(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 359 466**

(51) Int. Cl.:
G06F 21/20 (2006.01)
H04L 29/06 (2006.01)
G06F 17/30 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07857501 .6**
(96) Fecha de presentación : **12.12.2007**
(97) Número de publicación de la solicitud: **2104901**
(97) Fecha de publicación de la solicitud: **30.09.2009**

(54) Título: **Método y aparato para detectar fraude informático.**

(30) Prioridad: **16.01.2007 US 623516**

(45) Fecha de publicación de la mención BOPI:
23.05.2011

(45) Fecha de la publicación del folleto de la patente:
23.05.2011

(73) Titular/es: **INTERNATIONAL BUSINESS MACHINES CORPORATION**
New Orchard Road
Armonk, New York 10504, US

(72) Inventor/es: **Reumann, John y**
Verma, Dinesh

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Campo de la Invención

La presente invención se refiere generalmente a la tecnología de la información, y, más concretamente, a un método y aparato para detectar fraude informático.

Antecedentes de la Invención

Cuando un usuario recibe un correo electrónico u otra comunicación que parece contener un enlace a un sitio web "A", pero se redirecciona a una versión suplantada del sitio web "A", el usuario se dice que es objeto de un ataque de "suplantación de identidad" del sitio web. A los usuarios les gustaría saber si un sitio que están visitando es un sitio bien conocido, legítimo, o un sitio que parece un sitio legítimo pero no está situado en la misma ubicación que la versión legítima esperada del sitio web.

Un usuario puede iniciar una transferencia de una página web en un navegador escribiendo el URL, siguiendo un enlace, siguiendo un enlace integrado en un correo electrónico o en una sesión de mensajería instantánea, o a través de una redirección desde otra página. Como resultado, el navegador resolverá el protocolo que va a ser usado para buscar la página destino, contactará el sistema de nombre de dominio (DNS) para resolver el ordenador central de destino, conectará a la dirección del protocolo de internet (IP) nombrado por la búsqueda del DNS, descargará el contenido de la página, entregará la página y ejecutará simultáneamente cualesquiera secuencias de comandos donde sea adecuado. El contenido de esta página se puede falsificar de muchas formas.

Hay conocidas barras de herramientas del navegador que meramente extraen el localizador de recursos uniforme (URL) a partir del navegador web y lo normalizan para presentar al usuario el sitio efectivo al cual se conecta. Mientras que esto puede eliminar los ataques en los que un URL rebosa la ventana de localización del navegador reduciendo el nombre del sitio, no resuelve el problema en el que están siendo usados dos nombres de dominio de aspecto muy similar. Dado que la información sobre los sitios efectivos es bastante tosca, es posible para un atacante obtener un nombre de dominio de aspecto cercano en la misma geografía (por ejemplo Estados Unidos) y entonces intentar confundir tales detectores de suplantación de identidad. Adicionalmente, con la globalización en aumento, es bastante probable, por ejemplo, que un sitio legítimo para un banco con base en EE.UU. esté situado en otro país tal como, por ejemplo, India o Brasil, lo cual dirige a varias falsas alarmas. Usando las técnicas conocidas, el usuario todavía sería conducido a creer que está contactando con el sitio web correcto. Las técnicas conocidas confían en el usuario comprobar el nombre de dominio para cada sitio web visitado. Adicionalmente, las técnicas conocidas solamente extraen la información entregada en el URL real, y por lo tanto, estas técnicas no son seguras en el caso de ataques de envenenamiento del DNS, en el que los nombres de dominio reales se fuerzan a resolver una dirección IP del sitio corrupto que es distinta del objetivo que el usuario pretendió cuando escribió el nombre en la barra de localización del navegador.

La US 2004/123157 A1 y la EP 1 681 825 A revelan las técnicas de detección de suplantación de identidad en base a comparar las direcciones de destino y los contenidos frente a los datos almacenados, válidos.

La WO 2006/018647 revela los mecanismos para la autentificación de los proveedores de contenidos verificando la correspondencia del URL y las direcciones IP.

La WO 2006/026921 A revela los sistemas y métodos de detección de la suplantación de identidad. Algunas realizaciones implican obtener una reproducción gráfica de un destino, derivando una versión de texto de dicha reproducción gráfica y comparar dicho texto frente a las versiones de texto de los destinos válidos almacenados.

Sería deseable de esta manera superar las limitaciones en los planteamientos previos.

Resumen de la Invención

Los principios de la presente invención proporcionan técnicas para detectar el fraude informático. Un método ejemplar (que se puede implementar por ordenador) para detectar el fraude informático, de acuerdo con un aspecto de la invención, puede incluir los pasos de obtener una versión de texto de un destino candidato y una reproducción gráfica del destino candidato, comparando la versión de texto y la reproducción gráfica del destino candidato con una versión de texto correspondiente y una reproducción gráfica correspondiente de un destino almacenado, y generar un aviso de fraude si la reproducción gráfica del destino candidato es considerablemente similar a la reproducción gráfica del destino almacenado mientras que la versión de texto del destino candidato difiere considerablemente de la versión de texto correspondiente del destino almacenado.

En un aspecto de la invención, el destino candidato y el destino almacenado se representan como los URL. También, en otro aspecto de la invención, las técnicas para detectar el fraude informático se ejecutan automáticamente tras cargar una página web asociada con un destino candidato. Las técnicas también se pueden ejecutar usando un botón que se muestra a un usuario en al menos una de una ventana y una barra de estado externa para una ventana del navegador asociada con el destino candidato. Adicionalmente, en otro aspecto de la invención, se puede generar un aviso de fraude a través de una sugerencia visual visualizada por un usuario en al menos una de una ventana y una barra de

estado externa para una ventana del navegador asociada con el destino candidato. En otro aspecto de la invención, el destino candidato se identifica como limpio si todas las organizaciones determinadas coinciden con una organización almacenada correspondiente y si la organización almacenada no es considerablemente similar a otra organización clasificada como más popular en una base de datos. El destino candidato se identifica como desconocido si las referencias visuales pueden no encajar con una organización, pero para el cual el destino candidato coincide con un URL visual y destino poco probable que sea un destino de suplantación de identidad.

Un método ejemplar de generación de una base de datos, o lista blanca, de destinos a ser protegidos frente a fraude informático puede incluir los pasos de generar al menos una categoría de destinos a ser protegidos, y recuperar al menos una lista de destinos que pertenecen a al menos una categoría. El paso de recuperar al menos una lista de destinos que pertenecen a al menos una categoría comprende obtener una primera lista de destinos y una segunda lista de destinos, y fusionar las primera y segunda listas de destinos. También el paso de recuperación comprende el acceso a un motor de búsqueda de Internet y/o el acceso a un servicio de indexación de Internet.

Al menos una realización de la invención se puede implementar en forma de un producto informático que incluye un medio utilizable por ordenador con código de programa utilizable por ordenador para realizar los pasos del método indicados. Adicionalmente, al menos una realización de la invención se puede implementar en la forma de un aparato que incluye una memoria y al menos un procesador que se acopla a la memoria y operativo para realizar los pasos del método ejemplar.

Al menos una realización de la invención puede proporcionar uno o más efectos técnicos beneficiosos, tales como, por ejemplo, detectar el fraude informático cuando el candidato o la entidad de suplantación de identidad comprende un nombre de dominio que es de aspecto muy similar a aquél de una entidad prevista o almacenada. También, al menos una realización de la invención puede proporcionar el efecto beneficioso de detectar el fraude informático en situaciones en las que un nombre de dominio previsto se fuerza a resolver un destino candidato o de suplantación de identidad que es distinto del objetivo que un usuario pretendió cuando el usuario escribió el nombre en la barra de localización del navegador.

Estos y otros objetos, rasgos y ventajas de la presente invención llegarán a ser evidentes a partir de la siguiente descripción detallada de las realizaciones ilustrativas de la misma, la cual va a ser leída en conexión con los dibujos anexos.

Breve descripción de los dibujos

La FIG. 1 s un diagrama de flujo que ilustra un método ejemplar para detectar el fraude informático, de acuerdo con un aspecto de la invención;

La FIG. 2 es un diagrama de bloques que ilustra un sistema ejemplar que puede ejecutar un método ejemplar para detectar el fraude informático, de acuerdo con otro aspecto de la invención;

La FIG. 3 es un diagrama de flujo que ilustra un método ejemplar para generar una base de datos de destinos a ser protegidos frente al fraude informático, de acuerdo con otro aspecto de la invención; y

La FIG. 4 es un diagrama del sistema de un sistema informático ejemplar en el que se puede implementar al menos una realización de la presente invención.

Descripción detallada de las realizaciones preferidas

Una realización de la invención construye al menos una firma del sitio en base a qué puede ver el usuario en su ventana del navegador. Un agente del programa informático que computa estas firmas mantiene también una base de datos, o una lista blanca, de gráficos bien conocidos y otras firmas para los sitios web. Siempre que las firmas se computan para un sitio, se comparan frente a las firmas en la base de datos. Si algunas firmas coinciden con aquéllas de sitios bien conocidos mientras que otras firmas o bien no están registradas o bien coinciden con fuentes de ataques de suplantación de identidad (por ejemplo, ciertos nombres de dominio, propiedad de direcciones IP), la puntuación de la suplantación de identidad del sitio aumentará y la barra de estado del navegador presentará un símbolo para indicar el riesgo de suplantación de identidad (por ejemplo, <><).

Una forma común de los ataques de suplantación de identidad comprende incluir un enlace a un sitio que parece ser del sitio web “A”, pero en realidad apunta a algún otro sitio web. Con codificación de texto enriquecido y Lenguaje de Marcado de Hipertexto (HTML) del correo electrónico, un enlace típicamente se puede representar usando la siguiente sintaxis o equivalente:

 Texto Visualizado por el Usuario

En la mayoría de los lectores, solamente se muestra a un usuario la cadena marcada “Texto Visualizado por el Usuario”, y el “enlace objetivo” no se muestra. Mientras que algunos usuarios realmente pueden examinar el enlace, se hace algún esfuerzo para disfrazar el enlace de manera que el “enlace objetivo” parece que es un poco similar al enlace para

el sitio real que estaría indicado como “Texto Visualizado por el Usuario”. Algunos ejemplos de este tipo de enmascaramiento se proporcionan debajo.

A modo de ejemplo solamente, un correo electrónico puede contener un enlace integrado Acme Investments y de esta manera puede pretender venir desde el sitio web de Acme Investments, http://www.acmeinvestments.com. Cuando el usuario introduce este enlace en el navegador, es llevado al sitio www.acme1nvestments.com. A menos que el usuario sea lo bastante diligente para advertir que la letra novena en el URL es un 1 (uno numérico) en lugar de una “i”, creerá equivocadamente que está en el sitio web de Acme Investments.

Un caso malicioso particular de tal suplantación se hace posible debido a los estándares de codificación de caracteres en múltiples idiomas. Este estándar, el Nombres de Dominio Internacionalizados permite representar los nombres de dominio (el nombre de la máquina en el URL) que usan caracteres unicódigo en idiomas distintos del inglés. Por ejemplo, el carácter unicódigo U+0430, una letra minúscula Cirílica (“a”), puede parecer idéntica al carácter unicódigo U+0061, una letra minúscula Latina, (“a”) que es la “a” minúscula usada en inglés. De esta manera, un correo electrónico de suplantación de identidad puede referirse a un URL www.<a>cmeinvestments.com donde <a> se refiere a la letra minúscula Cirílica a, pero el usuario de un sitio web no sería capaz de distinguirla del URL de www.acmeinvestments.com. Varios navegadores son vulnerables a tales enmascaramientos.

Hay otras formas de engañar a un usuario para ir a un sitio web distinto de aquél al que uno pretende ir, que incluyen esquemas que comprometen el sistema de nombre de dominio (por ejemplo, se podría usar un virus para sobrescribir el archivo de los ordenadores centrales o la caché del navegador). No obstante, tal ataque requiere comprometer la seguridad de una máquina, y es menos probable que sea usado. Ejemplos de ataques de esta naturaleza se describen en los párrafos siguientes para la integridad. Por lo general, las técnicas de suplantación de identidad confían en engañar al usuario acerca de acceder a un URL distinto, dado que se puede hacer por medio de un correo electrónico engañoso sin ataques sofisticados en la seguridad del sistema operativo.

Por ejemplo, una forma en que la página se puede falsificar es a través de un ataque en el paso señalado arriba para resolver el protocolo que va a ser usado para buscar la página de destino. Es posible redirigir al usuario a una página en el propio disco duro del usuario apuntando el navegador a una referencia “file:/”. Este tipo de redirección puede ser especialmente peligroso porque elude la mayoría de los mecanismos de seguridad del navegador. El atacante puede ser capaz de colocar el código en el sistema de archivos del usuario en una ubicación conocida (por ejemplo, en la caché del navegador).

Otra forma, por ejemplo, de que la página se pueda falsificar es a través de un ataque en el paso señalado anteriormente al contactar el DNS para resolver el ordenador central de destino. El atacante puede “envenenar” un servidor de DNS para redireccionar al usuario a una dirección IP que se controla por el atacante en lugar de enviar el navegador a la ubicación solicitada. Por ejemplo, se podría dirigir a un usuario a la dirección IP 10.1.1.1 si la asignación de la dirección IP para www.acmeinvestments.com estuviera minada.

Como otro ejemplo, una forma de que la página pueda ser falsificada es a través de un ataque en el paso señalado anteriormente para conectar con la dirección IP nombrada por la búsqueda de DNS. Se puede iniciar una ocupación de la dirección IP mediante la redirección de las rutas o ataques de hombre en el medio donde el atacante se apropia de una máquina en el camino al objetivo real de la descarga de la página web. En estos casos, el atacante puede actuar como un intermediario y controlar e interceptar la entrada y/o salida (I/O) desde un navegador del usuario.

Todavía otra forma, por ejemplo, de que la página pueda ser falsificada es a través de un ataque en el paso señalado arriba para reproducir la página y ejecutar simultáneamente cualesquiera secuencias de comandos integrados donde sea adecuado. El atacante puede no ser capaz de ejecutar ninguno de los ataques señalados anteriormente y por lo tanto puede ser forzado a encubrir el hecho de que (el atacante) ha redireccionado al usuario al sitio web falsificado del propio atacante suplantando el aspecto del sitio web falsificado y ocultando la evidencia que muestra al usuario que no está navegando actualmente el sitio web que espera que va a navegar en base al contenido visionado en la ventana del navegador.

La FIG. 1 muestra un diagrama de flujo que ilustra un método para detectar el fraude informático, de acuerdo con una realización de la invención. El paso 102 incluye obtener una versión de texto de un destino candidato y una reproducción gráfica del destino candidato. Un destino candidato es una dirección de red o un Identificador de Recurso Universal (URI) o un Localizador de Recurso Uniforme (URL) a la que se dirige una parte de un mensaje. Una versión de texto del destino candidato es la reproducción del destino que usa una representación de texto estándar tal como, por ejemplo, ASCII o Unicódigo. Una reproducción gráfica es la representación del destino candidato en un formato de imagen, por ejemplo, como un formato gif, jpeg, o tiff. El paso 104 incluye comparar la versión de texto del destino candidato y la reproducción gráfica del destino candidato con, respectivamente, una versión de texto correspondiente de un destino almacenado y una reproducción gráfica correspondiente del destino almacenado. Un destino almacenado puede ser una dirección de red, URI o URL que se pretende que sea protegida frente al fraude y se mantiene en un repositorio en el ordenador. Tal repositorio puede ser un archivo de texto, una base de datos local, un archivo XML, etc. El paso 106 incluye generar un aviso de fraude si la reproducción gráfica del destino candidato es considerablemente similar a la reproducción gráfica del destino almacenado mientras que la versión de texto del destino candidato difiere

considerablemente de la versión de texto correspondiente del destino almacenado. Opcionalmente, el método ilustrado en la FIG. 1 también puede incluir el paso 108, que identifica una página del destino candidato como limpia si todas las organizaciones determinadas coinciden con una identificación (ID) y/o identidad de organización almacenada correspondiente en el repositorio y si la organización almacenada no es demasiado similar a otra organización que está clasificada como más popular en la base de datos del repositorio. El método ilustrado en la FIG. 1 también puede incluir opcionalmente el paso 110, que identifica la página del destino candidato como "origen desconocido" si las referencias visuales no podrían ser hechas coincidir con una organización, pero para la cual el destino candidato coincide con el URL visual y cuyo destino no es un destino de suplantación de identidad probable.

La FIG. 2 muestra un diagrama de bloques que ilustra un sistema ejemplar que puede ejecutar un método ejemplar para detectar el fraude informático, de acuerdo con una realización de la invención. El sistema 200 comprende los componentes que incluyen una base de datos, o repositorio, 202, el cual puede comprender al menos un destino bien conocido, direcciones IP, patrones o prefijos URL, marcas de contenidos (por ejemplo, logotipos), y registros de propiedad de direcciones IP. El sistema 200 también comprende un complemento anti suplantación de identidad 224, y un navegador 226. El sistema 200 también comprende los adecuados programas informáticos, componentes físicos, o mezcla de módulos de componentes físicos-programas informáticos para ejecutar los pasos del método como se describe debajo.

El paso 228 comprende una fase de análisis visual. El paso 228 puede incluir los pasos de reproducción del URL 204, la estimación del destino del URL 206, la extracción de las marcas de contenido 208, y la estimación del origen de contenidos 210. El paso 230 comprende un análisis físico. El paso 230 puede incluir los pasos de una prueba de origen de dirección IP 212, y la puntuación de similitud del nombre del DNS 214. El paso 216 incluye producir una puntuación de discrepancia visual a física. El paso 218 incluye producir la visualización de la puntuación. El paso 220 comprende un proceso alertador de suplantación de identidad, el cual puede incluir producir un desplegable de alerta de suplantación de identidad 222 en una ubicación al azar. Una ubicación al azar puede comprender generar un desplegable de aviso de fraude o alerta de suplantación de identidad 222 a través de una sugerencia visual visualizada por el usuario en al menos una de una ventana y una barra de estado externa para la ventana del navegador asociada con el destino candidato, en la que la ventana se abre en una ventana situada aleatoriamente separada del navegador para evitar ataques de superposición por los suplantadores de identidad.

Cuando un sitio web se reproduce completamente en el navegador, un agente del programa informático toma una instantánea de la información visualizada en la ventana del navegador. Esta instantánea incluye el contenido de la fuente que comprende, por ejemplo, las imágenes, el URL de la ubicación, y el texto visualizado. El agente del programa informático también toma una captura de pantalla de la imagen reproducida dentro del navegador.

Un aspecto de la invención es mantener una base de datos de los URL existentes conocidos objetivos para los ataques de suplantación de identidad, y la reproducción gráfica de esos URL, que usan un convenio predefinido. Las técnicas inventivas ejecutan los siguientes pasos en cada página web que se descarga o para la que el usuario inicia una comprobación. Las técnicas incluyen obtener una versión de texto de un destino candidato y una reproducción gráfica del destino candidato, comparando la versión de texto del destino candidato y la reproducción del destino candidato con, respectivamente, una versión de texto correspondiente de un destino almacenado y una reproducción gráfica correspondiente del destino almacenado, y generar un aviso de fraude si la reproducción gráfica del destino candidato es considerablemente similar a la reproducción gráfica del destino almacenado mientras que la versión de texto del destino candidato difiere considerablemente de la versión de texto del destino almacenado.

En una realización de la invención, el destino candidato y el destino almacenado se representan como URL. Las técnicas inventivas se pueden ejecutar automáticamente tras cargar una página web asociada con el destino candidato. También, las técnicas inventivas se pueden ejecutar usando un botón de prueba de suplantación de identidad que se muestra al usuario en la ventana o barra de estado externa a la ventana del navegador asociado con el destino candidato para evitar ataques de superposición por suplantadores de identidad. En otro aspecto de la invención, el paso de comparar la versión de texto y la reproducción gráfica del destino candidato con la versión de texto correspondiente y la reproducción gráfica del destino almacenado se realiza en un subconjunto del destino candidato y el destino almacenado, en donde un subconjunto puede comprender, por ejemplo, el prefijo y/o sufijo de un URL.

En un aspecto de la invención, las técnicas inventivas permiten a una página web que sea descargada a través de un navegador. Tras descargar exitosamente una página, pero antes de la ejecución de onLoad() Java y otras secuencias de comandos de la página, el complemento anti suplantación de identidad 224 extraerá el URL que se almacena en el campo de localización del navegador. El complemento 224 permite que la página sea reproducida completamente y extrae la ubicación del navegador visible tomando una imagen instantánea de la ventana del navegador. La función instantánea se usa, preferentemente, porque hay conocidos ataques en los que un sitio web de suplantación de identidad deshabilita la barra de herramientas del navegador y presenta la suya propia (por ejemplo, la versión JavaScript) del campo de ubicación al usuario.

El complemento 224 leerá el mapa de imágenes de la barra de herramientas del navegador asociada con el destino candidato y determinará una representación del carácter del mapa de imágenes usando un algoritmo de reconocimiento óptico de caracteres (OCR) para reconocimiento de caracteres. En un aspecto de la invención, las técnicas inventivas incluyen el análisis de la representación de los caracteres, y también la normalización de la representación de los

caracteres haciendo minúsculas todos los caracteres. Las técnicas inventivas también pueden incluir generar varias versiones derivadas del destino candidato a través de la sustitución y permutación de los caracteres en base a similitudes ópticas conocidas e identificación en un repositorio 202 que contiene los URL de destino bien conocidos a través de una búsqueda del repositorio 202 o base de datos. Las técnicas inventivas registran cualquier coincidencia entre los destinos bien conocidos y las versiones de los destinos candidatos.

El complemento 224 tomará una instantánea de la ventana de la página web asociada con el destino candidato, ejecutará el OCR sobre la imagen reproducida entera y almacenará las palabras reconocidas en un grupo. El complemento 224 realiza estas acciones porque los suplantadores de identidad pueden sustituir los elementos gráficos por texto plano para eludir el reconocimiento mediante pruebas automatizadas.

En otro aspecto de la invención, las técnicas inventivas leen solamente el texto de la página web asociada con el destino candidato en el grupo. También, un algoritmo calcula la firma de distribución de palabras de la página web extrayendo un histograma de palabras. Tales técnicas inventivas comparan el histograma de palabras extraído con los histogramas de páginas web destino bien conocidos que se graban en la base de datos o repositorio, graban cualesquiera coincidencias entre el histograma de palabras extraído y los histogramas de las páginas web destino bien conocidos, y tipifican las coincidencias por porcentaje de solapamiento en el histograma de palabras. En otro aspecto de la invención, las técnicas inventivas extraen las fuentes estimadas en base a las coincidencias más próximas en la superposición de contenidos en base del análisis de texto, y graban las fuentes como orígenes potenciales para el destino candidato.

Si la página web candidata contiene imágenes, las técnicas inventivas pueden convertir las imágenes a un formato de gráficos común (por ejemplo, el formato de intercambio gráfico (GIF)), generar las huellas de imagen para las imágenes, comparar las huellas de imagen frente a las firmas de logotipos bien conocidos, y grabar cualesquiera coincidencias entre las huellas de imágenes y las firmas de los logotipos bien conocidos. Preferentemente, las huellas de los logotipos en la base de datos o repositorio contienen huellas del mismo logotipo corporativo reproducido en una variedad de resoluciones distintas para evitar los efectos de la pixelación de la obstaculización de la identificación del logotipo.

El complemento 224 determina la dirección IP efectiva que se asigna por el destino candidato. Las técnicas inventivas determinan el efecto de organización de propiedad para la dirección IP efectiva desde su repositorio 202 o usando las bases de datos secundarias tales como, por ejemplo, “quién es”. El servicio quién es se describe en la Petición de Comentarios de Internet 954, del autor Harrenstein y otros en 1985, y disponible en el URL http://www.rfc-archive.org/getrfc.php?rfc=954, y está ampliamente desplegado en Internet. En otro aspecto de la invención, las técnicas inventivas comprueban el destino candidato para signos de ataque de suplantación de identidad típicos, por ejemplo, cadenas largas que desbordan la ventana de localización, ubicaciones que tienen una alta probabilidad de suplantación de identidad, o solamente diferencias sutiles para los nombres URL bien conocidos. También, las técnicas inventivas determinan la propiedad del dominio DNS que se identifica en el destino candidato.

En otro aspecto de la invención, las técnicas inventivas calculan una puntuación de suplantación de identidad para el destino candidato. Las técnicas identifican una página del destino candidato como limpia si todas de las organizaciones determinadas coinciden con una identificación (ID) o identidad de organización almacenada correspondiente en el repositorio 202 y si la organización almacenada no es demasiado similar a otra organización que se clasifica como más popular en la base de datos del repositorio 202.

En otro aspecto de la invención, si una página del destino candidato tiene referencias visuales conflictivas (por ejemplo, ID de la organización = X) y la organización física (ID = Y), las técnicas inventivas producen una ventana 222 que alerta al usuario del potencial de suplantación de identidad y muestra los resultados de la comprobación de la referencia visual y aquéllas de las trazas físicas de vuelta. Las técnicas generan un aviso de fraude 222 a través de una sugerencia visual mostrada al usuario en al menos una de una ventana y una barra de estado externa para la ventana del navegador asociada con el destino candidato. La ventana 222 está abierta en una ventana situada aleatoriamente separada del navegador para impedir los ataques de superposición por los suplantadores de identidad.

En otro aspecto de la invención, las técnicas inventivas identifican la página del destino candidato como “origen desconocido” si las referencias visuales podrían no coincidir con una organización, pero por las que el destino candidato coincide con el URL visual y cuyo destino no es un destino de suplantación de identidad probable. También, las técnicas identifican la página del destino candidato como “segura” si las referencias visuales de las páginas se asignan a un objetivo bien definido, y la determinación de la organización física obtuvo el mismo ID de la organización.

Las técnicas inventivas, en otro aspecto de la invención, determinan la ubicación del URL del destino candidato en la barra de herramientas del navegador. El usuario puede colaborar con el agente del programa informático para establecer la ubicación para el visualizador del URL respecto a la ventana del navegador. El agente del programa informático puede incluir programas informáticos de OCR para localizar la ubicación de la barra DIRECCIÓN. También, el agente del programa informático puede incluir una serie de pruebas que redirige el navegador a una lista de URL distintos que llenan la ventana de localización entera en la barra de herramientas del navegador. El contenido que va a ser visualizado en esos URL distintos es idéntico de manera que solamente el URL cambiará en la ventana del navegador entera. Usando una combinación de todas las letras y los códigos de caracteres regionales en el conjunto de URL probados, es posible determinar la altura exacta del texto. Esta prueba se puede automatizar en cada reinicio del

navegador. Un agente se puede instalar como un complemento del navegador que captura la ubicación del navegador actual, ejecuta la prueba de localización del URL, y restaura la localización del navegador original en cada cambio de tamaño para la ventana del navegador.

En otro aspecto de la invención, las técnicas inventivas se pueden realizar por un agente del programa informático, en un navegador web, o en un cliente de correo electrónico.

La FIG. 3 muestra un diagrama de flujo que ilustra un método para generar una base de datos de destinos a ser protegidos frente al fraude informático. El paso 302 incluye generar al menos una categoría de destinos a ser protegidos. El paso 304 incluye la recuperación de al menos una lista de destinos que pertenecen a al menos una categoría. El paso de recuperar al menos una lista de destinos que pertenecen a al menos una categoría puede incluir obtener una primera lista de destinos y una segunda lista de destinos, y fundir la primera lista de destinos y la segunda lista de destinos. El paso de recuperar al menos una lista de destinos que pertenecen a al menos una categoría puede incluir el acceso a al menos uno de un motor de búsqueda de Internet y un servicio de indexación de Internet.

Una variedad de técnicas, que utilizan componentes físicos dedicados, procesadores de propósito general, microprogramas, programas informáticos, o una combinación de los anteriores se puede emplear para implementar la presente invención. Al menos una realización de la invención se puede implementar en forma de un producto informático que incluye un medio utilizable por ordenador con código de programa utilizable por ordenador para realizar los pasos del método indicados. Adicionalmente, se puede implementar al menos una realización de la invención en forma de un aparato que incluye una memoria y al menos un procesador que se acopla a la memoria y la operativa para realizar los pasos del método ejemplar.

En la actualidad, se cree que la implementación preferente hará uso considerable del programa informático que se ejecuta en un ordenador de propósito general o estación de trabajo. Con referencia a la FIG. 4, tal implementación puede emplear, por ejemplo, un procesador 402, una memoria 404, y un interfaz de entrada y/o salida formado, por ejemplo, por un visualizador 406 y un teclado 408. El término “procesador” como se usa aquí dentro está destinado a incluir cualquier dispositivo de procesamiento, tal como, por ejemplo, uno que incluye una CPU (unidad central de proceso) y/u otras formas de circuitería de procesamiento. Además, el término “procesador” puede referirse a más de un procesador individual. El término “memoria” está destinado a incluir la memoria asociada con un procesador o CPU, tal como, por ejemplo, la RAM (memoria de acceso aleatorio), ROM (memoria solo de lectura), un dispositivo de memoria fijo (por ejemplo, disco duro), un dispositivo de memoria extraíble (por ejemplo, disco flexible), una memoria rápida y similares. Además, la frase “interfaz de entrada y/o salida” como se usa aquí dentro, está destinada a incluir, por ejemplo, uno o más mecanismos para la introducción de los datos a la unidad de procesamiento (por ejemplo, el ratón), y uno o más mecanismos para proporcionar los resultados asociados con la unidad de procesamiento (por ejemplo, la impresora). El procesador 402, la memoria 404, y el interfaz de entrada y/o salida tal como el visualizador 406 y el teclado 408 se pueden interconectar, por ejemplo a través del canal principal 410 como parte de una unidad de procesamiento de datos 412. Las interconexiones adecuadas, por ejemplo a través del canal principal 410, también se pueden proporcionar a un interfaz de red 414, tal como una tarjeta de red, que se puede proporcionar al interfaz con una red informática, y a un interfaz de medios 416, tal como un disco flexible o unidad de CD-ROM, que se puede proporcionar al interfaz con los medios 418.

Por consiguiente, el programa informático que incluye las instrucciones o código para realizar las metodologías de la invención, según se describe aquí dentro, se puede almacenar en uno o más de los dispositivos de memoria asociados (por ejemplo, la memoria extraíble o fija, ROM) y, cuando están listos para ser usados, cargar en parte o en su totalidad (por ejemplo, en la RAM) y ejecutar por una CPU. Tal programa informático podría incluir, pero no se limita a, microprogramas, programas informáticos residentes, microcódigo, y similares.

Adicionalmente, la invención puede tomar la forma de un producto de programa informático accesible desde un medio utilizable por ordenador o legible por ordenador (por ejemplo, los medios 418) que proporcionan el código de programa para el uso por o en conexión con un ordenador o cualquier sistema de ejecución de instrucciones. Para los propósitos de esta descripción, un medio utilizable por ordenador o legible por ordenador puede ser cualquier aparato para usar mediante o en conexión con el dispositivo, aparato o sistema de ejecución de instrucciones.

El medio puede ser un sistema (o aparato o dispositivo) electrónico, magnético, óptico, electromagnético, de infrarrojos, o semiconductor o un medio de propagación. Ejemplos de un medio legible por ordenador incluyen una memoria de semiconductor o de estado sólido (por ejemplo, la memoria 404), cinta magnética, un disco flexible de ordenador extraíble (por ejemplo, el medio 418), una memoria de acceso aleatorio (RAM), una memoria solo de lectura (ROM), un disco magnético rígido y un disco óptico. Los ejemplos actuales de discos ópticos incluyen el disco compacto-de memoria solo de lectura (CD-ROM), el disco compacto-de lectura y/o escritura (CD-R/W) y el DVD.

Un sistema de procesamiento de datos adecuado para almacenar y/o ejecutar el código de programa incluirá al menos un procesador 402 acoplado directa o indirectamente a los elementos de memoria 404 a través del canal principal del sistema 410. Los elementos de memoria pueden incluir la memoria local empleada durante la ejecución real del código de programa, el almacenamiento masivo, y las memorias caché las cuales proporcionan almacenamiento temporal de al menos algún código de programa para reducir el número de veces que el código debe ser recuperado desde la memoria masiva durante la ejecución.

Los dispositivos de entrada y/o salida o I/O (que incluyen pero no se limitan a teclados 408, visualizadores 406, dispositivos punteros, y similares) se pueden acoplar al sistema o bien directamente (tal como a través del canal principal 410) o a través de la intervención de controladores de I/O (omitidos por claridad).

Los adaptadores de red tales como el interfaz de red 414 también se pueden acoplar al sistema para permitir al sistema el procesamiento de datos que llegue a estar acoplado a otros sistemas de procesamiento de datos o impresoras remotas o dispositivos de almacenamiento a través de la intervención de redes públicas o privadas. Los modem, modem de cable y tarjetas Ethernet son solo unos pocos de los tipos de adaptadores de red disponibles actualmente.

En cualquier caso, se debería entender que los componentes ilustrados aquí dentro se pueden implementar en varias formas de componentes físicos, programas informáticos, o combinaciones de los mismos, por ejemplo, circuito(s) integrado(s) de aplicaciones específicas (ASICS), circuitería funcional, uno o más ordenadores de propósito general programados adecuadamente con memoria asociada, y similares. Dando las enseñanzas de la invención proporcionada aquí dentro, un experto común en la técnica relacionada será capaz de contemplar otras implementaciones de los componentes de la invención.

Aunque las realizaciones ilustrativas de la presente invención se han descrito aquí dentro con referencia a los dibujos anexos, se tiene que entender que la invención no está limitada a esas precisas realizaciones, y que se pueden hacer otros varios cambios y modificaciones por un experto en la técnica sin salir del alcance de la invención, como se define por las reivindicaciones.

REIVINDICACIONES

1. Un método de detección de fraude informático, que comprende los pasos de:

obtener (102) una versión de texto de un destino candidato y una reproducción gráfica de dicho destino candidato;

comparar (104) dicha versión de texto de dicho destino candidato y dicha reproducción gráfica de dicho destino candidato con, respectivamente, una versión de texto correspondiente de un destino almacenado y una reproducción gráfica correspondiente de dicho destino almacenado; y

generar (106) un aviso de fraude si dicha reproducción gráfica de dicho destino candidato es considerablemente similar a dicha reproducción gráfica de dicho destino almacenado mientras que dicha versión de texto de dicho destino candidato difiera considerablemente de dicha versión de texto correspondiente de dicho destino almacenado.

2. El método de acuerdo con la reivindicación 1, en donde el paso de comparación se realiza en un subconjunto de dicho destino candidato y dicho destino almacenado.

3. El método de acuerdo con la reivindicación 1, en donde el paso de comparar dicha versión de texto de dicho destino candidato y dicha reproducción gráfica de dicho destino candidato con, respectivamente, una versión de texto almacenado correspondiente y una reproducción gráfica almacenada correspondiente comprende los pasos de:

determinar una dirección IP, protocolo de internet, efectiva que se asigna mediante dicho destino candidato; y

determinar una organización propietaria efectiva para dicha dirección IP efectiva.

4. El método de acuerdo con la reivindicación 1, en donde el paso de obtener una versión de texto de un destino candidato y una reproducción gráfica de dicho destino candidato comprende los pasos de:

leer un mapa de imagen de una barra de herramientas del navegador de una página web asociada con dicho destino candidato; y

determinar una representación de los caracteres de dicho mapa de imagen usando un algoritmo de reconocimiento óptico de caracteres, OCR.

5. El método de acuerdo con la reivindicación 1, en donde el paso de obtener una versión de texto de un destino candidato y una reproducción gráfica de dicho destino candidato comprende los pasos de:

analizar una representación de caracteres;

normalizar dicha representación de caracteres; y

generar las versiones derivadas adecuadas de dicho destino candidato a partir de la sustitución y permutación de caracteres.

6. El método de acuerdo con la reivindicación 1, en donde el paso de comparar dicha versión de texto de dicho destino candidato y dicha reproducción gráfica de dicho destino candidato con, respectivamente, una versión del texto almacenado correspondiente y una reproducción gráfica almacenada correspondiente comprende los pasos de:

buscar una base de datos de destinos bien conocidos; y

grabar las coincidencias entre dichos destinos bien conocidos y las versiones derivadas de dicho destino candidato.

7. El método de acuerdo con la reivindicación 1, en donde el paso de obtener una versión de texto de un destino candidato y una reproducción gráfica de dicho destino candidato comprende el paso de:

leer solamente el texto de una página web asociada con dicho destino candidato en un grupo.

8. El método de acuerdo con la reivindicación 1, en donde el paso de obtener una versión de texto de un destino candidato y una reproducción gráfica de dicho destino candidato comprende los pasos de:

tomar una instantánea de una página web asociada con dicho destino candidato;

ejecutar el OCR sobre una imagen representada entera de dicha página web; y

almacenar las palabras reconocidas en un grupo.

9. El método de acuerdo con la reivindicación 8, que además comprende los pasos adicionales de:

calcular una firma de distribución de palabras de dicha página web extrayendo un histograma de palabras;

comparar dicho histograma de palabras con histogramas de páginas web de destino bien conocidos;

grabar las coincidencias entre dicho histograma de palabras y los histogramas de las páginas web de destinos bien conocidos;

clasificar dichas coincidencias por porcentaje de solapamiento en dicho histograma de palabras; y

extraer las fuentes estimadas de dicha página web a partir de dichas coincidencias con alto porcentaje de solapamiento.

10. El método de acuerdo con la reivindicación 1, en donde el paso de obtener una versión de texto de un destino candidato y una reproducción gráfica de dicho destino candidato comprende los pasos de:

convertir las imágenes en una página web asociada con dicho destino candidato con un formato de gráficos comunes;

generar las huellas de imagen para dichas imágenes;

comparar dichas huellas de imagen frente a las firmas de los logotipos bien conocidos; y

grabar cualquier coincidencia entre dichas huellas de imagen y dichas firmas de logotipos bien conocidos.

11. El método de acuerdo con la reivindicación 1, en donde el paso de comparar dicha versión de texto de dicho destino candidato y dicha reproducción gráfica de dicho destino candidato con, respectivamente, una versión del texto almacenado correspondiente y una reproducción gráfica almacenada correspondiente comprende uno o más de los pasos de:

comprobar dicho destino candidato para los signos de ataque de suplantación de identidad típicos;

determinar la propiedad de un dominio DNS, sistema de nombre de dominio, identificado en dicho destino candidato; y

calcular una puntuación de suplantación de identidad para dicho destino candidato.

12. El método de acuerdo con la reivindicación 1, que además comprende el paso de:

identificar dicho destino candidato como limpio si todas las organizaciones determinadas coinciden con una organización almacenada correspondiente y si dicha organización almacenada no es considerablemente similar a otra organización clasificada como más popular en una base de datos.

13. El método de acuerdo con la reivindicación 1, en donde los pasos se realizan por uno de un agente del programa informático, un navegador web, y un cliente de correo electrónico.

14. Un aparato (412) para detectar fraude informático, que consta de:

una memoria (404); y

al menos un procesador (402) acoplado a dicha memoria (404) y operativo para:

obtener (102) una versión de texto de un destino candidato y una reproducción gráfica de dicho destino candidato;

comparar (104) dicha versión de texto de dicho destino candidato y dicha reproducción gráfica de dicho destino candidato con, respectivamente, una versión de texto correspondiente de un destino almacenado y una reproducción gráfica correspondiente de dicho destino almacenado; y

generar (106) un aviso de fraude si dicha reproducción gráfica de dicho destino candidato es considerablemente similar a dicha reproducción gráfica de dicho destino almacenado mientras que dicha versión de texto de dicho destino candidato difiere considerablemente de dicha versión de texto correspondiente de dicho destino almacenado.

15. Un producto de programa informático que comprende un medio utilizable por ordenador que tiene el código de programa utilizable por ordenador para detectar fraude informático, dicho producto de programa informático que incluye:

el código de programa utilizable por ordenador para obtener (102) una versión de texto de un destino candidato y una reproducción gráfica de dicho destino candidato;

el código de programa utilizable por ordenador para comparar (104) dicha versión de texto de dicho destino candidato y dicha reproducción gráfica de dicho destino candidato con, respectivamente, una versión de texto correspondiente de un destino almacenado y una reproducción gráfica correspondiente de dicho destino almacenado; y

el código de programa utilizable por ordenador para generar (106) un aviso de fraude si dicha reproducción gráfica de dicho destino candidato es considerablemente similar a dicha reproducción gráfica de dicho destino almacenado mientras que dicha versión de texto de dicho destino candidato difiere considerablemente de dicha versión de texto correspondiente de dicho destino almacenado.

FIG. 1

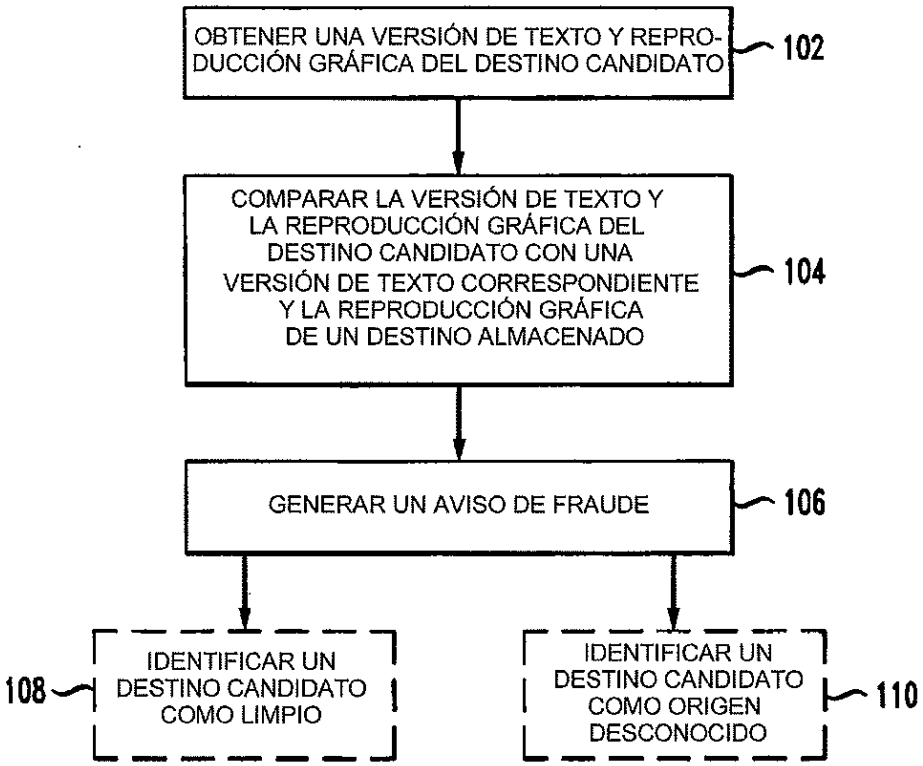

OBTENER UNA VERSIÓN DE TEXTO Y REPRODUCCIÓN GRÁFICA DEL DESTINO CANDIDATO
102
COMPARAR LA VERSIÓN DE TEXTO Y LA REPRODUCCIÓN GRÁFICA DEL DESTINO CANDIDATO CON UNA VERSIÓN DE TEXTO CORRESPONDIENTE Y LA REPRODUCCIÓN GRÁFICA DE UN DESTINO ALMACENADO
104
GENERAR UN AVISO DE FRAUDE
106
108
IDENTIFICAR UN DESTINO CANDIDATO COMO LIMPIO
IDENTIFICAR UN DESTINO CANDIDATO COMO ORIGEN DESCONOCIDO
110

FIG. 2

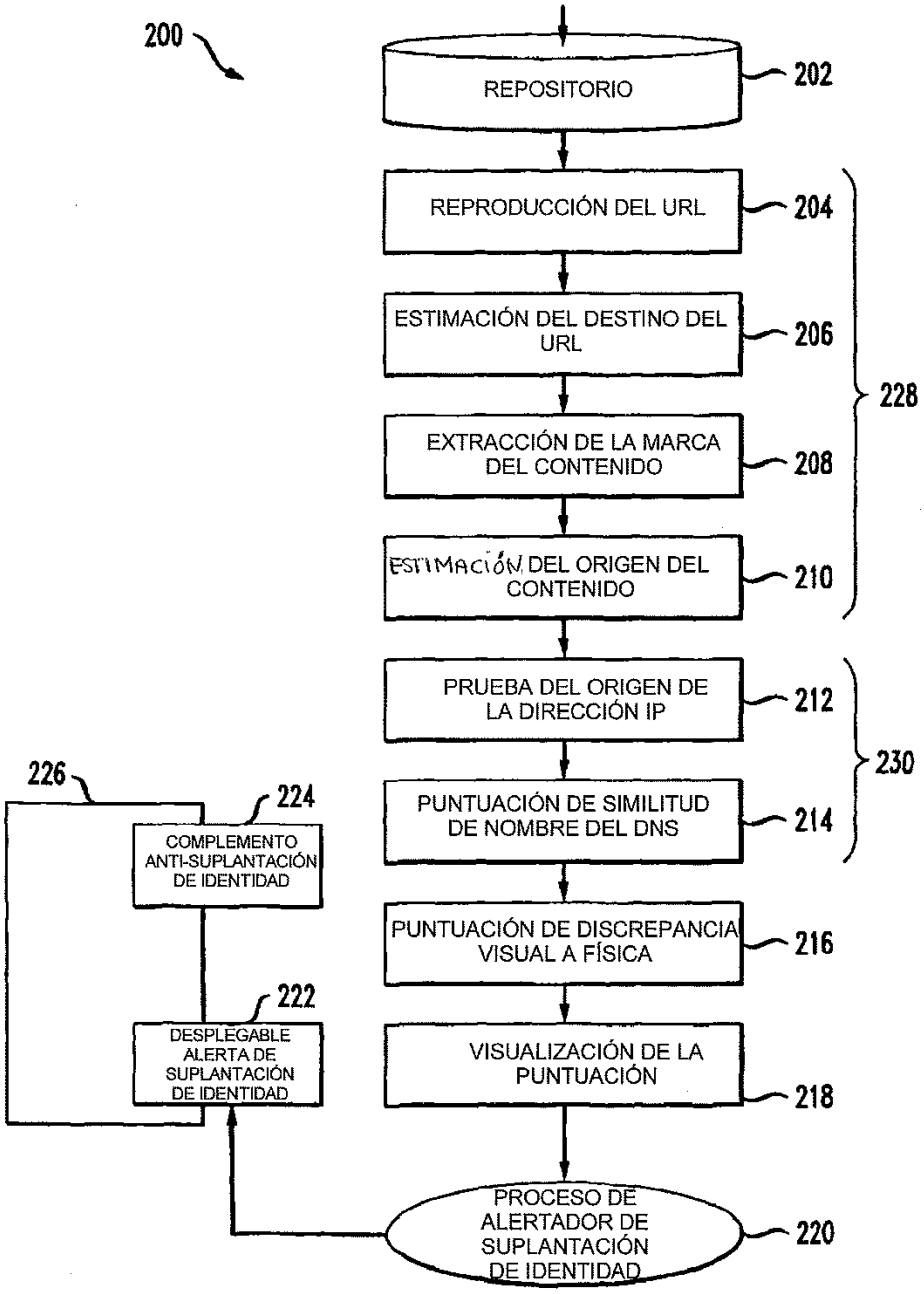

200
REPOSITORIO
202
REPRODUCCIÓN DEL URL
204
ESTIMACIÓN DEL DESTINO DEL URL
206
EXTRACCIÓN DE LA MARCA DEL CONTENIDO
208
ESTIMACIÓN DEL ORIGEN DEL CONTENIDO
210
228
PRUEBA DEL ORIGEN DE LA DIRECCIÓN IP
212
PUNTUACIÓN DE SIMILITUD DE NOMBRE DEL DNS
214
230
PUNTUACIÓN DE DISCREPANCIA VISUAL A FÍSICA
216
VISUALIZACIÓN DE LA PUNTUACIÓN
218
PROCESO DE ALERTADOR DE SUPLANTACIÓN DE IDENTIDAD
220
226
224
COMPLEMENTO ANTI-SUPLANTACIÓN DE IDENTIDAD
222
DESPLEGABLE ALERTA DE SUPLANTACIÓN DE IDENTIDAD

FIG. 3

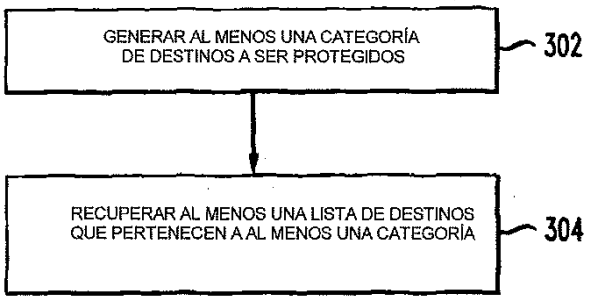
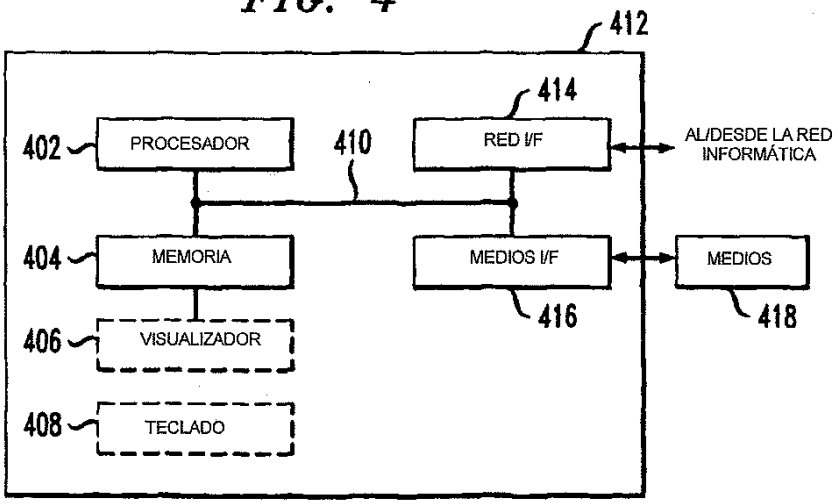

GENERAR AL MENOS UNA CATEGORÍA DE DESTINOS A SER PROTEGIDOS
302
RECUPERAR AL MENOS UNA LISTA DE DESTINOS QUE PERTENECEN A AL MENOS UNA CATEGORÍA
304

FIG. 4


412
414
402
PROCESADOR
410
RED I/F
AL/DESDE LA RED INFORMÁTICA
404
MEMORIA
MEDIOS I/F
MEDIOS
416
418
406
VISUALIZADOR
408
TECLADO