó un evento de ratón o teclado para enviar el formulario. Los escuchadores de eventos registrarán el ratón y eventos de teclado y pueden almacenar el registro temporalmente. El almacenamiento puede conseguirse, sin desear ser limitante, o bien en el lado de cliente como rutinas variables, cookies o almacenamiento local, o bien como alternativa en el servidor web a través de Ajax.

Típicamente, pero sin desear ser limitante, el registro grabará cualquier evento de formulario, tal como: (i) evento de desenfoque o de enfoque de elemento de formulario, (ii) cualquier cambio de valor de campo y el evento de envío de formulario y (iii) una lista de eventos de teclado y ratón que se realizaron antes de cada tal evento de formulario. El registro de eventos puede devolverse a la Máquina de Servicio para análisis cuando se envían el formulario y la CAPTCHA. La Máquina de Servicio puede aplicarse a un Conjunto de Reglas de Eventos de Usuario para establecer si el campo de texto de CAPTCHA o cualquier otro campo de formulario se ha rellenado sin los eventos de ratón y/o teclado correlacionados esperados. La falta de los eventos esperados puede ser evidencia de que tuvieron lugar un procedimiento automatizado y/o un procedimiento de retransmisión. En tales casos de automatización, el valor fraudDetected se establecerá desde su valor por defecto de "OK" a "Automatización".

En otra realización ilustrativa, el dicho Conjunto de Reglas de Eventos de Usuario puede configurarse para satisfacerse si ha habido pulsaciones de tecla o eventos de ratón, o como alternativa, si ha habido al menos un evento de pulsación de tecla o ratón por cada enfoque de campo de usuario o cada desenfoque de campo de formulario o cada cambio de valor de campo de formulario o cualquier combinación de estos. Adicionalmente, el Conjunto de Reglas de Eventos de Usuario puede establecerse para probar las pulsaciones de tecla separadas y emparejar las mismas con los valores enviados en ciertos campos de formulario.

En otra realización ilustrativa, para el fin de la grabación de los historiales de usuarios, la Máquina de Servicio puede asignar una identidad de usuario única (en lo sucesivo: "etiqueta de usuario") a cada usuario. La etiqueta de usuario se enviará al usuario final en una rutina, que almacenará la misma en la máquina del usuario, o bien como una

cookie de navegador o bien una cookie Flash (también conocido como "almacenamiento global") o bien como un valor de almacenamiento local de navegador o bien como un fichero de rutina en caché que contiene la etiqueta como un valor o cualquier combinación de estos procedimientos. La Máquina de Servicio también servirá una rutina que recogerá las etiquetas de usuario desde el navegador del usuario, si el usuario ya tiene tal etiqueta de usuario. Cualquier información recogida en una sesión de CAPTCHA puede grabarse de una manera que permite la restauración de los datos más tarde a base de la etiqueta de usuario como una clave.

En otra realización ilustrativa, para el fin de la identificación de usuarios que tratan de evitar el etiquetamiento mediante el borrado de cookies y caché, y para habilitar que la Máquina de Servicio restablezca sus historiales, la Máquina de Servicio puede recoger de los dispositivos de usuarios finales y atributos de navegador, comúnmente conocidos como "huellas del dispositivo." Tales huellas se recogen mediante una combinación de código de lado de servidor y lado de cliente, como se demuestra en 'EFF.org' y 'browserspy.com.' La Máquina de Servicio servirá el código al navegador de usuario final y almacenará los resultados necesarios.

Estos atributos pueden incluir, sin desear ser limitante, el tipo de navegador, tipo de sistema operativo, resolución de pantalla, fuentes disponibles, versión y revisión de Javascript, módulos instalados, tal como Flash y otros y sus versiones, complementos de buscador tal como Adobe Acrobat, Skype y así sucesivamente, desfase horario entre el reloj de cliente y el reloj de servidor, versión de flash, encabezamientos de HTTP, pila de TCP/IP, uso de intermediarios, intervalo de IP y geolocalización y otros. La combinación de estos atributos puede crear una huella única, en niveles de precisión variables, comenzando desde uno a unas pocas decenas de miles y creciendo hasta uno en unos pocos millones, como se demuestra en el sitio web de EFF.ORG. Estos atributos se almacenarán, de forma separada o como una cadena (tal como un valor troceado) a lo largo de cualquier etiqueta de usuario creada recientemente, así que siempre que se crea una etiqueta de usuario y guarda en la máquina del usuario, la etiqueta de usuario también se almacena en la Máquina de Servicio con estos atributos de dispositivo, de una manera que permite restaurar los atributos de dispositivo mediante la etiqueta de usuario y viceversa.

En otra realización ilustrativa, para el fin de la identificación de un usuario retornante, la Máquina de Servicio establecerá primero si la etiqueta de usuario se ha creado recientemente en la sesión actual, o una veterana que se ha recogido del usuario. Si la etiqueta de usuario es veterana (significando que el usuario inició la sesión con una etiqueta existente), la Máquina de Servicio buscará la etiqueta en la base de datos y, si encuentra la misma, usará esta etiqueta de usuario para el almacenamiento de cualquier información acerca de esta sesión. También puede marcar esta etiqueta de usuario como una "etiqueta veterana", significado que este usuario tenía al menos dos o un número mayor de sesiones con la misma etiqueta (indicando que este usuario no tiende a borrar cookies y caché). Si el usuario no tiene ninguna etiqueta de usuario veterana o la etiqueta recogida no pudiera encontrarse en la base de datos, la Máquina de Servicio puede buscar la etiqueta de usuario mediante atributos de dispositivo. Los atributos recogidos por Máquina de Servicio en la sesión actual pueden compararse o bien con todos los demás atributos de dispositivo anteriormente almacenados, o bien como alternativa solo con etiquetas que no tengan una bandera de "etiqueta veterana", significando que son o bien nuevos usuarios o sospechosos de usuarios que borran cookies y caché del navegador - potencialmente con el fin de ocultar sus identidades. Si se encuentra una coincidencia, se buscará la etiqueta de usuarios coincidente y usará para esta sesión.

En otra realización ilustrativa, para el fin de la grabación de historiales de usuario, después de la creación y restauración de una etiqueta de usuario, cualquier evento de sesión de CAPTCHA puede almacenarse con la etiqueta de usuario de una manera que permite restaurar el historial de usuario más tarde mediante la etiqueta de usuario. Tales eventos pueden ser la hora de inicio de sesión, la hora de respuesta del usuario, los detalles del sitio web, los resultados de Análisis de Entrada del Usuario y los resultados de Análisis de Fraude por sesión. En una realización ilustrativa, la Máquina de Servicio puede realizar un Análisis de Historial del Usuario en casos de etiquetas de usuario recogidas desde el usuario o encontradas a través de una búsqueda de atributos de dispositivo. Para el fin de Análisis de Historial de Usuario, la Máquina de Servicio usará la etiqueta de usuario para restaurar todos o recientes datos de sesión de esa etiqueta de usuario. Las sesiones recientes pueden ser un número limitado de últimas sesiones (tal como las últimas 100 sesiones) o todas las sesiones durante los últimos minutos u horas. La Máquina de Servicio, después de recoger el Historial de Usuario, aplicará un Conjunto de Reglas de Análisis de Historial para establecer si este puede ser un creador de correo basura potencial. Los resultados del Análisis de Historial de Usuario se enviarán a la aplicación web con el Análisis de Entrada del Usuario.

En una realización ilustrativa, el Conjunto de Reglas de Historial de Usuario establecerá que un usuario es un creador de correo basura potencial si se cumple una o más de las siguientes condiciones: (i) si el usuario tiene más de una sesión de CAPTCHA predefinida por límite de tiempo (pueden comprobarse diversos intervalos de tiempo, tal como último minuto, últimos 10 minutos etc.); (ii) si el usuario tiene más de un número predefinido de grabaciones de Retransmisión, (iii) si el usuario tiene más de un número predeterminado de grabaciones de Automatización o (iv) si el usuario ha superado un umbral de relación predeterminada de grabaciones de Fallada en comparación con Pasada.

En aún otra realización ilustrativa, la Máquina de Servicio puede ser una máquina o máquinas especializadas (ya sea física o virtual) establecidas para el fin del Servicio de CAPTCHA Avanzado. La Máquina de Servicio puede servir el código de lado de cliente directamente al usuario final (a través de iFrame), o indirectamente, pasando partes o todo el código e imágenes al servidor de aplicación web, que servirá las mismas a los usuarios finales, o

enviará el código al servidor web, que enviará el mismo a sus clientes finales. Típicamente, pero sin desear ser limitante, el servidor web creará un ID de transacción, y pedirá al servidor de CAPTCHA el código, usando el ID de transacción (a través de HTTP/servicio web).

En una realización ilustrativa, la Máquina de Servicio comprende una máquina independiente, que comunica tanto con la aplicación web como el usuario final. La aplicación web llama a la máquina de servidor (habitualmente a través de servicio web) cuando se necesita el servicio de CAPTCHA y consigue un ID de transacción y código de lado de cliente para embeber a una página, para mostrar la CAPTCHA progresiva. El código contiene los escuchadores de eventos necesarios para cualquier Análisis de Eventos de Usuario y una función que genera un Iframe en el que se mostrará la imagen de CAPTCHA, y un campo de formulario en el que tecleará el valor de CAPTCHA. El origen de Iframe llama a un URL en la Máquina de Servicio, con el ID de transacción embebido en el URL. La Máquina de Servicio, cuando consigue la llamada desde el navegador del usuario final genera las cadenas de CAPTCHA e imágenes de CAPTCHA y devuelve el código usado para coger atributos de dispositivo desde el navegador del usuario, un código que llama y muestra las imágenes de CAPTCHA con partes de la misma ocultas como se ha descrito anteriormente, y la imagen de CAPTCHA completa. Cuando la CAPTCHA se rellena y el formulario se envía al servidor de aplicación web, la aplicación web consultará a la Máquina de Servicio acerca de los resultados de análisis, habitualmente a través del servicio web que contiene el ID de transacción en la petición.

Otras realizaciones ilustrativas de la presente técnica incluyen un procedimiento adaptado para detectar un cliente final legítimo, o navegador, y eliminar el reto CAPTCHA para tales clientes legítimos. Sin embargo, si el procedimiento reconoce al cliente o navegador como una rutina automatizada o un creador de correo basura, el reto CAPTCHA no se elimina para tal cliente final.

De acuerdo con la presente invención, (i) el código y todos los medios usados para decidir si un reto CAPTCHA debe presentarse a un cliente final y (ii) todo el código y medios necesarios para comunicar con una aplicación web y/o un software de CAPTCHA o servicio de CAPTCHA, puede residir o bien en un servidor web en el que reside el sitio web o bien en otro servidor o dispositivo.

Preferentemente, el servidor o dispositivo funciona para comunicar con un cliente final de sitio web, o bien (i) directamente (tal como mediante una llamada de iFrame desde un documento que se origina desde el servidor web), o bien (ii) indirectamente (tal como mediante la comunicación de código o direcciones a la aplicación web que sirve el código a los clientes finales. Tal comunicación puede conseguirse mediante cualquier protocolo, tal como mediante un servicio web o mediante cualquier combinación de los anteriores. El servidor o dispositivo que se usa para decidir si un cierto cliente final será presentado con una CAPTCHA se denominará en lo sucesivo como la "Máquina de Servicio" y el servicio proporcionado por la Máquina de Servicio se denomina en lo sucesivo como "Eliminación de CAPTCHA Condicional."

Por consiguiente, volviendo a la Figura 2, se proporciona un diagrama 80 de flujo de acuerdo con una realización ilustrativa de la técnica presente. Por lo tanto, cuando una CAPTCHA se presenta a un cliente final en un sitio web en el que se integra Eliminación de CAPTCHA Condicional, la Máquina de Servicio comprobará la existencia de un identificador de usuario (en lo sucesivo "etiqueta de usuario") en el dispositivo de cliente final. Se buscará tal etiqueta de usuario, a través de rutina de lado de cliente servida al cliente final, en una cookie de navegador, almacenamiento local de navegador, cookie de Flash (conocido como "almacenamiento global") y página de JavaScript en caché para determinar si existe una cookie de etiqueta de usuario, en el bloque 82 de decisión.

Si una cookie de etiqueta de usuario está presente y se devuelve a la Máquina de Servicio, el procedimiento se mueve al bloque 84 de decisión en el que la Máquina de Servicio busca el dispositivo de cliente final en una base de datos de Máquina de Servicio (SM). Si el dispositivo de cliente final está listado en la base de datos de SM, el procedimiento continúa a la etapa 86 para obtener la etiqueta de historial de usuario desde la base de datos de SM. Si detalles adicionales de dispositivo de cliente final están presentes en la base de datos de SM (tal como huellas del dispositivo, como se describe a continuación), la Máquina de Servicio puede comparar algunos o todos los atributos de dispositivo de cliente final actual con los atributos guardados con la regla de etiqueta de usuario establecida en la base de datos de SM, para verificar que la cookie de etiqueta de usuario no se ha robado, en la etapa 88.

Si se sospecha que el cliente final es un creador de correo basura, en el bloque 90 de decisión, se presenta el reto CAPTCHA, en la etapa 92. De otra manera, si los atributos de cliente final están en orden, el procedimiento continúa a la etapa 94 en la que se elimina el reto CAPTCHA para este cliente final particular. Si la búsqueda de base de datos de SM determina que el dispositivo de cliente final es un dispositivo desconocido, es decir, el dispositivo de cliente final o bien (i) no tiene ninguna etiqueta de usuario o bien (ii) tiene una etiqueta de usuario que no puede encontrarse o validarse, la Máquina de Servicio asignará una etiqueta de usuario única al dispositivo de cliente final y colocará la etiqueta de usuario única en el dispositivo de cliente final a través de una cookie, en la etapa 96.

Como se entiende en la técnica pertinente, una cookie puede ser una cookie de navegador estándar, un almacenamiento local de navegador, una cookie de flash (almacenamiento global) o un fichero de JavaScript en caché que contiene la etiqueta de usuario. La Máquina de Servicio pueden también recoger atributos desde el dispositivo de cliente final, en la etapa 98, ayudado por código de lado de cliente. Tales detalles, conocidos extensamente como "huella de dispositivo", pueden incluir, sin desear ser limitante, tipo y versión de navegador, tipo

y versión de SO, revisión de navegador, revisión de JavaScript, fuentes existentes, encabezamientos de http, módulos de navegador disponibles y sus versiones, complementos de navegador (tal como Acrobat Reader, Skype y otros). Estos atributos se almacenarán con la etiqueta de usuario recientemente creada, para múltiples fines, tal como: (i) la verificación de que una etiqueta de retorno pertenece al cliente final y no se ha robado (como se ha descrito anteriormente) o (ii) el reconocimiento de dispositivos de cliente que eliminan cookies y caché.

En una realización ilustrativa, cuando una CAPTCHA se presenta a un cliente final en un sitio web en el que se integra Eliminación de CAPTCHA Condicional, siempre que se inicia un reto, se notificará a la Máquina de Servicio (habitualmente a través de servicio web) y almacenará el evento con la etiqueta de usuario. Siempre que se envían las entradas de usuario al reto, la Máquina de Servicio, obtendrá y almacenará el análisis del reto CAPTCHA.

Tal análisis se realiza habitualmente mediante cualquier software de CAPTCHA o servicio comparando la cadena de CAPTCHA con la entrada de cliente y determinando si la prueba de CAPTCHA fue satisfactoria o no. Servicios de CAPTCHA Avanzados también pueden detectar signos de intentos de sortear una prueba de CAPTCHA, habitualmente mediante automatización de OCR o solucionadores humanos de tercera parte (conocido como "retransmisión de CAPTCHA"). Estos servicios pueden incluir alternativas más allá de éxito o fallo binarios.

Finalmente, el servicio de servidor de CAPTCHA obtendrá, o bien desde el software de CAPTCHA o bien desde la aplicación web en la que el reto CAPTCHA se presentó, un mensaje indicando si la cadena de CAPTCHA se introdujo o no correctamente, o si el reto CAPTCHA se ha automatizado o retransmitido. Este resultado de análisis se almacenará con la etiqueta de usuario. La Máquina de Servicio almacenará la etiqueta de usuario y el resultado de análisis. Además, la Máquina de Servicio puede obtener y almacenar detalles tal como los atributos de dispositivo recogidos, el URL de la CAPTCHA, el nombre de sitio y una indicación de tiempo.

Posteriormente, cuando la Máquina de Servicio se consulta por una aplicación web, y pregunta si mostrar o eliminar un reto CAPTCHA para un cliente final identificado que tiene una etiqueta de usuario, la Máquina de Servicio buscará la respectiva etiqueta de usuario en la base de datos de SM para determinar si se ha configurado una regla de historial de cliente final, en el bloque 100 de decisión. La Máquina de Servicio también puede recoger atributos de dispositivo adicionales de cliente final, como se ha descrito anteriormente, para comparar todos o algunos de los atributos con los recogidos con la primera grabación guardada cuando se asignó la etiqueta de usuario original al cliente final identificado. Si se encuentra una coincidencia, la Máquina de Servicio recuperará la regla de historial de dispositivo de cliente final establecida y aplicará reglas en el historial, en la etapa 102, mediante las cuales responderá finalmente si mostrar o eliminar un reto CAPTCHA al cliente final identificado.

Como se desvela en la presente invención, la información usada para concluir si una CAPTCHA debería mostrarse a un cliente final con un historial grabado se basa preferentemente en los siguientes artículos de datos en un historial del usuario: (i) los resultados de análisis de condición de las pruebas de CAPTCHA anteriores; (ii) la relación entre pruebas de CAPTCHA satisfactorias y falladas en el historial del cliente final, o en un intervalo del historial reciente (tal como la relación en últimos intentos o últimas horas/días); (iii) la cantidad de CAPTCHA enfrentados por el cliente final durante recientes intervalos de tiempo, tal como los últimos 10 segundos, el último minuto, la ultima hora, etc., y los resultados de los enfrentamientos (es decir, si las CAPTCHA se mostraron realmente u ocultaron mediante la Eliminación de CAPTCHA Condicional); y, (iv) la presencia de "convicciones" de automatización o retransmisión.

Además, se proporcionan reglas en un conjunto de reglas para concluir si una CAPTCHA debería mostrarse a un cliente final con un historial grabado. Estas reglas incluyen las siguientes: (i) si la cadena de CAPTCHA anteriormente mostrada no se introdujo nada o son se introdujo correctamente, debería mostrarse una CAPTCHA; (ii) si la cadena de CAPTCHA anteriormente mostrada se introdujo correctamente, debería mostrarse una nueva CAPTCHA únicamente en los siguientes casos: (a) si se excedió un cierto umbral de retos CAPTCHA por intervalo de tiempo dado (por ejemplo, más de un reto CAPTCHA en los últimos 10 segundos), o (b) si la relación entre pruebas de CAPTCHA falladas y satisfactorias en todo el historial o reciente historial limitada a un número de pruebas o tiempo, supera un umbral predefinido (por ejemplo, siete pruebas falladas de los diez retos más recientes sería una relación de historial que supera un valor predefinido de cinco pruebas falladas por diez retos), o (c) si se encontrasen convicciones de automatización o retransmisión de CAPTCHA en el historial del usuario, o (d) una porción reciente de convicciones que superan un cierto umbral (por ejemplo, dos informes de automatización en un día superando un umbral de uno, o (e) un informe de retransmisión en el historial del cliente final, superando el umbral de cero).

En una realización ilustrativa, la Máquina de Servicio incluye el código otros medios para conectar a terceras partes que retienen el historial del cliente final, habitualmente a través de API ofrecida por esas terceras partes. Tales terceras partes pueden ser entidades, que colocan cookies en muchas máquinas de usuario en muchos sitios web diferentes (conocidas como "cookies de tercera parte"), y registra las visitas de usuarios y acciones para sus necesidades, tal como, y sin desear ser limitante, publicidad dirigida. Estas terceras partes pueden rastrear a clientes finales y recoger su historial visible para fines tal como el análisis de los hábitos de los usuarios para ayudar a publicistas y/o editores a decidir que anuncios son más adecuados para cada usuario. Como puede apreciarse por un experto en la materia, es posible determinar si un cierto cliente final se ha rastreado mediante un servicio de este tipo, y si el usuario final tiene un historial grabado como consecuencia. Esta determinación puede hacerse a través

de la API u otros procedimientos de comunicación proporcionados por estos proveedores para conseguir la información que ofrecen.

La Máquina de Servicio incluirá, por lo tanto, el código o medios para conseguir información acerca de un cierto dispositivo de usuario final o navegador de estas terceras partes y, a base de la información, establecerá si el cliente final tiene un conjunto de reglas de historial de uso de Internet grabado y, si es posible, desde cuando está este historial, en el bloque 104 de decisión. Puede asumirse que agentes automatizados no tienen cookies de terceras partes ni conjunto de reglas de historial, o al menos no un historial más largo que de unos pocos días, ya que borran las cookies, caché y cualquier historial de navegación para mantener un total anonimato. La comprobación de historial de usuario de tercera parte se aplicará a dispositivos desconocidos (sin cookie de etiqueta o etiqueta desconocida) y su resultado se guardará en una base de datos o un almacenamiento, con la recientemente asignada etiqueta de usuario.

Además, sitios web populares que registran datos e identidad del cliente final también pueden consultarse, a través de API o cualquier otro medio proporcionado o disponible, para establecer si el cliente final tiene una cuenta en ese sitio web y, en la medida de lo posible, cómo de veterana es la cuenta y cuando se usó. Tales sitios web de terceras partes pueden ser, sin desear ser limitante, redes sociales, plataformas de correo por web, suministradores de inicio de sesión generales tal como el proyecto de openID y otros. Teniendo cuentas en esos sitios web y el uso real de la cuenta puede indicar un cliente humano válido que tiene un papel activo en otros sitios web populares y que no borra cookies y caché. Estas comprobaciones de historial de usuario de terceras partes se aplican a dispositivos desconocidos (sin cookie de etiqueta o etiqueta desconocida) y sus resultados se guardan en una base de datos de SM o un almacenamiento, con la etiqueta de usuario recientemente asignada.

Algunos sitios de terceras partes, tal como redes sociales o otras plataformas, pueden requerir un consentimiento del usuario para transmitir datos a la Máquina de Servicio. Tal consentimiento puede proporcionarse embebiendo una rutina o una porción de una página (conocido como "artilugio" y también conocido en Facebook como "aplicación de facebook ") del sitio de tercera parte, o redirigiendo al usuario al sitio de tercera parte en una página específica, tal como una página de aplicación o a página de fans creada para el fin de autorización del servicio de Eliminación de CAPTCHA Condicional. En cada una de estas alternativas, el cliente final debería iniciar sesión en el sitio de tercera parte y, clicando en una cierta casilla de verificación o cualquier botón requerido, debería confirmar detalles reveladores o exponer la cuenta personal a la Máquina de Servicio. En tales casos, el servidor de Eliminación de CAPTCHA Condicional puede incluir el código requerido para acompañar al usuario a través del procedimiento de confirmación del servicio de CAPTCHA.

En una realización ilustrativa, la presente invención puede incluir una explotación de navegador bien conocida, conocida como "explotación de CSS," en la que los enlaces a sitios web se sirven al navegador con una rutina que comprueba el atributo de color de los enlaces. Los navegadores aplican diferentes colores a enlaces nuevos y enlaces visitados, por lo tanto puede saberse si un usuario visitó ciertas direcciones web por su color. Junto con la CAPTCHA, la página o servidor de códigos por la Máquina de Servicio pueden incluir enlaces a sitios web más populares o imágenes en estos sitios web, para ver si se ha visitado o no, utilizando la explotación de CSS. Visitas a esos sitios web también pueden servir como una pista de que el cliente final es humano y no está ocultando el historial de navegación.

Una alternativa a esta explotación, que ya está bloqueada en algunos navegadores, puede ser embeber imágenes populares (tal como URL de logotipos de sitios web populares) en la página web y medir, a través de una rutina de lado de cliente que contiene un temporizador y un evento de onLoad, su tiempo de carga. Esto puede usarse para determinar si las imágenes populares se cargan desde la caché local (que normalmente tardaría unos pocos milisegundos) o desde la Internet, siendo un caché una indicación de que el sitio web se ha visitado. Estas comprobaciones de historial de navegación se aplican a dispositivos de cliente final desconocidos (sin cookie de etiqueta o etiqueta desconocida), y sus resultados se guardan en una base de datos o un almacenamiento, con la etiqueta de usuario recientemente asignada.

Cuando la Máquina de Servicio se consulta por una aplicación web, y pregunta si mostrar o eliminar un reto CAPTCHA para un cierto usuario que no tiene etiqueta de usuario, o tiene un etiqueta de usuario que no puede validarse en la base de datos de SM, la Máquina de Servicio o bien (i) responderá que un reto CAPTCHA debería mostrarse, o bien, (ii) si la Eliminación de CAPTCHA Condicional se configura de forma diferente, ya sea globalmente o por cierto sitio web, la Máquina de Servicio usará alguna o toda la siguiente información para concluir si una CAPTCHA debería mostrarse a un cliente final: (a) el historial del cliente final con rastreadores de cookies de terceras partes, (b) la disponibilidad de cuenta del cliente final, (c) uso en plataformas web de terceras partes, tal como redes sociales, plataformas de identidad o plataformas correo por web, y (d) el historial de navegación del cliente final en sitios web populares, tal como obtenidos a través de explotación de CSS o imágenes en caché.

En una realización ilustrativa, cuando la Máquina de Servicio se consulta por una aplicación web, en el bloque 104 de decisión, y pregunta si mostrar o eliminar un reto CAPTCHA para un cierto cliente final que no tiene etiqueta de usuario, o tiene una tarjeta de usuario que no puede validarse en la base de datos de SM, la Máquina de Servicio aplicará reglas para decidir que un reto CAPTCHA debería mostrarse porque el usuario no tiene un historial válido, en la etapa 92, o que el reto CAPTCHA no debería mostrarse porque el usuario sí tiene un historial válido, en la

etapa 94.

Tales reglas pueden establecerse de tal forma que: (i) si un cliente final ha visitado un número predefinido de sitios web populares, o (ii) si un cliente final un historial rastreado con rastreadores de cookies de terceras partes, o (iii) este historial rastreado es más largo de un número predefinido de días, o (iv) si un cliente final tiene cuentas en plataformas web populares, o (v) si el cliente final ha estado usando la cuenta en la actualidad, o (vi) cualquier combinación de estas, se supondrá que el cliente final es un usuario válido que tiene un historial de navegación de Internet visible y no es probable que sea un creador de correo basura. Si se cumple cualquiera de estas condiciones (i) a (vi), o una combinación predefinida de las mismas, la Máquina de Servicio señalizará que no debería mostrarse un reto CAPTCHA.

La Figura 4 ilustra una red 150, de acuerdo con una realización ilustrativa de la técnica presente. La red 150 es una realización ilustrativa de una plataforma en la que se proporciona un servicio de CAPTHA y/o procesa como se describe anteriormente con referencia a las Figuras 1-3. Por consiguiente, la red 150 es una red de comunicaciones adaptada para la conexión de diversos nodos, tal como servidores, sistemas informáticos y usuarios finales, así como para la facilitación de la transferencia de datos entre los nodos y usuarios finales. Además, la red 150 puede formarse de diversos sistemas informáticos y/o servidores especializados, alguno de los cuales puede funcionar como una agrupación informática y/o nube informática para proporcionar y distribuir servicios de CAPTCHA de acuerdo con realizaciones ilustrativas de la presente técnica.

Más específicamente, la Figura 4 ilustra, nodos/puntos de extremo/usuarios 152 y 154 finales, así como, servidores 156 y sistema 158 informático (CS). El usuario 152 y/o 154 puede ser ordenadores de cliente tal como ordenador personal (PC) doméstico o de oficina, un cliente remoto, un cliente liviano u otro tipo de ordenador y/o interfaz de procesamiento adaptada para el procesamiento general de datos y para la conexión a la red 150. Aunque no se ilustra mediante la Figura 1, los ordenadores cliente pueden acoplarse adicionalmente y/o conectarse a otros dispositivos periféricos, tal como monitores, teclados, ratones, impresoras, encaminadores, dispositivos inalámbricos, micrófonos, altavoces, cámaras, identificadores de huella digital, dispositivos de memoria externa y otros dispositivos. El PC 12 puede incluir plataformas de software y sistemas operativos, tales como Windows, Linux-Red Hat y otros programas de soporte.

Debería tenerse en cuenta que aunque la presente invención se describe con respecto a un "ordenador" en una "red informática", debería observarse que el término "ordenador" puede comprender cualquier dispositivo que consta de un procesador de datos y/o la capacidad de ejecutar una o más instrucciones. Tal dispositivo puede incluir, pero no limitarse a: un ordenador personal (PC), un servidor, un microordenador, un teléfono celular, un teléfono inteligente, un asistente de datos personal (PDA), un buscapersonas, un decodificador de TV, una consola de juegos, un reproductor de música digital, un cajero automático (ATM), un terminal de tarjeta de crédito de punto de venta (POS) o caja registradora electrónica. Cualquiera dos o más de tales dispositivos en comunicación con entre sí y/o cualquier ordenador en comunicación con otro ordenador puede constituir opcionalmente una "red informática."

Por lo tanto, usuarios, es decir, los usuarios 152 y 154 que tienen acceso a la red 10 pueden estar provistos de páginas web como parte de cualquier navegación general o búsqueda de la red 150. Debería tenerse en cuenta que la red 150 puede accederse por una pluralidad de usuarios, tal como los usuarios 152 y 154, formarse de diversos segmentos, ubicaciones, preferencias y/o otros atributos que caracterizan la conformación personal de la red usuarios.

Además, el servidor 156 y/o CS 158 pueden adaptarse para el almacenamiento, encaminamiento y/o comunicación de datos dentro de la red 150 y/o otras redes a las que pueden conectarse el servidor 156 y CS 18. Por lo tanto, el servidor 156 puede almacenar información relacionada con material incluido como parte del sitio web de vendedor, tal como los que pertenecen a ciertos anunciantes de vendedores, promotores, administradores y así sucesivamente. Como alternativa, el servidor 156 puede almacenar anuncios creados originalmente, así como parámetros que especifican la manera por la que deberían presentarse personalizados.

Además, en una realización ilustrativa, el servidor 156 puede ser del tipo disponible por Sun Microsystems, Hewlett Packard, Dell, International Business Machines (IBM) y/o otros vendedores de servidores y proveedores conocidos. Por consiguiente, el servidor 156 y CS 158 pueden incluir diversos dispositivos de hardware, tal como microprocesadores, tarjetas de memoria, tarjetas gráficas, encaminadores, dispositivos inalámbricos y otros módulos de recepción, transmisión y/o procesamiento de datos. Además, los servidores pueden incluir diversas plataformas de software y paquetes, tal como los que proporcionan código escrito en Java, Python, Ruby on Rails y/o otros lenguajes informáticos, para la facilitación de la operación y uso diarios del servidor 154 y CS 158 como parte de la red 150. Debería tenerse en cuenta adicionalmente que los nodos 152 y 154 de usuario y los servidores 156 y CS 158 son ilustrativos y que la red 150 puede incluir muchos otros nodos de usuario adicionales similares a los usuarios 152 y 154, así como, múltiples otros servidores similares a los analizados en el presente documento.

Además, el servidor 156 puede adaptarse para almacenar datos, tal como sitios web, generalmente accesibles para el usuario 152 y/o 154 a través de la red 150. Los expertos en la materia apreciarán que cada sitio web accesible, por ejemplo, para el usuario puede contener múltiples páginas web que también pueden ser accesibles para los usuarios 152 y 154 tras petición. Por ejemplo, el servidor 14 puede almacenar sitios web de empresas privadas y/o

corporaciones, así como organizaciones gubernamentales y/o otras organizaciones públicas. Por lo tanto, el servidor 154 proporciona acceso al usuario 12 de páginas web proporcionadas por las anteriormente mencionadas entidades privadas o públicas de modo que el usuario, por ejemplo, puede realizar negocios y/o gestionar diversas tareas a través de la red 150. Por ejemplo, el usuario 152 puede acceder al servidor 154 para la descarga de una página web que pertenece a un vendedor a través de la que el usuario 12 puede realizar transacciones financieras tal como cuando se adquieren artículos de consumo o similares. Mediante ejemplo adicional, el usuario 152 puede acceder al servidor 14 para la descarga de páginas web, tal como las asociadas con diversas instituciones públicas, a través de las que los usuarios 152 y 154 pueden proporcionar información personal y/o de otro tipo de para realizar asuntos personales diarios y/o de trabajo y así sucesivamente. Por consiguiente, los usuarios 152 y 154 puede formar generalmente sesiones de comunicación durante las que el usuario 152 y servidor 154 intercambian información a través de la red 150.

De acuerdo con realizaciones ilustrativas de la presente técnica, una sesión de CAPTCHA puede iniciarse por el CS 158, en el que una Máquina de Servicio puede implementarse. La Máquina de Servicio se adapta para devolver un ID de transacción y un código al servidor 156 web o aplicación web. Por consiguiente, el servidor 156 web o aplicación web emite una rutina al usuario 152/154. El usuario 154/156 final recibe la rutina de creación de una Iframe. La Máquina de Servicio (por ejemplo, CS 158) recibe una transmisión desde el usuario 152/154 final y consigue una etiqueta de usuario o aplica una etiqueta de usuario, en la etapa 20. La Máquina de Servicio se adapta adicionalmente para obtener los atributos del dispositivo 152/154 de usuario para generar imágenes y código.

Como se ha explicado anteriormente con referencia a las Figuras 1 y 2, el CS 158 se adapta para enviar el código de CAPTCHA al usuario 152/154 final. El usuario final obtiene el código de CAPTCHA, y solicita una imagen de CAPTCHA. El CS 158 recibe la petición de usuario y envía la imagen de CAPTCHA al usuario 152/154 final. Por consiguiente, el dispositivo de usuario final muestra una imagen parcial, registra eventos y envía el formulario al servidor 156 web o aplicación web. El servidor 156 web o aplicación web obtiene las entradas del formulario, incluyendo los campos de CAPTCHA. El servidor 156 web o aplicación web a continuación consulta al CS 158 para validar la CAPTCHA.

Además, el CS 158 obtiene la CAPTCHA y los eventos de dispositivo de usuario (por ejemplo, usuarios 152/154). El CS a continuación genera un análisis de entradas de usuario, un análisis de eventos de dispositivo de usuario, análisis de historial de dispositivo de usuario. Los resultados y alertas de prueba de CAPTCHA resultantes se devuelven al dispositivo de usuario 152/154 final mediante el CS 158. El dispositivo de usuario final recibe los resultados y alertas de prueba de CAPTCHA desde el CS 158.

En otra realización ilustrativa de la presente técnica, el sistema de red 150 se adapta para la implementación de un procedimiento de retar selectivamente a un usuario 152/154 con una prueba de Turing pública automatizada al usuario 152/154 en respuesta a una comunicación del usuario 152/154. Por consiguiente, cuando el usuario 152/154 accede a un sitio web, tal como uno hecho disponible por el servidor 156, el CS 158 se adapta para comprobar la existencia de un identificador de usuario. Si el CS 158 está provisto de un identificador del usuario 152/154, el CS 158 verifica que dicho identificador de usuario devuelto es genuino y no un identificador robado. Además, si no se devuelve el identificador de usuario, el CS 158 asigna un identificador de usuario al usuario. Posteriormente, el CS 158 presenta la prueba de Turing pública automatizada al usuario a no ser que criterios predeterminados, tal como los relacionados con el atributo e historial de usuario 152/154, como se exponen anteriormente con referencia a la Figura 3. Además, el CS 158 se adapta para obtener y almacenar un análisis de la respuesta del usuario a la prueba de Turing pública automatizada.

A menos que se defina de otra manera, todas las expresiones técnicas o científicas usadas en el presente documento tienen el mismo significado como se entiende comúnmente por un experto en la materia a la que pertenece la presente invención. Los materiales, procedimientos, y ejemplos proporcionados en el presente documento son ilustrativos únicamente y no pretendes ser limitantes.

Muchos de los detalles específicos de ciertas realizaciones de la invención se exponen en la anterior descripción y dibujos relacionados para proporcionar un completo entendimiento de tales realizaciones. Un experto en la materia entenderá, sin embargo, que la presente invención puede practicarse sin varios de los detalles descritos en la anterior descripción. Además, en la descripción, se entiende que las figuras relacionadas con las diversas realizaciones no deben interpretarse para transmitir ninguna dimensión física específica o relativa.

REIVINDICACIONES

1. Un procedimiento de administración de un reto CAPTCHA y de detección del uso de un robot o retransmisor de CAPTCHA por un ordenador cliente, que comprende, mediante un servidor:

proporcionar un reto CAPTCHA al ordenador cliente (30), comprendiendo el reto CAPTCHA una imagen y código de navegador para visualizar la imagen, comprendiendo la imagen una cadena de caracteres en la que una primera subcadena más pequeña que dicha cadena corresponde a una solución al reto CAPTCHA y al menos una segunda subcadena más pequeña que dicha cadena corresponde a caracteres extra que no son parte de la solución, funcionando el código de navegador para restringir la visualización de la imagen en el ordenador cliente para únicamente la primera subcadena (32), recibir una respuesta desde el ordenador cliente indicativa de una solución al reto (34) CAPTCHA, comparar la respuesta con la al menos una segunda subcadena, y determinar, si la respuesta incluye la al menos una segunda subcadena, que el ordenador cliente usó un robot o retransmisor de CAPTCHA.

2. El procedimiento de la reivindicación 1, en el que dicho reto CAPTCHA comprende capacidad de animación de tal forma que en cualquier momento dado una porción variante de la primera subcadena está oculta a la vista en la pantalla del ordenador cliente.

3. El procedimiento de la reivindicación 1, que comprende además evaluar al menos uno de: un número de eventos de enfoque de elementos de formulario realizados por el ordenador cliente, un número de eventos de ratón realizados por el ordenador cliente y un número de eventos de teclado realizados por el ordenador cliente.

4. El procedimiento de la reivindicación 1, que comprende además comparar la dirección IP del ordenador cliente con una dirección IP asociada con dicha respuesta.

5. El procedimiento de la reivindicación 1, que comprende además determinar si existe una iFrame en el ordenador cliente, y si es así, determinar el URL de dicha iFrame; y verificar el URL asociado con un documento padre de dicha iFrame.

6. Un programa informático almacenado en un medio de almacenamiento legible por ordenador, que cuando se ejecuta implementa el procedimiento como se describe en una cualquiera de las reivindicaciones 1-5.

7. Un sistema de administración de un reto CAPTCHA y de detección del uso de un robot o retransmisor de CAPTCHA por un ordenador cliente, que comprende un servidor configurado para realizar el procedimiento como se describe en una cualquiera de las reivindicaciones 1-5.

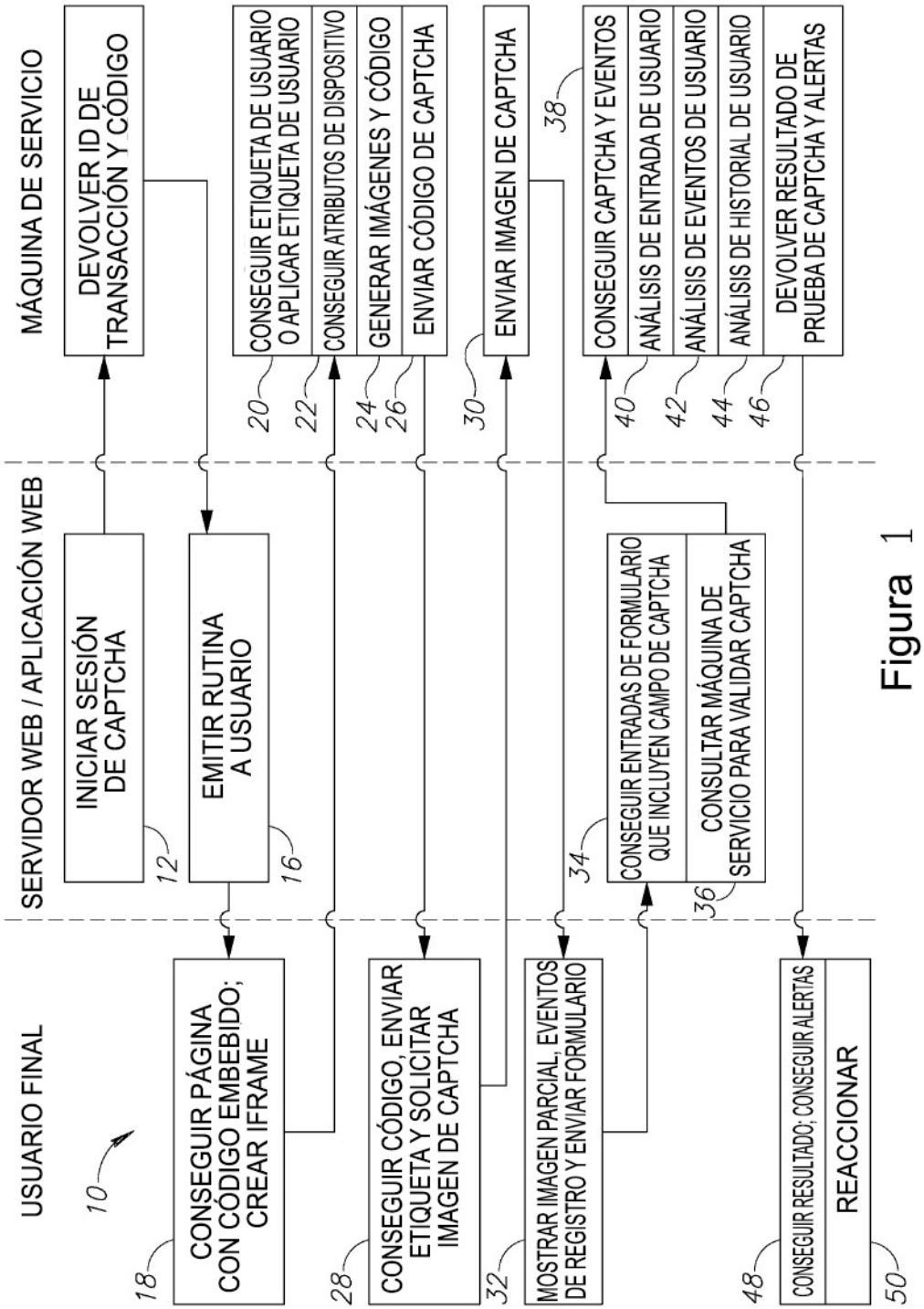
USUARIO FINAL
SERVIDOR WEB / APLICACIÓN WEB
MÁQUINA DE SERVICIO
10
INICIAR SESIÓN DE CAPTCHA
12
DEVOLVER ID DE TRANSACCIÓN Y CÓDIGO
EMITIR RUTINA A USUARIO
16
CONSEGUIR PÁGINA CON CÓDIGO EMBEBIDO; CREAR IFRAME
18
CONSEGUIR ETIQUETA DE USUARIO O APLICAR ETIQUETA DE USUARIO
20
CONSEGUIR ATRIBUTOS DE DISPOSITIVO
22
GENERAR IMÁGENES Y CÓDIGO
24
ENVIAR CÓDIGO DE CAPTCHA
26
CONSEGUIR CÓDIGO, ENVIAR ETIQUETA Y SOLICITAR IMAGEN DE CAPTCHA
28
ENVIAR IMAGEN DE CAPTCHA
30
MOSTRAR IMAGEN PARCIAL, EVENTOS DE REGISTRO Y ENVIAR FORMULARIO
32
CONSEGUIR CAPTCHA Y EVENTOS
38
ANÁLISIS DE ENTRADA DE USUARIO
40
ANÁLISIS DE EVENTOS DE USUARIO
42
ANÁLISIS DE HISTORIAL DE USUARIO
44
DEVOLVER RESULTADO DE PRUEBA DE CAPTCHA Y ALERTAS
46
CONSEGUIR ENTRADAS DE FORMULARIO QUE INCLUYEN CAMPO DE CAPTCHA
34
CONSULTAR MÁQUINA DE SERVICIO PARA VALIDAR CAPTCHA
36
CONSEGUIR RESULTADO; CONSEGUIR ALERTAS
REACCIONAR
48
50

Figura 1

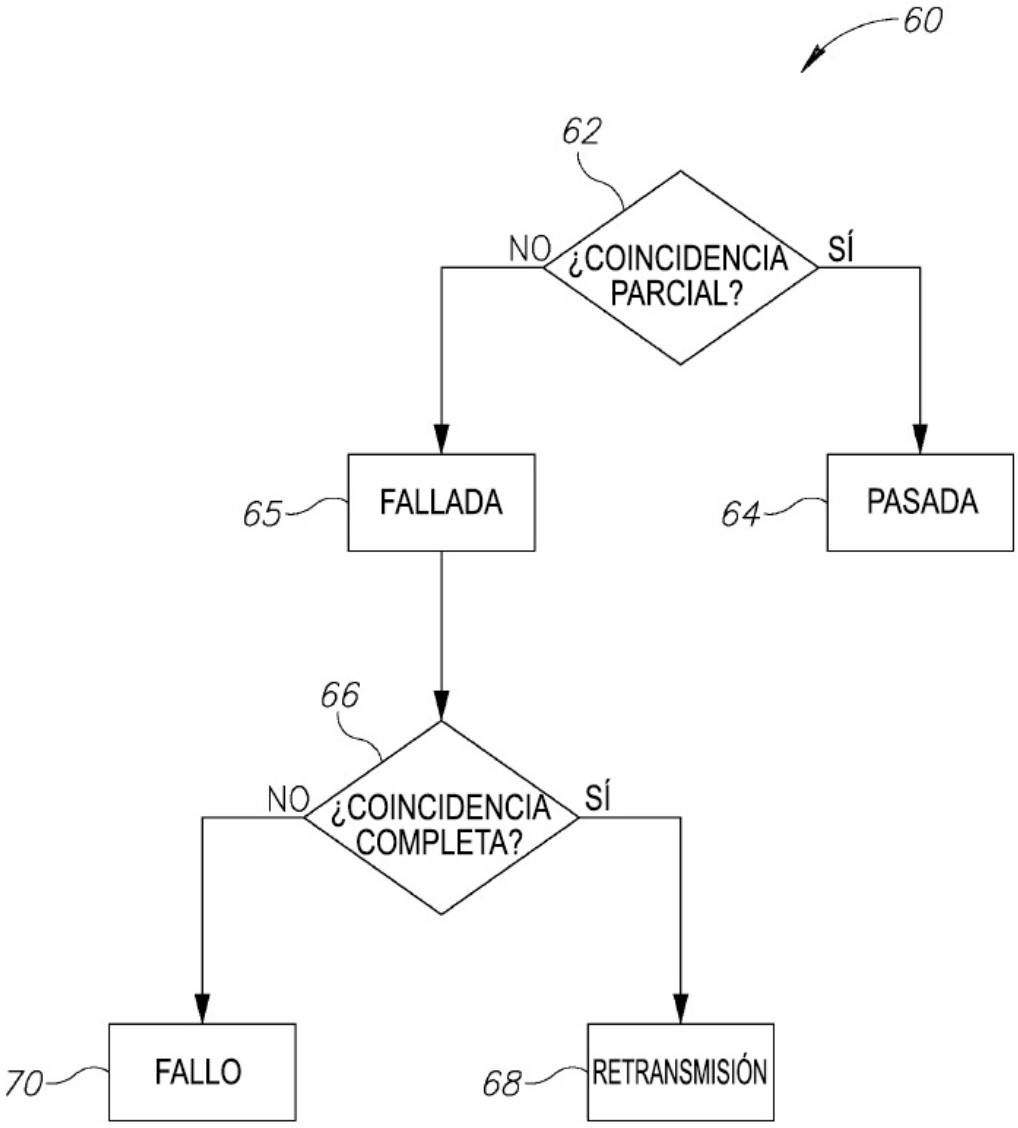
60
62
NO
¿COINCIDENCIA PARCIAL?
SÍ
65
FALLADA
64
PASADA
66
NO
¿COINCIDENCIA COMPLETA?
SÍ
70
FALLO
68
RETRANSMISIÓN

Figura 2

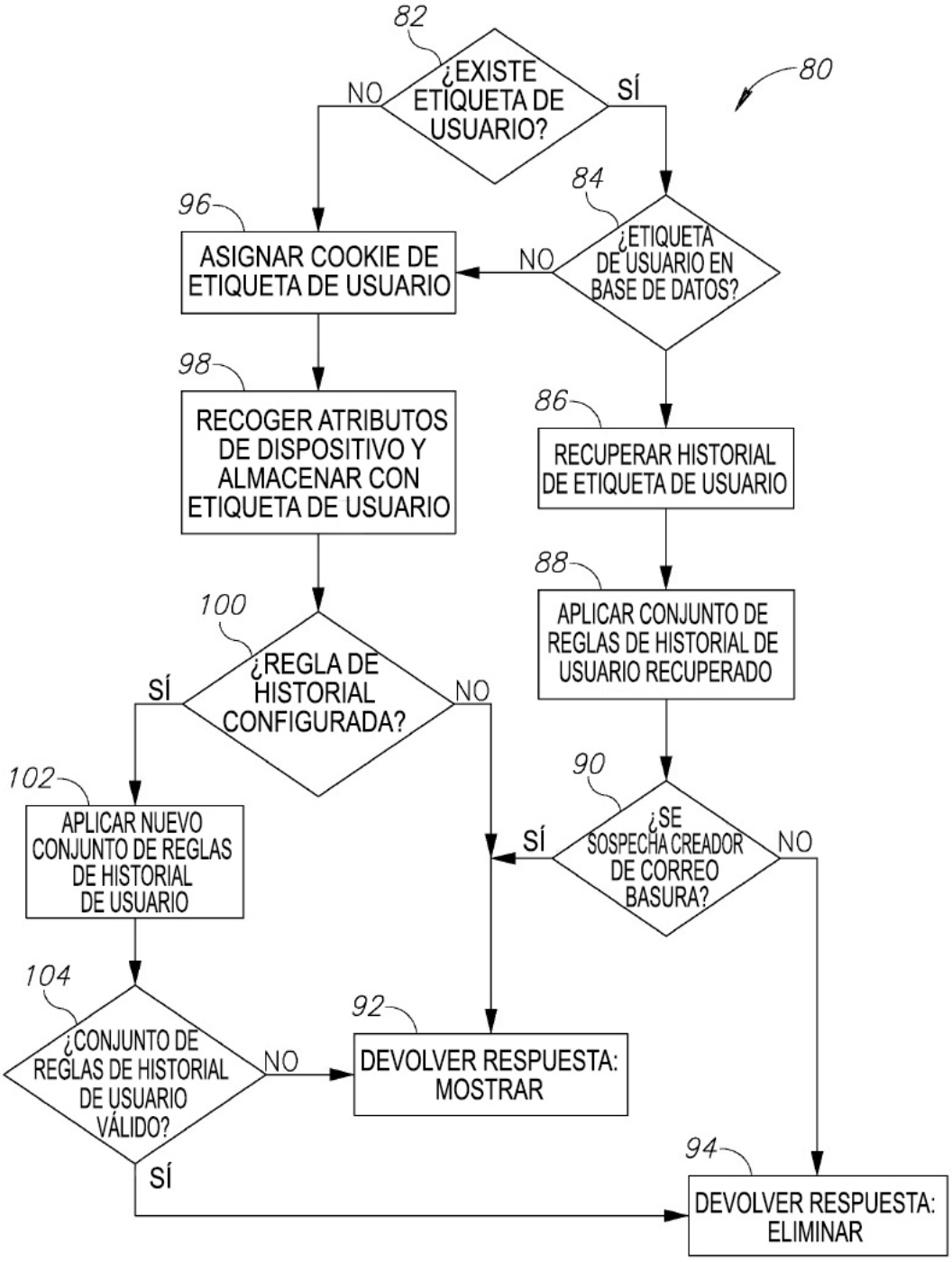
82
¿EXISTE ETIQUETA DE USUARIO?
NO
SÍ
80
84
¿ETIQUETA DE USUARIO EN BASE DE DATOS?
NO
96
ASIGNAR COOKIE DE ETIQUETA DE USUARIO
98
RECOGER ATRIBUTOS DE DISPOSITIVO Y ALMACENAR CON ETIQUETA DE USUARIO
86
RECUPERAR HISTORIAL DE ETIQUETA DE USUARIO
88
APLICAR CONJUNTO DE REGLAS DE HISTORIAL DE USUARIO RECUPERADO
100
¿REGLA DE HISTORIAL CONFIGURADA?
SÍ
NO
102
APLICAR NUEVO CONJUNTO DE REGLAS DE HISTORIAL DE USUARIO
90
¿SE SOSPECHA CREADOR DE CORREO BASURA?
SÍ
NO
104
¿CONJUNTO DE REGLAS DE HISTORIAL DE USUARIO VÁLIDO?
NO
92
DEVOLVER RESPUESTA: MOSTRAR
SÍ
94
DEVOLVER RESPUESTA: ELIMINAR

Figura 3

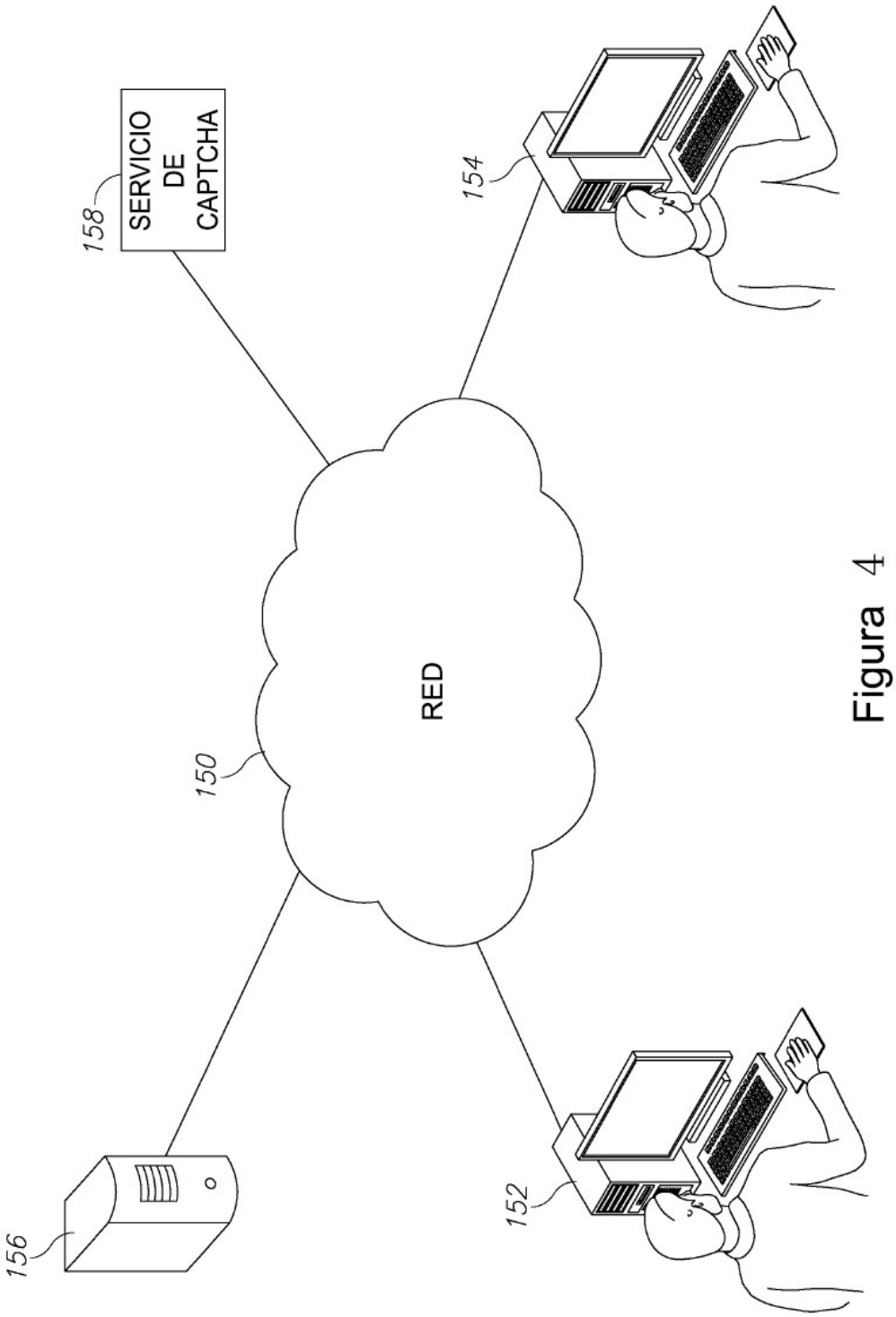

Figura 4