

AUTOMATIZACIÓN DE VALIDACIÓN DE IMAGEN

ANTECEDENTES

5 Muchas empresas cuentan con sistemas de apoyo al cliente donde los clientes proporcionan regularmente fotografías o imágenes a agentes de soporte para probar su elegibilidad para soporte, reembolso, u otras concesiones. Sin embargo, si las imágenes proporcionadas a los agentes de soporte han sido modificadas de forma fraudulenta, el cliente podría recibir apoyo o concesiones que el cliente no es elegible. Actualmente, las empresas deben verificar una imagen ya sea manualmente mediante la confirmación de la validez de la imagen con el creador del documento, o ejecutando un sofisticado proceso forense de la imagen. Sin embargo, estas técnicas requieren una gran cantidad de tiempo y/o recursos de cómputo, lo que se traduce en un servicio al cliente deficiente o en costos adicionales para las empresas que proporcionan soporte o concesiones a los clientes que no son elegibles para el soporte o concesiones.

BREVE DESCRIPCIÓN DE LA INVENCIÓN

Esta descripción describe técnicas para realizar un proceso automatizado para la identificación de imágenes originales, sin modificar. Las técnicas descritas en este documento incluyen la realización de un análisis multifactorial en una imagen para determinar la probabilidad de que una imagen o un objeto representado en la imagen ha sido modificado y producir un resultado que indica la probabilidad de que la imagen o el objeto representado en la imagen ha sido modificado. En algunos ejemplos, un portal electrónico (por ejemplo, aplicación web, sitio Internet, etc.) se presenta en un dispositivo de cómputo para recibir una imagen. Por ejemplo, un agente de soporte al cliente puede acceder a una aplicación web a través de un dispositivo de cómputo huésped y presentar una imagen que se le proporciona de un cliente. En otros ejemplos, el usuario puede enviar la imagen directamente (por ejemplo, en un ejemplo de auto-servicio). La aplicación web puede enviar la imagen a un sistema de validación de imagen, tal como llamando a una interfaz de programa de aplicación (API) basada en web asociada con el sistema de validación de imagen. El sistema de validación de imagen puede recibir la imagen para verificación y realizar un análisis multifactorial en la imagen usando diversos indicadores de modificación/alteración para determinar la probabilidad de que la imagen (y/o el objeto representado en la imagen) ha sido modificada de su forma original. Los indicadores de modificación pueden incluir cualquier tipo de operación que demuestran que la modificación de una imagen se ha producido, tal como analizando la imagen para detectar un cambio en la densidad de píxeles entre varias porciones de la imagen, comparando la imagen con una miniatura de la imagen para detectar diferencias, analizando los metadatos de la imagen para determinar si un *software* de edición de imagen ha sido utilizado en la imagen, analizando los metadatos de la imagen para identificar el momento en que se capturó la imagen o una ubicación geográfica en la que se capturó la imagen, y así sucesivamente. Uno o más de los

diversos indicadores de modificación pueden ser utilizados para determinar la probabilidad de que la imagen (o el objeto de la imagen) fue modificada. En algunos casos, los diversos indicadores de modificación pueden ser ponderados en mayor o menor medida a la hora de determinar la probabilidad de que la imagen fue modificada. Una vez que el servicio de validación de imagen determina la probabilidad de que la imagen se ha modificado, puede producir la salida de un indicador de la probabilidad de que la imagen se ha modificado. Por ejemplo, el sistema de modificación de imagen puede producir una indicación de que se han producido alteraciones, la alteración es probable, o no ha ocurrido ninguna alteración. En algunos ejemplos, la indicación de la probabilidad de que la modificación o alteración se ha producido puede reproducirse, o enviarse, al dispositivo de cómputo que aloja la aplicación web, la cual a su vez puede causar el resultado que se presenta en una interfaz de usuario de la aplicación web accesible a través del dispositivo de cómputo. De esta forma, un agente de servicio al cliente puede ser informado de la posibilidad de que la imagen se ha modificada y toma una acción apropiada, tal como rechazar la solicitud del cliente para soporte o concesiones directamente, solicitando información adicional del cliente para determinar la elegibilidad para el soporte o concesión, o proporcionar al cliente con el soporte o concesiones que sean elegibles.

En algunos ejemplos, las técnicas que se describen en este documento incluyen además almacenar la información en almacenamiento basado en nube. Las imágenes pueden ser almacenadas en el almacenamiento basado en nube o bien antes de que las imágenes sean enviadas al servicio de validación de imagen, o después de que el servicio de validación de imagen haya analizado las imágenes. En algunos casos, se puede almacenar información adicional en el almacenamiento basado en nube junto con la imagen. Por ejemplo, los resultados del análisis realizado por el servicio de validación de imagen y/o la indicación de la probabilidad de modificación también pueden ser almacenados y asociados con una imagen particular. En algunos ejemplos, las imágenes almacenadas que anteriormente se recibieron a través de la aplicación web y se analizaron por el servicio de validación de imagen pueden proporcionar indicadores de modificación adicionales. Por ejemplo, el servicio de validación de imagen puede comparar una imagen en particular con imágenes almacenadas previamente, o tener otro proceso/servicio que compare las imágenes y devuelva resultados. La comparación puede indicar diversas relaciones entre imágenes almacenadas previamente y la imagen particular que actualmente está siendo analizada que puede sugerir la modificación de la imagen. Por ejemplo, si la imagen particular tiene más de una cantidad de umbral de similitudes con otras imágenes almacenadas, esto puede sugerir la alteración de la imagen en particular porque puede ser simplemente una versión modificada de una imagen almacenada previamente para la cual se solicitó soporte. Así, las técnicas aquí descritas automatizan la verificación de imágenes mediante la implementación de un proceso para analizar las imágenes recibidas utilizando un análisis multifactorial y determinar la probabilidad de que la imagen ha sido modificada de su forma original.

Esta Breve Descripción se proporciona para introducir una selección de técnicas en una forma simplificada que se describen a continuación en la Descripción Detallada. Esta Breve Descripción no pretende identificar características clave o características esenciales de la materia objeto reclamada, ni

tampoco es la intención de que esta Breve Descripción se utilice para limitar el alcance de la materia objeto reclamada. Además, la materia objeto reclamada no se limita a implementaciones que resuelven cualquiera o todas las desventajas observadas en cualquier parte de esta descripción.

5

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Descripción Detallada se establece con referencia a las figuras que acompañan al texto, en donde el dígito más a la izquierda de un número de referencia identifica la figura en la que el número de referencia aparece primero. El uso de los mismos números de referencia en la misma o diferentes figuras indica artículos o características similares o idénticas.

10

La Figura 1 es un diagrama esquemático que muestra un entorno ilustrativo para recibir una imagen para la que se solicita soporte y analizar la imagen para determinar la probabilidad de que la imagen ha sido modificada de su forma original.

La Figura 2 es un diagrama esquemático que muestra un servicio de validación de imagen ilustrativo para realizar varias operaciones para analizar una imagen utilizando múltiples indicadores de modificación para determinar la probabilidad de que la imagen ha sido modificada de su forma original.

15

La Figura 3 es un diagrama esquemático que muestra un dispositivo de cómputo huésped ilustrativo para ejecutar una aplicación web para recibir una imagen y dar salida a resultados que indican la probabilidad de que la imagen ha sido modificada de su forma original.

20

Las Figuras 4A y 4B son los diagramas ilustrativos de una imagen almacenada y una imagen que a ser analizada utilizando uno o más indicadores para determinar la probabilidad de que la imagen ha sido modificada.

La Figura 5 es un diagrama de flujo que muestra un proceso ilustrativo para determinar la autenticidad de una imagen basada en indicadores y generar una indicación de la probabilidad de que la imagen ha sido modificada de su forma original.

25

La Figura 6 es un diagrama de flujo que muestra un proceso ilustrativo para obtener una imagen que va a ser verificado como modificada o no, enviar la imagen a ser analizada y generar una indicación de la probabilidad de que la imagen ha sido modificada de su forma original.

La Figura 7 es un diagrama de flujo que muestra un proceso ilustrativo para analizar una imagen digital para determinar la probabilidad de que al menos una de las imágenes digitales o un objeto representado en la imagen digital ha sido modificado con base en al menos dos operaciones, y generar una indicación de la probabilidad de que la imagen digital o el objeto representado en la imagen se ha modificado de su forma original.

30

35

DESCRIPCIÓN DETALLADA

Esta invención describe técnicas para realizar un proceso para determinar la probabilidad de que una imagen ha sido alterada o modificada de su forma original. Muchas empresas cuentan con sistemas

de soporte al cliente, en donde los clientes proporcionan imágenes electrónicas o digitales (es decir, fotografías, imágenes escaneadas, etc.) a los agentes de soporte al cliente para demostrar la elegibilidad para soporte, reembolsos, u otras concesiones. Por ejemplo, los clientes pueden proporcionar imágenes de tarjetas de prepago que supuestamente no funcionan de manera correcta o imágenes de recibos mostrando fechas de compra para los productos o las garantías que un cliente está tratando de probar, a fin de recibir soporte o concesiones por parte del negocio. Sin embargo, los clientes pueden enviar imágenes fraudulentas o imágenes modificadas, para intentar ganar el soporte y/o concesiones para las cuales los clientes no son elegibles. El soporte de estas reclamaciones fraudulentas de los clientes o de ofrecer concesiones a los clientes inelegibles puede costar a las empresas considerables cantidades de tiempo y recursos, tal como el tiempo para verificar manualmente la validez de garantías con vendedores originales o costos para proporcionar reembolsos para los productos o servicios que no son elegibles para reembolso.

Las técnicas descritas aquí proporcionan un portal, tal como una aplicación web, que recibe una imagen que va a ser verificada o autenticada y envía la imagen a un servicio de validación de imagen para analizar la imagen y proporcionar una indicación de la probabilidad de que la imagen ha sido modificada. En algunos ejemplos, la imagen de servicio de validación de imagen además o alternativamente puede analizar la imagen para determinar la probabilidad de que un objeto (por ejemplo, tarjeta de regalo, recibo, justificante de compra, etc.), representado en la imagen ha sido modificado. En algunos ejemplos, la aplicación web puede estar alojada en un dispositivo de cómputo, tal como un dispositivo de cómputo huésped operado por un agente de soporte o un cliente. La aplicación web puede ser una aplicación descargable que es utilizada por los consumidores, o una aplicación provista a los agentes de soporte de una empresa para verificar las imágenes recibidas de los clientes. En algunos ejemplos, un agente de soporte puede recibir una imagen de un cliente tal como, por ejemplo, por correo electrónico, texto, portal web, o algún otro portal electrónico, y cargar la imagen a través de una interfaz de usuario de una aplicación web para determinar si la imagen ha sido modificada y/o si un objeto representado en la imagen ha sido modificado. En varios ejemplos, la aplicación web puede enviar la imagen a un servicio de validación de imagen. Por ejemplo, la aplicación web puede llamar a una API web que envía la imagen al servicio de validación de imagen. Además, la aplicación web puede almacenar la imagen en una base de datos, tal como un almacenamiento basado en nube, para su posterior comparación con otras imágenes.

Después de recibir la imagen, el servicio de validación de imagen puede analizar la imagen utilizando uno o más indicadores de modificación para determinar si la imagen ha sido modificada de su forma original, o si un objeto representado en la imagen ha sido modificado. En algunos ejemplos, los indicadores pueden incluir varias pruebas de alteración o modificación, tal como analizar la imagen para detectar un cambio en la densidad de píxeles entre diversas porciones de la imagen (especialmente cerca de regiones "sensibles", tales como códigos legibles por máquinas, claves de producto, precio, fechas, etc.), comparar la imagen con una miniatura de la imagen para detectar diferencias que indican la modificación y/o comparar con otras imágenes almacenadas para determinar si las imágenes tienen una

cantidad de umbral de similitud. Estos y otros indicadores pueden sugerir que la imagen fue modificada. Por ejemplo, si se detectan cambios de píxeles en una imagen, esto puede sugerir que la imagen fue editada en determinadas regiones, resultando en diferentes densidades de píxeles, o que el objeto (es decir, documento) contenido en la imagen fue modificado (por ejemplo, corrector, cinta, etc.). En otro ejemplo, si una imagen tiene una cantidad de umbral de similitud con otra imagen almacenada, esto puede sugerir la modificación de la imagen porque la imagen es sustancialmente similar a o idéntica a otra imagen que ya ha sido analizada, lo que puede indicar que la imagen ha sido utilizada previamente por un cliente para obtener concesiones o soporte. Además, o alternativamente, el servicio de búsqueda de validación pueden comparar la imagen en tiempo de ejecución con las imágenes en la web, tal como las imágenes que se pueden encontrar utilizando servicios de búsqueda en línea (por ejemplo, BING®, GOOGLE®, etc.), lo que puede indicar que la imagen ha sido modificada.

En algunos ejemplos, el servicio de validación de imagen puede además realizar técnicas de extracción de datos en la imagen para extraer metadatos de la imagen para utilizar como indicadores de modificación. En algunos casos, la extracción de datos puede revelar que los metadatos de la imagen no existen o han sido eliminados, lo que puede indicar que la imagen ha sido modificada. En algunos ejemplos, los metadatos pueden ser comparados con los metadatos de otras imágenes almacenadas para determinar si los diferentes metadatos se asemejan entre sí, lo que puede indicar que las imágenes son las mismas y que dicha modificación ha ocurrido. En algunos ejemplos, los metadatos extraídos pueden mostrar evidencia de la edición por parte de un cliente de *software* (por ejemplo, PHOTOSHOP®, Gimp, Sketch, etc.), lo cual puede indicar la modificación de la imagen. En varios ejemplos, los metadatos pueden indicar además un dispositivo asociado con la imagen, tal como una identificación de dispositivo (ID) de un dispositivo de cómputo que envió la imagen, una dirección de Protocolo de Internet (IP) asociada con el dispositivo de cómputo que capturó la imagen o envió la imagen, y/o una ubicación geográfica en la que se capturó la imagen, o desde la cual la imagen se envió. Utilizando esta información de identificación del dispositivo de cómputo, una imagen puede ser clasificada como probablemente modificada porque ese dispositivo de cómputo presentó previamente una imagen modificada de manera fraudulenta, el dispositivo de cómputo está situado en una ubicación desde la cual imágenes fraudulentas han sido presentadas anteriormente, la imagen se capturó en un lugar en donde las imágenes fraudulentas han sido previamente capturadas o similares. En otros ejemplos, los metadatos pueden incluir además información de fecha, tal como una fecha en la que se capturó la imagen. La imagen de la fecha en la que se tomó puede ser comparada con otras fechas, tal como la fecha en la que el producto o garantía presuntamente fue comprado, para determinar si la imagen ha sido modificada, o si un objeto representado en la imagen ha sido modificado. Por ejemplo, si una imagen se creó en una fecha antes de la supuesta fecha de compra del producto o de la garantía, esto puede sugerir que la imagen ha sido modificada ya que el consumidor sería incapaz de crear una imagen del producto o la garantía antes de la fecha de compra.

En algunos ejemplos, la extracción de datos puede incluir realizar un análisis reconocimiento de carácter óptico (OCR) de la imagen para extraer el texto de la imagen. El texto se puede utilizar como

indicadores de si la imagen ha sido modificada. Por ejemplo, si el texto contiene caracteres que no se utilizan para claves de producto o si los caracteres de clave de producto no están dispuestos en un formato en el que tradicionalmente están los caracteres de clave de producto (por ejemplo, 5x5, 4x4, etc.), el texto puede indicar que la imagen ha sido modificada. Asimismo, el código legible por máquina (por ejemplo, códigos de barras, códigos QR, marca de agua, etc.) en la imagen puede ser comparado con productos autorizados (es decir, productos listados como vendidos en una base de datos del comerciante) para determinar si el código legible por máquina está asociado con un producto que realmente se vendió. Si el código legible por máquina está en un recibo que indica una fecha y ubicación de negocios en donde el producto fue adquirido, pero la base de datos para el negocio no muestra que el código legible por máquina particular está asociado con la venta de un producto, esto puede indicar la modificación de la imagen.

En algunos ejemplos, el servicio de validación de imagen puede determinar la probabilidad de que la imagen se ha modificado con base en uno o más de los indicadores mencionados anteriormente. En varios ejemplos, los indicadores pueden ser ponderados en mayor o menor medida cuando se utilizan para determinar la probabilidad de que la imagen ha sido modificada. Por ejemplo, un indicador, tal como los metadatos, que muestra evidencias de la edición por parte de un cliente de *software* puede ser ponderado con más peso para mostrar la modificación de una imagen que un indicador tal como la variación de píxeles en la imagen. Con base en los diversos indicadores, o diversos indicadores ponderados, el servicio de validación de imagen puede determinar la probabilidad de que la imagen ha sido modificada. Por ejemplo, los indicadores pueden indicar una probabilidad que cae dentro de los diversos umbrales e indicar uno o más resultados tales como la alteración es detectada, la alteración es probable, o no concluyente debido a que no existe una clara evidencia de alteración. El servicio de verificación de imagen puede devolver los resultados del análisis a la aplicación web. Por ejemplo, el servicio de verificación de imagen puede dar salida a la aplicación web de una o más de las probabilidades de que la imagen fue modificada, el análisis y los indicadores utilizados para determinar la probabilidad y/o los metadatos que se extrajeron de la imagen.

La aplicación web puede enviar la indicación de la probabilidad de que la imagen se ha modificado. Por ejemplo, la aplicación web puede presentar la indicación de la probabilidad de que la imagen ha sido modificada en una pantalla del dispositivo de cómputo huésped para informar al agente de soporte u otro usuario la probabilidad de que la imagen fue modificada. Además, la aplicación web puede presentar tareas o acciones sugeridas o realizar tareas o acciones, con base en la indicación de la probabilidad de que la imagen se ha modificado. Por ejemplo, si se detectan alteraciones, se puede utilizar un proceso automatizado para notificar al cliente que la imagen no se ha aceptado o ha sido marcada por fraude y rechazar la solicitud de soporte o concesiones. En otro ejemplo, si la alteración es probable pero no segura, la aplicación web puede solicitar información adicional del agente de soporte o el cliente, tal como las imágenes del documento en cuestión desde ángulos diferentes, o un vídeo del documento desde ángulos diferentes, para ayudar a determinar si la modificación se ha producido. Ya que la modificación se realiza utilizando *software* de edición después de crear la imagen, puede ser difícil

para un estafador recrear las modificaciones exactas sobre la imagen desde distintos ángulos del documento.

En varios ejemplos, la aplicación web puede causar uno o más de la imagen, la indicación de la probabilidad de modificación, los indicadores utilizados en el análisis, y/o los metadatos de la imagen que se va a almacenar en un almacenamiento basado en nube, tal como en el caso de almacenamiento de objetos binarios grandes (BLOB, según sus siglas en inglés). Por ejemplo, la aplicación web puede enviar cualquiera de los datos anteriores al almacenamiento BLOB. Los datos pueden ser indexados u organizados de tal manera que la información está asociada con la imagen adecuada. De esta manera, las imágenes almacenadas en el almacenamiento BLOB y sus datos asociados se pueden utilizar por el servicio de validación de imagen u otro proceso, para determinar si una imagen en particular ha sido modificada o si un objeto representado en la imagen ha sido modificado.

Mientras las técnicas aquí descritas son descritos como siendo realizadas por un servicio de validación de imagen, una aplicación web y un almacenamiento basado en nube, las técnicas pueden ser realizadas por un solo dispositivo de cómputo o entidad, o cualquier combinación de dispositivos de cómputo y entidades.

Entornos Ilustrativos

La Figura 1 es un diagrama esquemático que muestra un ejemplo de entorno 100 para recibir una imagen para la que se solicita soporte y analizar la imagen para determinar la probabilidad de que la imagen ha sido modificada de su forma original. Más particularmente, el entorno ilustrativo 100 puede incluir uno o más dispositivos de cómputo huésped 102, un servicio de validación de imagen 104 y un almacenamiento basado en nube 106.

El dispositivo(s) de cómputo huésped 102 puede incluir cualquier tipo de entidad, servidor, consola, computadora, etc., configurado con uno o más módulos configurados para presentar una interfaz de usuario 108 en una pantalla asociada con el dispositivo(s) de cómputo huésped 102 para recibir una imagen, enviar la imagen al servicio de validación de imagen 104 y presentar un resultado 110 del análisis realizado por el servicio de validación de imagen 104. El dispositivo(s) de cómputo huésped 102 puede comprender cualquier tipo de computadora, tal como una computadora portátil, computadora de escritorio, dispositivo de cómputo de teléfono inteligente o cualquier otro tipo de dispositivo de cómputo, que pueda ser operado por una entidad tal como un agente de soporte. El dispositivo(s) de cómputo huésped 102 puede ejecutar una aplicación basada en web que presenta la interfaz de usuario 108 para recibir una o más imágenes 112. En algunos ejemplos, un cliente puede acceder a la aplicación basada en web y cargar la imagen(es) 112 directamente para ser verificada. La imagen(es) 112 puede comprender cualquier tipo de imagen en forma electrónica o digital, tal como una fotografía o una imagen escaneada. Como se muestra en la Figura 1, la imagen(es) 112 es una imagen de un documento (es decir, tarjetas de prepago, recibo, garantía, etc.) para el cual un consumidor puede estar intentando obtener soporte o concesiones. Una vez que la imagen(es) 112 ha sido presentada a través de la interfaz de usuario 108 de una aplicación web alojada en el dispositivo(s) de cómputo huésped 102, el

dispositivo(s) de cómputo huésped 102 puede enviar la imagen(es) 112 a través de una o más red(es) 116 al servicio de validación de imagen 104. En algunos ejemplos, el dispositivo(s) de cómputo huésped 102 puede enviar la imagen al llamar a una API web asociada con el servicio de validación de imagen 104 para que el servicio de validación de imagen realice un análisis sobre la imagen(es) 112. En algunos ejemplos, el dispositivo(s) de cómputo huésped 102 puede además enviar la imagen(es) 112 al almacenamiento basado en nube 106 para ser almacenada para su uso posterior.

La(s) red(es) 116 puede incluir cualquiera de o una combinación de varios tipos diferentes de redes, tales como redes celulares, redes inalámbricas, Redes de Área Local (LAN), Redes de Área Ancha (WAN), Redes de Área Personal (PAN) y el Internet.

El servicio de validación de imagen 104 puede ser cualquier entidad, servidor, consola, computadora, etc., configurada con uno o más módulos para analizar la imagen(es) 112 utilizando uno o más indicadores para determinar si la imagen(es) 112 ha sido modificada o si un objeto representado en la imagen(es) 112 ha sido modificado. En algunos ejemplos, el dispositivo de cómputo huésped 102, el servicio web y el servicio de validación de imagen 104 podrían todos ser un dispositivo de cómputo o una entidad. El servicio de validación de imagen 104 puede incluir uno o más módulos para la extracción de los metadatos de la imagen(es) 112 para utilizarlos como indicadores para determinar si la imagen(es) 112 ha sido modificada. En algunos casos, los indicadores pueden incluir varias pruebas de alteración o modificación, tal como analizar la imagen para detectar un cambio en la densidad de píxeles entre varias porciones de la imagen, comparar la imagen con una miniatura de la imagen para detectar diferencias indicando la modificación, la comparación con otras imágenes almacenadas para determinar si las imágenes tienen una cantidad de umbral de similitud, información que indica una fuente de la imagen, evidencia de *software* de edición que se muestra en los metadatos de la imagen, y/o diversas técnicas de análisis de texto. Estos y otros indicadores, que se describen con más detalle con respecto a las Figuras 4A y 4B, pueden sugerir que la imagen fue modificada. Basado en el análisis de la imagen(es) 112 utilizando los diversos indicadores, el servicio de validación de imagen 104 puede determinar la probabilidad de que la imagen se ha modificado con base en uno o más de los indicadores mencionados anteriormente. Por ejemplo, los indicadores pueden indicar una probabilidad que cae dentro de los diversos umbrales de probabilidad e indicar uno o más resultados, tales como la alteración es detectada, la alteración es probable, o no concluyentes debido a que no existe una clara evidencia de alteración. El servicio de verificación de imagen 104 puede regresar entonces los resultados del análisis al dispositivo(s) de cómputo huésped 102. Por ejemplo, el servicio de verificación de imagen 104 puede dar salida a datos de análisis 114 a la aplicación web alojada en el dispositivo(s) de cómputo huésped 102, en donde los datos de análisis 114 incluyen uno o más de la probabilidad de que la(s) imagen(es) 112 fue modificada, el análisis realizado y los indicadores utilizados para determinar la probabilidad y/o los metadatos que se extrajeron de la imagen(s) 112.

La interfaz de usuario 108 puede presentar la probabilidad de que la(s) imagen(es) 112 fue modificado como resultado 110 en una pantalla asociada con el dispositivo(s) de cómputo huésped 102. Por ejemplo, la interfaz de usuario 108 puede presentar el resultado de "Alteración Probable", o cualquier

otro resultado devuelto del servicio de validación de imagen 104.

En algunos ejemplos, el dispositivo(s) de cómputo huésped 102 puede almacenar datos de imagen 118 en el almacenamiento basado en nube 106. Por ejemplo, la aplicación web en el dispositivo(s) de cómputo huésped 102 puede ocasionar que los datos de imagen 118 sean enviados al almacenamiento basado en nube 106. En algunos ejemplos, los datos de imagen 118 pueden incluir la imagen(es) 112 y/o de cualquier información contenida en los datos del análisis 114, tales como la probabilidad de que la(s) imagen(es) 112 fue modificada, el análisis realizado y los indicadores utilizados para determinar la probabilidad y/o los metadatos que se extrajeron de la imagen(es) 112. Como se señaló anteriormente, el almacenamiento basado en nube 106 puede ser cualquier tipo de almacenamiento, tal como el almacenamiento BLOB, en donde los datos de imagen 118 se almacenan. Los datos de imagen 118 pueden almacenarse en varios formatos, tales como en Notación de Objeto JavaScript (JSON, según sus siglas en inglés) o Lenguaje de Marcación Extensible (XML, según sus siglas en inglés). En algunos ejemplos, el almacenamiento basado en nube 106 puede organizar los datos de imagen 118 de manera que la imagen(es) 112 se indexa o de otra manera se asocia con sus respectivos datos de análisis 114. De esta forma, los datos de imagen 118 para una imagen(es) particular 112 pueden ser fácilmente accesibles para análisis. El servicio de validación de imagen 104 puede incluir, o solicitar un servicio basado en web para analizar los datos de imagen 118 almacenados en el almacenamiento basado en nube 106 y regresar los resultados para utilizarlos como indicadores de si una imagen ha sido modificada. Por ejemplo, el servicio de validación de imagen 104 puede almacenar o llamar a un servicio web o proceso para determinar si una imagen(es) particular 112 siendo analizada tiene similitudes con otras imágenes u otros metadatos almacenados en el almacenamiento basado en nube 106. Las similitudes entre las imágenes almacenadas previamente se pueden utilizar como indicadores de si una imagen(es) particular 112 siendo analizada por el servicio de validación de imagen 104 ha sido modificada.

Aunque el entorno ilustrativo 100 está representado en la Figura 1 como incluyendo un dispositivo(s) de cómputo huésped 102, un servicio de validación de imagen 104 y un almacenamiento basado en nube 106 como entidades separadas, en varias implementaciones, cualquier combinación de diferentes entidades podrán realizar las técnicas descritas. En algunos ejemplos, todas las técnicas pueden ser realizadas por una sola entidad. En varios ejemplos, el servicio de validación de imagen 104 y el almacenamiento basado en nube 106 pueden ser la misma entidad o servidor.

La Figura 2 es un diagrama esquemático que muestra un servicio de validación de imagen 200 ilustrativo para realizar varias operaciones para analizar una imagen utilizando varios indicadores de modificación para determinar la probabilidad de que la imagen ha sido modificada de su forma original. El servicio de validación de imagen 200 puede comprender cualquier tipo de servicio de validación de imagen, tal como el servicio de validación de imagen 104, y cualquier tipo de dispositivo de cómputo o combinación de dispositivos de cómputo, tal como un servidor en línea, configurado con uno o más módulos para determinar si una imagen electrónica ha sido modificada de su forma original, o si un objeto representado en la imagen digital ha sido modificado. Como se muestra en la Figura 2, el servicio de

validación de imagen 200 puede incluir uno o más procesadores 202 acoplados a medios legibles por computadora 204, como por ejemplo, por un conductor común de comunicación. El procesador(es) 202 puede incluir una unidad de procesamiento central (CPU), unidad de procesamiento de gráficos (GPU), un microprocesador, y así sucesivamente.

5 Los medios legibles por computadora 204 pueden almacenar un sistema operativo 206 y un módulo de determinación de modificación 208. El sistema operativo 206 puede incluir instrucciones legibles por computadora que manejan los recursos de *hardware* y *software* del servidor de controlador 200.

10 El módulo de determinación de modificación 208 puede incluir instrucciones legibles por computadora que, cuando se ejecutan por los procesadores 202, realizan diversas operaciones para determinar si una imagen se ha modificada de su forma original. Además, o alternativamente, el módulo de determinación de modificación 208 puede determinar si un objeto (es decir, tarjetas de regalo, recibos, etc.), representado en la imagen ha sido modificado. Por ejemplo, el módulo de determinación de modificación 208 puede incluir uno o más módulos para obtener una imagen (por ejemplo, recibir una
15 imagen, tener acceso a una imagen almacenada, etc.), extraer datos de la imagen y analizar la imagen utilizando varios indicadores.

En algunos ejemplos, el módulo de determinación de modificación 208 puede incluir un módulo de extracción de datos 210 que puede incluir instrucciones legibles por computadora que, cuando se ejecutan por los procesadores 202, realizan diversas operaciones para extraer datos de una imagen. En
20 algunos ejemplos, la extracción de datos puede incluir instrucciones legibles por computadora para realizar técnicas de reconocimiento de carácter óptico (OCR) para extraer o determinar el texto incluido en la imagen. En algunos ejemplos, el módulo de extracción de datos 210 puede extraer además los metadatos del archivo de imagen, tales como los datos temporales que indican cuando se capturó la imagen, datos geográficos que identifican la ubicación en donde se capturó la imagen, evidencia del
25 *software* de edición utilizado en la imagen o información de identificación del dispositivo tal como un ID de dispositivo del dispositivo particular que ha creado y/o enviado la imagen para el análisis, una dirección IP del dispositivo particular y/o una ubicación geográfica de un dispositivo particular.

En algunos ejemplos, el módulo de determinación de modificación 208 puede incluir un indicador(es) 212 que puede incluir instrucciones legibles por computadora que, cuando se ejecutan por
30 los procesadores 202, realizan varias operaciones para analizar una imagen y datos asociados con la imagen para determinar la probabilidad de que la imagen fue modificada de su versión original. Por ejemplo, los indicadores pueden estar asociados con operaciones tales como (i) analizar la imagen para detectar un cambio en la densidad de píxeles en varias porciones de la imagen, (ii) comparar la imagen con una miniatura de la imagen para detectar una diferencia entre la imagen y la imagen en miniatura, (iii)
35 analizar los datos asociados con la imagen para determinar si el *software* de edición de imagen ha sido utilizado en la imagen, (iv) analizar los datos de la imagen para identificar al menos uno de un tiempo en el que se capturó la imagen o una ubicación geográfica en la que se capturó la imagen, (v) determinar que el código legible por máquina (por ejemplo, códigos de barras, códigos de Respuesta Rápida (QR,

según sus siglas en inglés), marcas de agua, etc.) incluido en el texto de la imagen está asociado con un producto particular, (vi) determinar que una clave de producto incluido en el texto de la imagen está en un formato apropiado para las claves de producto, (vii) determinar que una clave de producto incluido en el texto de la imagen incluye caracteres inválidos y/o (viii) analizar una comparación entre la imagen y la imagen almacenada para identificar similitudes entre la imagen y la imagen digital almacenada. La descripción adicional de los distintos indicadores se puede encontrar a continuación con referencia a las Figuras 4A y 4B. Uno o más de los indicadores 212 puede ser utilizado por el módulo de determinación de modificación 208 para determinar la probabilidad de que la imagen ha sido modificada de su forma original.

En varios ejemplos, el módulo de determinación de modificación 208 puede incluir un módulo de ponderación 214, que puede incluir instrucciones legibles por computadora que, cuando se ejecutan por los procesadores 202, realizan varias operaciones para la ponderación uno o más del indicador(es) 212. El módulo de ponderación 214 puede ponderar algún indicador(es) 212 más fuertemente ya que esos indicadores particulares pueden mostrar una mayor probabilidad de modificación de una imagen que otro indicador(es) 212, que se ponderan en menor medida. Por ejemplo, un indicador tal como el análisis de la imagen para determinar que se ha utilizado el *software* de edición de la imagen puede ser ponderado con mayor medida con un factor de ponderación que un indicador demostrando que el ID de dispositivo particular del dispositivo de cómputo que envió la imagen ha presentado una imagen modificada en el pasado. El módulo de ponderación 214 puede aplicar cualquier variedad y combinación de los factores de ponderación para el indicador(es) 212 en varias modalidades.

En algunos ejemplos, el módulo de determinación de modificación 208 puede incluir además una base de datos de imagen 216 que almacena las imágenes que van a ser analizadas, o ya se están analizando, por el módulo de determinación de modificación 208. La base de datos de imagen 216 puede comprender cualquier tipo de medio de almacenamiento, tal como el almacenamiento basado en nube 106. En algunos ejemplos, la base de datos de imagen puede almacenar además datos de imagen para una imagen respectiva, tal como la probabilidad de que la imagen particular fue modificada, los datos de análisis y los indicadores utilizados para la imagen particular y/o los metadatos extraídos de la imagen. Los datos de imagen pueden ser indexados o de otra manera asociados con la imagen. En algunos ejemplos, el módulo de determinación de modificación 208 puede incluir un indicador(es) 212 que analiza una comparación entre las imágenes almacenadas en la base de datos de imagen 216 y una imagen que se está analizando actualmente. El módulo de determinación de modificación 208 en algunos de los ejemplos pueden llamar o solicitar un proceso o entidad exterior al servicio de validación de imagen 200 para realizar la comparación entre las imágenes almacenadas y las imágenes que actualmente se analizan, lo cual regresa resultados de la comparación al módulo de determinación de modificación 208 indicando cualesquiera similitudes entre las imágenes analizadas. En algunos casos, la base de datos de imagen 216 puede ser una entidad separada del servicio de validación de imagen 200.

El servicio de validación de imagen puede incluir además la interfaz(ces) de red 218 (es decir, conexiones de comunicación) para enviar y recibir datos a través de una o más redes. La interfaz(ces) de

red 218 puede incluir uno o más controladores de interfaz de red (NIC, según sus siglas en inglés) u otros tipos de dispositivos de transceptor para enviar y recibir comunicaciones a través de una red, tal como la red(es) 116. Por ejemplo, la interfaz(ces) de red 218 puede recibir imágenes a ser analizadas para determinar si las imágenes han sido modificadas y enviar una indicación de la probabilidad de que la imagen ha sido modificada junto con los datos de análisis de imagen. En algunos ejemplos, la interfaz(ces) de red 218 puede permitir que el servicio de validación de imagen 200 tenga acceso a una imagen a través de una red en lugar de recibir la imagen a través de una red.

El servicio de validación de imagen 200 además puede incluir uno o más interfaces de entrada/salida (I/O) 220 para permitir que el servicio de validación de imagen 200 se comuniquen con otros dispositivos tales como dispositivos periféricos de entrada (por ejemplo, un teclado, un ratón, una pluma, un controlador de juego, un dispositivo de entrada de voz, un dispositivo de entrada táctil, un dispositivo de entrada gestual, un dispositivo de seguimiento, un dispositivo de asignación, una cámara de artículo de contenido visual, un sensor de profundidad, un sensor fisiológico y similares) y/o dispositivos periféricos de salida (por ejemplo, una pantalla, una impresora, altavoces de audio, una salida háptica y similares). De esta manera, los usuarios (es decir, los administradores) del servicio de validación de imagen 200 pueden interactuar con el servicio de validación de imagen 200 para realizar diversas operaciones, tales como la actualización de instrucciones legibles por computadora almacenadas en el servicio de validación de imagen 200.

La Figura 3 es un diagrama esquemático que muestra un dispositivo de cómputo huésped 300 ilustrativo para ejecutar una aplicación web para recibir una imagen y producir resultados que indican la probabilidad de que la imagen ha sido modificada de su forma original. El dispositivo de cómputo huésped 300 puede incluir cualquier tipo de dispositivo de cómputo, tal como el dispositivo(s) de cómputo huésped 102. En algunos ejemplos, el dispositivo de cómputo huésped 300 puede ser un dispositivo de cómputo operado por un agente de soporte de un servicio de atención al cliente que envía las imágenes recibidas de los clientes que intentan obtener soporte y/o concesiones para productos o servicios. En otros ejemplos, el dispositivo de cómputo huésped 300 puede comprender un dispositivo de cómputo de cliente, tal como una computadora personal o un teléfono móvil.

El dispositivo de cómputo huésped 300 puede incluir uno o más procesadores 302 comunicativamente acoplados a los medios legibles por computadora 304, como por ejemplo, a través de un conductor común de comunicación. El procesador(es) 302 puede incluir una unidad de procesamiento central (CPU), una unidad de procesamiento de gráficos (GPU), un microprocesador, y así sucesivamente. Los medios legibles por computadora 304 pueden almacenar un sistema operativo 306, una o más aplicaciones web 308 y una interfaz de programa de aplicación web (API) 310. El sistema operativo 306 puede incluir instrucciones legibles por computadora que manejan los recursos de *hardware* y *software* del dispositivo de cómputo huésped 300.

En algunos ejemplos, la aplicación(es) web 308 puede comprender instrucciones legibles por computadora que, cuando se ejecutan por el procesador(es) 302, realizan operaciones para recibir una imagen. Por ejemplo, la aplicación(es) web 308 puede presentar una interfaz de usuario, tal como la

interfaz de usuario 108, para recibir presentaciones o imágenes a ser analizadas por un servicio de validación de imagen. La aplicación(es) web 308 puede comprender un portal web que recibe la imagen a través de una interfaz de usuario, y en respuesta a la recepción de la imagen, llama o solicita la API web 310 para analizar la imagen para determinar la probabilidad de que la imagen ha sido modificada. En algunos ejemplos, la API 310 puede estar asociada con un servicio de validación de imagen, tal como los servicios de validación de imagen 104 y/o 200.

La aplicación(es) web 308 puede además enviar datos que serán almacenados en el almacenamiento basado en nube (es decir, el almacenamiento basado en nube 106). Por ejemplo, tras la recepción de la imagen, la aplicación(es) web 308 puede enviar la imagen al almacenamiento basado en nube para ser almacenada para su uso y análisis posterior. Además, la aplicación(es) web 308 puede recibir datos de análisis del servicio de validación de imagen junto con la indicación de la probabilidad de que la imagen presentada fue modificada. La aplicación(es) web 208 además causa que estos datos de análisis sean enviados y almacenados en el almacenamiento basado en nube e indexados o de otra manera asociados con la imagen respectiva.

En varios ejemplos, la interfaz de usuario de la aplicación(es) web 308 puede presentar la indicación de la probabilidad de que la imagen fue modificada. Por ejemplo, la interfaz de usuario de la aplicación(es) web 308 puede presentar una indicación de que ha ocurrido una alteración, la alteración es probable, o no ocurrió alteración.

En varios ejemplos, dependiendo de la indicación de la probabilidad de que se han producido alteraciones, diferentes acciones o sugerencias pueden ser producidas de la aplicación(es) web 308. Por ejemplo, la aplicación(es) web 308 podrá solicitar fotografías de una imagen desde diferentes ángulos cuando una indicación de probabilidad demuestra que la alteración es probable, pero se necesita más evidencia. La aplicación(es) web 308 puede sugerir el soporte o concesiones cuando la indicación de la probabilidad de que la modificación se ha producido indica que la alteración no ha ocurrido. Alternativamente, la aplicación(es) web 308 puede sugerir o tomar medidas tales como la realización de un proceso automatizado de rechazo cuando la probabilidad de modificación indica que se han producido alteraciones. Estas y otras sugerencias y acciones pueden realizarse por la aplicación(es) web basándose en la probabilidad de que se ha producido una modificación en la imagen.

El dispositivo de cómputo huésped 300 además puede incluir una o más interfaces de red 312 (es decir, conexiones de comunicaciones) para enviar y recibir datos a través de una o más redes. La interfaz(ces) de red 312 puede incluir uno o más controladores de interfaz de red (NIC) u otros tipos de los dispositivos de transceptor para enviar y recibir comunicaciones a través de una red, tal como la red(es) 116. Por ejemplo, la interfaz(ces) de red 312 puede enviar imágenes a través de una red a un servicio de validación de imagen para analizar la imagen para verificar que la imagen ha sido modificada. En algunos ejemplos, la interfaz(ces) de red 312 puede recibir datos, tales como datos de análisis, a través de la red desde varios dispositivo de cómputo, tal como un servicio de validación de imagen.

El dispositivo de cómputo huésped 300 puede además incluir uno o más de interfaces de entrada/salida (I/O) 314 para permitir que el dispositivo de cómputo huésped 300 se comunique con otros

dispositivos tales como dispositivos periféricos de entrada (por ejemplo, un teclado, un ratón, una pluma, un controlador de juego, un dispositivo de entrada de voz, un dispositivo de entrada táctil, un dispositivo de entrada gestual, un dispositivo de seguimiento, un dispositivo de asignación, una cámara de artículo de contenido visual, un sensor de profundidad, un sensor fisiológico y similares) y/o dispositivos periféricos de salida (por ejemplo, una pantalla, una impresora, altavoces de audio, una salida háptica y similares). Por ejemplo, las interfaces de I/O 314 pueden incluir una pantalla para presentar una interfaz de usuario de la aplicación(es) web 308 de acuerdo con las técnicas aquí descritas.

Los medios legibles por computadora 204 y 304 pueden incluir medios de almacenamiento por computadora y/o medios de comunicación. Los medios de almacenamiento por computadora pueden incluir memoria volátil, memoria no volátil, y/u otros medios de almacenamiento por computadora persistentes y/o auxiliares, medios de almacenamiento por computadora removibles y no removibles implementados en cualquier método o tecnología para el almacenamiento de información, tal como instrucciones legibles por computadora, estructuras de datos, módulos de programas u otros datos. La memoria de computadora es un ejemplo de los medios de almacenamiento. Por lo tanto, los medios de almacenamiento por computadora incluyen formas tangibles y/o físicas de los medios que se incluyen en un dispositivo y/o componente de *hardware* que es parte de un dispositivo o en un dispositivo externo, incluyendo, pero no limitándose a, memoria de acceso aleatorio (RAM), memoria estática de acceso aleatorio (SRAM), memoria de acceso aleatorio dinámica (DRAM), memoria de cambio de fase (PRAM), memoria de sólo lectura (ROM), memoria de sólo lectura programable borrable (EPROM), memoria de sólo lectura eléctricamente borrable y programable (EEPROM), memoria flash, memoria de sólo lectura de disco compacto (CD-ROM), discos versátiles digitales (DVD), tarjetas ópticas u otros medios de almacenamiento óptico, discos duros en miniatura, tarjetas de memoria, casetes magnéticas, cintas magnéticas, almacenamiento en discos magnéticos, tarjetas magnéticas u otros dispositivos o medios de almacenamiento magnéticos, dispositivos de memoria de estado sólido, cabinas de almacenamiento, almacenamiento conectado a la red, redes de área de almacenamiento, almacenamiento de computadora huésped o cualquier otra memoria de almacenamiento, dispositivos de almacenamiento y/o medio de almacenamiento que puede utilizarse para almacenar y mantener información para acceso mediante un dispositivo de cómputo.

En contraste, los medios de comunicación pueden modalizar instrucciones legibles por computadora, estructuras de datos, módulos de programa u otros datos en una señal de datos modulada, tal como una onda portadora, u otro mecanismo de transmisión. El término "señal de datos modulada" significa una señal que tiene una o más de sus características fijadas o cambiadas de tal manera que codifica la información en la señal. Tales señales u ondas portadoras, etc. pueden ser propagadas en medios alámbricos, tal como una red alámbrica o conexión de cable directo, inalámbrica y/o medios inalámbricos tales como medios acústicos, RF, infrarrojos y otros medios inalámbricos. Como se define aquí, los medios de almacenamiento por computadora no incluyen medios de comunicación.

En algunos ejemplos, el procesador(s) 202 y 302 puede representar, por ejemplo, una unidad de procesamiento de tipo CPU, unidad de procesamiento de tipo GPU, una unidad de procesamiento de tipo

HPU, una matriz de puerta programable por campo (FPGA), otra clase de procesador de señal digital (DSP), u otros componentes lógicos de *hardware* que pueden, en algunos casos, ser accionados por una CPU. Por ejemplo, y sin limitación, los tipos ilustrativos de componentes lógicos de *hardware* que pueden usarse incluyen circuitos integrados de aplicación específica (ASIC), Productos Estándares de aplicación específica (ASSP), sistemas de sistema en un chip (SOC), dispositivos lógicos programables complejos (CPLDs), etc. En varios ejemplos, el procesador(es) 202 y 302 puede ejecutar uno o más módulos y/o procesos para hacer que el servicio de validación de imagen 200 y el dispositivo de cómputo huésped 300 realicen operaciones para obtener una imagen, analizar la imagen para determinar si la imagen ha sido modificada, y generar una indicación de la probabilidad de que la imagen ha sido modificada. Además, cada uno de los procesadores 202 y 302 pueden poseer su propia memoria local, que también puede almacenar módulos de programa, datos de programa, y/o uno o más sistemas operativos.

Diagramas Ilustrativos

Las Figuras 4A y 4B son los diagramas ilustrativos de una imagen almacenada y una imagen que va a ser analizada mediante uno o más indicadores para determinar la probabilidad de que la imagen ha sido modificada.

La Figura 4A es una imagen ilustrativa 400, tal como una imagen que ha sido previamente analizada por un servicio de validación de imagen. En algunos ejemplos, la imagen 400 puede ser alternativamente una miniatura para otra imagen, tal como la imagen 402. Como se muestra en la Figura 4A, la imagen 400 puede comprender una representación electrónica de un objeto, tal como una tarjeta de prepago. La imagen 400 de la Figura 4A tiene varias características que han sido determinadas mediante un servicio de validación de imagen, tal como una porción de faltante 404, un producto 406, una fecha de expiración 408, una clave de producto 410 y un código legible por máquina 412 (por ejemplo, código de barras, código QR, etc.). Como se explicó anteriormente con relación a la Figura 2, el módulo de determinación de modificación 208 puede incluir un módulo de extracción de datos 210, el cual realiza varias técnicas, tales como técnicas de OCR, para extraer texto y otro tipo de información de una imagen.

La Figura 4B es una imagen ilustrativa 402 que también contiene una porción de faltante 414, un producto 416, una fecha de expiración 418 y un código legible por máquina 420. El texto de la imagen puede ser extraído o identificado por el módulo de extracción de datos 208, tal como, por ejemplo, mediante técnicas de OCR. Generalmente, el producto 416 puede indicar la presencia de un producto o servicio que es proporcionado por la tarjeta de prepago en la imagen 402, como una membresía o suscripción de 3 meses o 12 meses para un determinado servicio (por ejemplo, juegos en línea, acceso a la biblioteca de música, etc.). La fecha de expiración 418 puede indicar una fecha cuando la tarjeta de prepago ya no es válida y el código legible por máquina 420 es una representación legible por máquina de los datos asociados con la tarjeta de prepago.

En varios ejemplos, una vez que el módulo de extracción de datos 208 ha extraído el texto y/o los metadatos de las imágenes 400 y 402, el módulo de determinación de modificación 208 puede aplicar diversos indicadores, tales como el indicador(es) 112, al texto y metadatos para determinar la

probabilidad de que la imagen 402 ha sido modificada de su forma original. Por ejemplo, el módulo de determinación de modificación 208 puede analizar la imagen e identificar una diferencia de píxeles 422 que demuestra un cambio en la densidad de píxeles (u otra característica de píxeles) de una porción de la imagen a otra. El módulo de determinación de modificación 208 puede identificar un cambio de densidad de píxeles entre las porciones de la imagen 402, discrepancias de color del píxel o cualquier otro tipo de cambio de los píxeles entre las porciones de la imagen 402 que pueden indicar que la imagen 402 ha sido modificada. El cambio de características de píxeles puede indicar que la imagen 402 se ha editada, tal como al tener un parche con diferentes datos superpuestos en una porción de la imagen 402. Además, o alternativamente, la diferencia de píxeles 422 puede indicar que el objeto representado en la imagen ha sido modificado, tal como por tener corrector o cinta aplicada a él. En algunos ejemplos, la densidad de píxeles asociada con regiones de diferencia puede ser particularmente importante y ponderada en mayor escala tal como indicando la modificación, tal como los cambios de píxeles alrededor de claves de producto, fechas u otros datos sensibles de la imagen 402. En algunos ejemplos, el módulo de determinación de modificación 208 puede además identificar otros indicadores en el texto de la imagen 402 que sugieren la modificación. Por ejemplo, un carácter 424 puede ser identificado en una porción de la imagen, tal como la clave de producto, que no es apropiada para esa porción de la imagen 402. Como se muestra en la imagen 402, un carácter 424 ha sido identificado como una "y" minúscula, pero las claves de producto para este tipo de producto 416 no pueden utilizar caracteres en minúsculas, lo que puede sugerir que la letra se ha modificado o reemplazado. El uso de caracteres 424 que son inválidos para varias porciones de la imagen 402 puede indicar que la imagen 402 ha sido modificada.

En ejemplos en donde la imagen 400 comprende una miniatura asociada con la imagen 402, la miniatura y la imagen pueden compararse para determinar o identificar las diferencias entre las dos. Como se muestra en las Figuras 4A y 4B, existen varias similitudes entre la imagen 400 y la imagen 402, tales como porciones de faltante 404 y 414 y las fechas de expiración 408 y 418. Sin embargo, existen varias diferencias, tales como el producto 406 y el producto 416. Generalmente, una miniatura comprende una versión comprimida de una imagen que se asocia con o de otra manera se almacena con la imagen. La miniatura puede ser creada cuando se crea la imagen y se asemeja a las características de la imagen. Sin embargo, cuando se utiliza el *software* de edición en una imagen para modificar la imagen, las modificaciones no se pueden aplicar a la miniatura. Así pues, las diferencias entre la imagen de miniatura 400 y la imagen 402 pueden indicar que la imagen 402 fue modificada. Por consiguiente, dado que el producto 406 de la imagen 400 difiere del producto 416 de la imagen 402, el módulo de determinación de modificación 208 puede determinar que estas diferencias indican o sugieren la posibilidad de que la imagen 402 haya sido modificada de su forma original. Por ejemplo, un cliente puede intentar obtener una suscripción más larga a un servicio en particular al modificar la imagen 402.

Como se señaló anteriormente, la imagen 400 también puede representar una imagen que ha sido previamente analizada por el módulo de determinación de modificación 208 y se almacena en una base de datos para su posterior análisis, tal como el almacenamiento basado en nube 106. El módulo de

determinación de modificación 208 puede acceder al almacenamiento basado en nube 106 y comparar la imagen 400 con la imagen 402, o llamar a otro proceso o servicio basado en web para acceder al almacenamiento basado en nube 106 y comparar la imagen 400 con la imagen 402. El módulo de determinación de modificación 208 puede analizar la comparación entre la imagen 400 y la imagen 402 para identificar similitudes entre las imágenes. Por ejemplo, una similitud, tal como porciones de faltante 404 y 414 o código legible por máquina y 412 y código legible por máquina 420 puede ser identificada. Si hay similitudes entre las imágenes 400 y 402, o más de un umbral predeterminado de similitudes, esto puede indicar que la imagen 402 es una versión modificada de la imagen 400. Si la imagen 402 es una versión modificada de la imagen 400 que ha sido previamente presentada para soporte u otras concesiones, esto puede indicar además que la imagen 402 es una imagen modificada. Por ejemplo, un cliente puede haber guardado una imagen e intentar modificar la imagen ligeramente para obtener soporte o concesiones que no son elegibles. Por lo tanto, las similitudes identificadas por comparación entre imágenes previamente analizadas e imágenes actualmente analizadas pueden indicar que una imagen, tal como la imagen 402, ha sido modificada.

En algunos ejemplos, la información en el código legible por máquina 420 se puede utilizar para determinar si una imagen ha sido modificada, o si un objeto representado en la imagen ha sido modificado. Por ejemplo, el código legible por máquina 420 puede incluir datos que indican que la tarjeta de prepago en la imagen 402 es una tarjeta de membresía de 3 meses. Sin embargo, el producto 416 indica que la tarjeta de prepago es una membresía de 12 meses. Esta discrepancia en el tipo de producto indica que el producto 416 puede haber sido modificado por un cliente para obtener concesiones adicionales. Además, el módulo de determinación de modificación 208 puede comparar el código legible por máquina 420 con productos autorizados para determinar si ese código de barras particular es de un producto autorizado. Por ejemplo, el módulo de determinación de modificación 208 puede realizar una consulta en una base de datos de un comerciante que vende el producto en la imagen 402 para determinar si el código legible por máquina 420 está asociado con un producto válido o no se encuentra en la base de datos.

En varios ejemplos, el formato de varias porciones de la imagen 402 puede ser indicadores de la modificación de la imagen 402. Por ejemplo, la clave de producto 426 de la imagen 402 puede disponerse en un formato que no es apropiado para el producto 416. Por ejemplo, las claves de producto para un producto 416 de membresía de 12 meses pueden disponerse en un formato de 4x4, mientras que la clave de producto 426 está organizada en un formato de 5x5. Esto puede indicar que la clave de producto 426 y/o el producto 416 ha sido modificado en la imagen 402 basado en esta discrepancia de estructura de clave.

En varios ejemplos, el módulo de extracción de datos 210 puede extraer otros datos de la imagen 402. Por ejemplo, los datos de fuente que indican que el dispositivo de fuente de la imagen 402 pueden determinarse mediante el módulo de extracción de datos 210, tal como un ID de dispositivo, una dirección IP del dispositivo, un área geográfica del dispositivo, etc. Esta información puede indicar que la imagen 402 ha sido modificada. Por ejemplo, si los datos de fuente están asociados con un dispositivo que ha

presentado anteriormente imágenes modificadas, esto puede indicar que la imagen actual 402 también se modificó, o bien, requiere de otro análisis de profundidad. Además, los metadatos extraídos de la imagen 402 pueden indicar la modificación de la imagen 402. En un ejemplo, el módulo de extracción de datos 210 puede comparar los metadatos de la imagen 402, o llamar a un servicio o proceso externo para
5 comparar los metadatos de la imagen 402, con los metadatos de imágenes almacenadas en una base de datos para identificar las similitudes entre los metadatos. Si existen similitudes, o existen similitudes sobre un umbral predeterminado, esto puede indicar que la imagen 402 ha sido modificada desde una imagen previamente presentada. En otros ejemplos, los metadatos de la imagen 402 pueden haber sido borrados o sacados, lo que puede indicar que la imagen 402 ha sido modificada, también. Como se explicó
10 anteriormente, los metadatos de la imagen 402 pueden incluir la evidencia de uso de *software* de edición en la imagen 402. La evidencia del uso de *software* de edición puede ser un fuerte indicador de la modificación de la imagen 402.

En algunos ejemplos, varias fechas asociadas con la imagen 402 pueden indicar la modificación de la imagen 402. Por ejemplo, una fecha de cuando se capturó la imagen puede ser comparada con la
15 fecha de cuando se compró el producto. Si la fecha de cuando la imagen 402 se creó precede a la fecha de cuando el producto fue supuestamente adquirido por el cliente, esto puede indicar que la imagen 402 ha sido modificada porque el cliente no tenía la posesión de la tarjeta de prepago en la imagen 402 para crear la imagen del producto antes de la fecha en que supuestamente se compró el producto.

En varios ejemplos, se pueden emplear otras técnicas por el módulo de determinación de
20 modificación 208 para determinar si la imagen 402 ha sido modificada, o si un objeto representado en la imagen 402 ha sido modificado. Por ejemplo, se pueden utilizar técnicas de análisis de nivel de error (ELA, según sus siglas en inglés) para determinar si una porción de la imagen 402 no es original o se ha editado. El módulo de determinación de modificación 208 puede emplear técnicas de ELA para procesar la imagen y producir un resultado, en donde las regiones que son claramente de una fuente diferente a la
25 de la imagen original se resaltan, lo cual su vez se utiliza para determinar si la imagen 402 ha sido alterada.

En algunos ejemplos, el dispositivo(s) de cómputo huésped 102 y/o el servicio de validación de imagen 104 puede extraer datos (es decir, metadatos) de otras imágenes almacenadas en un dispositivo de cómputo de presentación (es decir, dispositivo de cómputo de cliente) que ha presentado la imagen
30 402 al dispositivo(s) de cómputo huésped 102 para verificación para determinar si la imagen 402 ha sido modificada. Por ejemplo, el dispositivo(s) de cómputo huésped 102 y/o el servicio de validación de imagen 104 puede extraer metadatos asociados con otras imágenes almacenadas en el dispositivo de cómputo de presentación. El servicio de validación de imagen 104 puede comparar los metadatos asociados con las otras imágenes almacenadas en el dispositivo de cómputo de presentación con los
35 metadatos extraídos de la imagen 402 para identificar las diferencias entre los distintos metadatos. Las diferencias detectadas entre los metadatos de las imágenes almacenadas en el dispositivo de presentación y la imagen 402 presentada para verificación pueden indicar que la imagen 402 ha sido verificada. Como un ejemplo, muchos dispositivos de cómputo almacenan o dividen imágenes en

diferentes carpetas, ubicaciones o archivos en un dispositivo de cómputo. Una imagen capturada por el dispositivo de cómputo puede almacenarse en una ubicación o carpeta llamada "Cámara", mientras que una imagen que se ha descargado al dispositivo de cómputo (es decir, no capturada) puede almacenarse en una ubicación o carpeta llamada "Descargas" y una captura de pantalla puede ser almacenada en una carpeta o ubicación llamada "Capturas de pantalla". Si los metadatos obtenidos o extraídos de las otras imágenes almacenadas en el dispositivo de cómputo de presentación indican que se almacenaron en la carpeta o ubicación de "Cámara", pero los metadatos de la imagen 402 indican que la imagen se almacenó en la carpeta o ubicación de "Descargas", esta diferencia puede indicar que la imagen 402 fue modificada ya que no fue capturada por el dispositivo de cómputo de presentación, pero en lugar de eso fue descargada de una fuente tal como Internet.

En algunos ejemplos, los dispositivos utilizados por los clientes para presentar imágenes pueden indicar la modificación de la imagen 402. Por ejemplo, si un cliente particular ha presentado anteriormente una imagen cuyos metadatos indican que fue capturada y/o presentada por un primer dispositivo de cómputo, y los metadatos de la imagen 402 indican que fue capturada y/o presentada con un segundo dispositivo de cómputo diferente, esto puede indicar que la imagen fue modificada. Por ejemplo, el primer dispositivo de cómputo puede ser un teléfono móvil y el segundo dispositivo de cómputo puede ser una computadora portátil. Esto puede indicar que la imagen 402 ha sido modificada porque una computadora de escritorio o portátil puede tener capacidades de *software* de edición de imagen requeridas para modificar la imagen 402, mientras que un teléfono móvil puede no tener esas capacidades. Por lo tanto, una imagen previamente presentada desde un cliente utilizando un primer dispositivo distinto de un segundo dispositivo de cómputo utilizado para presentar la imagen 402 puede indicar esa imagen 402 fue modificada.

El módulo de determinación de modificación 208 puede emplear uno o cualquier combinación de los indicadores anteriores para determinar si la imagen 402 ha sido modificada o si un objeto representado en la imagen ha sido modificado. Los indicadores pueden ser ponderados por el módulo de ponderación 214 en mayor o menor medida para mostrar la modificación de la imagen 402. El módulo de determinación de modificación 208 puede utilizar los diversos indicadores explicados anteriormente para determinar la probabilidad de que la imagen 402 ha sido modificada. Si la probabilidad de modificación cae en diversos umbrales o rangos, entonces los resultados pueden ser tales como "alteración detectada", "alteración probable" o "ninguna alteración detectada". Aunque las técnicas se explican con referencia a una tarjeta de prepago, otros tipos de documentos en imágenes se pueden analizar utilizando técnicas similares, tales como garantías, recibos, informes de gastos, etc.

Procesos Ilustrativos

Los procesos descritos en las Figuras 5-7 a continuación se ilustran como una colección de bloques en una gráfica de flujo lógico, que representan una secuencia de operaciones que se pueden implementar en *hardware*, *software* o una combinación de los mismos. En el contexto de *software*, los bloques representan instrucciones ejecutables por computadora almacenadas en uno o más medios de

almacenamiento legibles por computadora que, cuando se ejecutan por uno o más procesadores, realizan las operaciones citadas. Generalmente, las instrucciones ejecutables por computadora incluyen rutinas, programas, objetos, componentes, estructuras de datos y similares que realizan determinadas funciones o implementan determinados tipos de datos abstractos. El orden en el que se describen las operaciones no está pensado para ser interpretada como una limitación, y cualquier número de los bloques descritos se puede combinar en cualquier orden y/o en paralelo para implementar los procesos. Los procesos descritos a continuación pueden realizarse por módulos almacenados en uno o más de servicio de validación de imagen 200 y/o dispositivo de cómputo huésped 300, tal como el módulo de determinación de modificación 208 y aplicación(es) web 308.

La Figura 5 es un diagrama de flujo que muestra un proceso ilustrativo 500 para determinar la autenticidad de una imagen basándose en indicadores y generando una indicación de la probabilidad de que la imagen ha sido modificada de su forma original.

En el bloque 502, un servicio de validación de imagen 200 puede obtener (por ejemplo, recibir, acceder, etc.) una imagen para su verificación.

En el bloque 504, un módulo de determinación de modificación 208 puede determinar la autenticidad de la imagen basándose por lo menos en dos operaciones. Las operaciones pueden incluir las operaciones de los bloques 506-512.

En el bloque 506, el módulo de determinación de modificación 208 puede analizar la imagen para detectar un cambio en la densidad de píxeles de una primera porción de la imagen a una segunda porción de la imagen.

En el bloque 508, el módulo de determinación de modificación 208 puede comparar la imagen con una miniatura de la imagen para detectar una diferencia entre la imagen y la miniatura.

En el bloque 510, el módulo de determinación de modificación 208 puede analizar los datos asociados con la imagen para determinar si se ha utilizado el *software* de edición en la imagen.

En el bloque 512, el módulo de determinación de modificación 208 puede analizar los datos asociados con la imagen para determinar, al menos de uno de un tiempo en el que se capturó la imagen o una ubicación geográfica en la que se capturó la imagen.

En el bloque 514, el servicio de validación de imagen 200 puede producir, a través de una o más interfaces de red 218, una indicación de la probabilidad de que la imagen ha sido modificada. En algunos ejemplos, la salida puede basarse al menos en parte en la determinación de la autenticidad de la imagen.

La Figura 6 es un diagrama de flujo que muestra un proceso ilustrativo 600 para obtener una imagen que será verificada según modificada o no, enviar la imagen a ser analizada y producir una indicación de la probabilidad de que la imagen ha sido modificada de su forma original.

En el bloque 602, un dispositivo de cómputo huésped 300 puede obtener una imagen que será verificada.

En el bloque 604, el dispositivo de cómputo huésped 300 puede enviar la imagen, por una API web 310 y a través de uno o más interfaces de red 312, a un servicio de verificación de imagen para verificar que la imagen está siendo alterada o no se basa en un análisis multifactorial.

En el bloque 606, el dispositivo de cómputo huésped puede recibir, a través de una o más interfaces de red 312, una indicación de la probabilidad de que la imagen ha sido alterada.

En el bloque 608, el dispositivo de cómputo huésped 300 puede producir, a través de una interfaz de usuario de la aplicación web 308, la indicación de la probabilidad de que la imagen ha sido alterada.

5 La Figura 7 es un diagrama de flujo que muestra un proceso ilustrativo 700 para analizar una imagen digital para determinar la probabilidad de que al menos una de las imágenes digitales o un objeto representado en la imagen digital ha sido modificado basándose en al menos dos operaciones, y produciendo una indicación de la probabilidad de que la imagen digital o el objeto representado en la imagen se ha modificado de su forma original.

10 En el bloque 702, un servicio de validación de imagen 200 puede obtener (por ejemplo, recibir, acceder, etc.) una imagen digital para su verificación.

En el bloque 704, un módulo de determinación de modificación 208 del servicio de validación de imagen 200 puede analizar la imagen digital para determinar la probabilidad de que al menos una de las imágenes digitales o un objeto representado en la imagen digital ha sido modificado, en donde el análisis se compone de al menos dos operaciones. Las operaciones pueden incluir cualquiera de las operaciones de los bloques 706-712.

En el bloque 706, el módulo de determinación de modificación 208 puede analizar la imagen digital para detectar un cambio en la densidad de píxeles de una primera porción de la imagen digital a una segunda porción de la imagen digital.

20 En el bloque 708, el módulo de determinación de modificación 208 puede comparar la imagen digital con una miniatura de la imagen digital para detectar una diferencia entre la imagen digital y la miniatura.

En el bloque 710, el módulo de determinación de modificación 208 puede analizar los metadatos de la imagen digital para determinar si se ha utilizado el *software* de edición en la imagen digital.

25 En el bloque 712, el módulo de determinación de modificación 208 puede analizar una comparación entre la imagen digital y una imagen digital almacenada para identificar similitudes entre la imagen digital y la imagen digital almacenada.

En el bloque 714, el servicio de validación de imagen 200 puede producir una indicación, a través de una o más interfaces de red 218, de la probabilidad de que al menos uno de la imagen digital o el objeto representado en la imagen digital ha sido modificado. En algunos ejemplos, el servicio de validación de imagen 200 puede producir la indicación basándose, al menos en parte, en el análisis de la imagen digital.

Cláusulas Ilustrativas

35 A. Un sistema de validación de imagen que comprende: uno o más procesadores; y una memoria comunicativamente acoplada a uno o más de los procesadores y que almacena uno o más módulos que, cuando se ejecutan mediante el uno o más procesadores, hacen que el sistema de validación de imagen realice operaciones que comprenden: obtener, de un dispositivo de cómputo, una

imagen para verificación; en respuesta a la obtención de la imagen, determinar la autenticidad de la imagen basándose en al menos dos de las siguientes operaciones: analizar la imagen para detectar un cambio en la densidad de píxeles de una primera porción de la imagen a una segunda porción de la imagen; comparar la imagen con una miniatura de la imagen para detectar una diferencia entre la imagen y la vista en miniatura; analizar los datos asociados con la imagen para determinar si el *software* de edición de imagen ha sido utilizado en la imagen; y analizar los datos asociados con la imagen para identificar al menos uno de un tiempo en el que se capturó la imagen o una ubicación geográfica en la que se capturó la imagen; y generar una indicación, basada al menos en parte en la determinación de la autenticidad de la imagen, de la probabilidad de que la imagen ha sido modificada.

B. Un sistema de validación de imagen como el párrafo A recita, en donde las operaciones además comprenden realizar el reconocimiento óptico de caracteres en la imagen para identificar el texto incluido en la imagen; y en donde la determinación de la autenticidad de la imagen incluye además: determinar que un código legible por máquina incluido en el texto de la imagen está asociado con un producto particular; determinar que una clave de producto incluida en el texto de la imagen está en un formato adecuado para las claves de producto; y determinar que la clave de producto incluida en el texto de la imagen incluye uno o más caracteres inválidos.

C. Un sistema de validación de imagen como el párrafo A o B recita, en donde la imagen se compone de un comprobante de compra; y en donde la indicación de la probabilidad de que la imagen ha sido modificada comprende una indicación de que la imagen es una prueba válida de compra.

D. Un sistema de validación de imagen como cualquiera de los párrafos A-C recita, en donde cada una de las operaciones está asociada con un factor de ponderación; y en donde la determinación de la autenticidad de la imagen incluye además: aplicar un factor de ponderación respectivo a cada una de al menos dos operaciones para crear al menos dos operaciones ponderadas; y determinar la probabilidad de que la imagen se ha modificado basándose, al menos en parte, en al menos dos operaciones ponderadas.

E. Un sistema de validación de imagen como cualquiera de los párrafos A-D recita, en donde la generación de la indicación de la probabilidad comprende: determinar que la probabilidad de que la imagen se ha modificada está por encima de un primer umbral de probabilidad, por debajo de un segundo umbral de probabilidad, o entre el primer umbral de probabilidad y el segundo umbral de probabilidad; y en respuesta a la determinación de que la probabilidad de que la imagen ha sido modificada está por encima del primer umbral de probabilidad, generar la indicación para el dispositivo de cómputo indicando que la modificación de la imagen ha sido detectada.

F. Un sistema de validación de imagen como cualquiera de los párrafos A-E recita, en donde la generación de la indicación de la probabilidad comprende: determinar que la probabilidad de que la imagen se ha modificado está por encima de un primer umbral de probabilidad, por debajo de un segundo umbral de probabilidad, o entre el primer umbral de probabilidad y el segundo umbral de probabilidad; y en respuesta a la determinación de que la probabilidad de que la imagen ha sido modificada está por debajo del segundo umbral de probabilidad, generar la indicación para el dispositivo

de cómputo indicando que la modificación de la imagen no ha sido detectada.

G. Un sistema de validación de imagen como cualquiera de los párrafos A-F recita, en donde la generación de la indicación de la probabilidad comprende: determinar que la probabilidad de que la imagen se ha modificado está por encima de un primer umbral de probabilidad, por debajo de un segundo umbral de probabilidad, o entre el primer umbral de probabilidad y el segundo probabilidad umbral; y en respuesta a la determinación de que la probabilidad de que la imagen ha sido modificada se encuentra entre el primer umbral de probabilidad y el segundo umbral de probabilidad, generar la indicación para el dispositivo de cómputo indicando que la modificación de la imagen es probable.

H. Un sistema de validación de imagen como el párrafo G recita, en donde las operaciones además comprenden: enviar una solicitud al dispositivo de cómputo para obtener información adicional, la información adicional comprendiendo al menos uno de los siguientes: una imagen adicional del objeto representado en la imagen, la imagen adicional que captura el objeto desde un ángulo diferente de un ángulo a partir del cual se capturó la imagen; o un video del objeto contenido en la imagen.

I. Un sistema de validación de imagen como cualquiera de los párrafos A-H recita, en donde al menos dos operaciones además incluyen: comparar al menos uno de los siguientes: características de la imagen con las características de una imagen almacenada; o los metadatos de la imagen con los metadatos de la imagen almacenada.

J. Un sistema de validación de imagen como cualquiera de los párrafos A-I recita, en donde la probabilidad de que la imagen ha sido modificada incluye una probabilidad de que un objeto representado en la imagen ha sido modificado.

K. Un método implementado por computadora que comprende, a través de un dispositivo de cómputo, una imagen que será verificada; enviar, por el dispositivo de cómputo, la imagen a un servicio de verificación de imagen para determinar si la imagen ha sido alterada o no se basa en un análisis multifactorial; recibir, en el dispositivo de cómputo y desde el servicio de verificación de imagen, una indicación de la probabilidad de que la imagen ha sido alterada; y generar, por el dispositivo de cómputo, la indicación de la probabilidad de que la imagen ha sido alterada.

L. Un método implementado por computadora como el párrafo K recita, que además comprende: recibir metadatos asociados con la imagen y el análisis realizado por el servicio de verificación de imagen; y causar que la imagen, la probabilidad, los metadatos y el análisis para sean almacenados en un almacenamiento de datos.

M. Un método implementado por computadora como el párrafo K o L recita, que además comprende: identificar información adicional asociada con la imagen, la información adicional incluyendo al menos uno de un identificación de dispositivo (ID) de un dispositivo de cómputo de consumidor asociado con la imagen, una dirección de Protocolo de Internet (IP) asociada con el dispositivo de cómputo de consumidor o una ubicación geográfica asociada con el dispositivo de cómputo de consumidor; y enviar la información adicional al servicio de verificación de imagen.

N. Un método implementado por computadora como cualquiera de los párrafos K-M recita, en donde el enviar la imagen al servicio de verificación de imagen comprende presentar la imagen a una

interfaz de programa de aplicación (API) asociada con el servicio de verificación de imagen.

O. Un método implementado por computadora como cualquiera de los párrafos K-O recita, en donde la indicación de la probabilidad de que la imagen ha sido alterada comprende una indicación de que la alteración es probable, y en donde el método implementado por computadora comprende además
5 generar, por el dispositivo de cómputo, una solicitud de información adicional para determinar si la imagen ha sido alterada o no.

P. Un método implementado por computadora que comprende: obtener, a través de un dispositivo de cómputo, una imagen digital para su verificación; en respuesta a la obtención de la imagen digital, analizar la imagen digital para determinar la probabilidad de que al menos una de la imagen digital
10 o un objeto representado en la imagen digital ha sido modificado, el análisis comprende al menos dos de las siguientes operaciones: analizar la imagen digital para detectar un cambio en la densidad de píxeles de una primera porción de la imagen digital a una segunda porción de la imagen digital; comparar la imagen digital con una miniatura de la imagen digital para detectar una diferencia entre la imagen digital y la vista en miniatura; analizar los metadatos de la imagen digital para determinar si el *software* de edición
15 ha sido utilizado en la imagen digital; y analizar una comparación entre la imagen digital y una imagen digital almacenada para identificar similitudes entre la imagen digital y la imagen digital almacenada; y generar una indicación, basándose al menos en parte en el análisis de la imagen digital, de la probabilidad de que al menos uno de la imagen digital o el objeto representado en la imagen digital ha sido modificado.

Q. Un método implementado por computadora tal como el párrafo P recita, en donde las operaciones además incluyen al menos uno de los siguientes: determinar que un código legible por máquina incluido en la imagen digital está asociado con un producto particular; determinar que una clave de producto incluida en la imagen digital está en un formato apropiado para las claves de producto; o
20 determinar que la clave de producto incluida en la imagen digital incluya caracteres inválidos para las claves de producto.
25

R. Un método implementado por computadora tal como el párrafo P o Q recita, en donde las operaciones incluyen además al menos uno de los siguientes: analizar los datos asociados con la imagen digital para identificar una fuente de la imagen digital; o analizar los datos asociados con la imagen digital para identificar una fecha de cuando se creó la imagen digital.

S. Un método implementado por computadora tal como cualquiera de los párrafos P-R recita, en donde el análisis de la imagen digital para determinar la probabilidad de que al menos uno de la imagen digital o el objeto representado en la imagen digital ha sido modificado comprende: aplicar un factor de ponderación para al menos dos operaciones para crear al menos dos operaciones ponderadas; y determinar la probabilidad de que al menos uno de la imagen digital o el objeto representado en la
30 imagen digital ha sido modificado basándose, al menos en parte, en al menos dos operaciones ponderadas.
35

T. Un método implementado por computadora tal como cualquiera de los párrafos P-S recita, en donde la indicación de la probabilidad de que al menos uno de la imagen digital o el objeto

representado en la imagen digital ha sido modificado comprende al menos uno de una indicación de que se ha detectado una alteración, la alteración no ha sido detectada, o la alteración es probable.

U. Uno o más medios legibles por computadora codificados con instrucciones que, cuando se ejecutan en un procesador, configuran una computadora para realizar un método implementado por computadora como cualquiera de los párrafos K-T recita.

V. Un dispositivo que consta de uno o más procesadores y uno o más medios legibles por computadora codificados con instrucciones que, cuando se ejecutan mediante uno o más procesadores, configuran una computadora para realizar un método implementado por computadora como cualquiera de los párrafos K-T recita.

Conclusión

Para cerrar, aunque las varias modalidades han sido descritas en el lenguaje específico de características estructurales y/o actos metodológicos, se entiende que la materia objeto definida en las representaciones anexas no está necesariamente limitada a las características o actos específicos descritos. Más bien, las características específicas y los actos se describen como formas ilustrativas para implementar la materia objeto reclamada.

REIVINDICACIONES

1. Un sistema de validación de imagen que comprende:

uno o más procesadores; y

5 memoria comunicativamente acoplada a uno o más de los procesadores y almacenando uno o más módulos que, cuando se ejecutan mediante uno o más de los procesadores, hacen que el sistema de validación de imagen realice operaciones que comprenden:

obtener, a partir de un dispositivo de cómputo, una imagen para verificación;

en respuesta a la obtención de la imagen, determinar la autenticidad de la imagen

10 basándose en al menos dos de las siguientes operaciones:

analizar la imagen para detectar un cambio en la densidad de píxeles de una primera porción de la imagen a una segunda porción de la imagen;

comparar la imagen con una miniatura de la imagen para detectar una diferencia entre la imagen y la imagen en miniatura;

15 analizar los datos asociados con la imagen para determinar si el *software* de edición de imagen ha sido utilizado en la imagen; y

analizar los datos asociados con la imagen para identificar al menos uno de un tiempo en el que se capturó la imagen o una ubicación geográfica en la que la imagen se capturó; y

20 generar una indicación, basándose al menos en parte en la determinación de la autenticidad de la imagen, de la probabilidad de que la imagen ha sido modificada.

2. El sistema de validación de imagen de acuerdo con la reivindicación 1, en donde las operaciones además comprenden realizar el reconocimiento óptico de caracteres en la imagen para identificar el texto incluido en la imagen; y

25 en donde la determinación de la autenticidad de la imagen incluye además:

determinar que un código legible por máquina incluido en el texto de la imagen está asociado con un producto particular;

determinar que una clave de producto incluida en el texto de la imagen está en un formato apropiado para las claves de producto; y

30 determinar que la clave de producto incluida en el texto de la imagen incluye uno o más caracteres inválidos.

3. El sistema de validación de imagen de acuerdo con la reivindicación 1 o reivindicación 2, en donde la imagen comprende un comprobante de compra; y en donde la indicación de la probabilidad de que la imagen ha sido modificada incluye una indicación de que la imagen es de un comprobante

35 válido de compra.

4. El sistema de validación de imagen de acuerdo con cualquiera de las reivindicaciones 1-3, en donde cada una de las operaciones está asociada con un factor de ponderación; y

en donde determinar la autenticidad de la imagen incluye además:

aplicar un factor de ponderación respectivo a cada una de los al menos dos operaciones para crear al menos dos operaciones ponderadas; y

determinar la probabilidad de que la imagen se ha modificada basándose, al menos en parte, en al menos dos operaciones ponderadas.

5 5. El sistema de validación de imagen de acuerdo con cualquiera de las reivindicaciones 1-4, en donde la generación de la indicación de la probabilidad comprende:

determinar que la probabilidad de que la imagen se ha modificado está por encima de un primer umbral de probabilidad, por debajo de un segundo umbral de probabilidad, o entre el primer umbral de probabilidad y el segundo umbral de probabilidad; y

10 en respuesta a la determinación de que la probabilidad de que la imagen ha sido modificada está por encima de un primer umbral de probabilidad, generar la indicación para el dispositivo de cómputo indicando que la modificación de la imagen ha sido detectada.

6. El sistema de validación de imagen de acuerdo con cualquiera de las reivindicaciones 1-4, en donde la generación de la indicación de la probabilidad comprende:

15 determinar que la probabilidad de que la imagen se ha modificado está por encima de un primer umbral de probabilidad, por debajo de un segundo umbral de probabilidad, o entre el primer umbral de probabilidad y el segundo umbral de probabilidad; y

20 en respuesta a la determinación de que la probabilidad de que la imagen ha sido modificada está por debajo de un segundo umbral de probabilidad, generar la indicación para el dispositivo de cómputo indicando que la modificación de la imagen no ha sido detectada.

7. El sistema de validación de imagen de acuerdo con cualquiera de las reivindicaciones 1-4, en donde la generación de la indicación de la probabilidad comprende:

25 determinar que la probabilidad de que la imagen se ha modificado está por encima de un primer umbral de probabilidad, por debajo de un segundo umbral de probabilidad, o entre el primer umbral de probabilidad y el segundo umbral de probabilidad; y

en respuesta a la determinación de que la probabilidad de que la imagen ha sido modificada se encuentra entre el primer umbral de probabilidad y el segundo umbral de probabilidad, generar la indicación para el dispositivo de cómputo indicando que la modificación de la imagen es probable.

30 8. El sistema de validación de imagen de acuerdo con la reivindicación 7, en donde las operaciones además comprenden:

enviar una solicitud al dispositivo de cómputo para obtener información adicional, la información adicional comprendiendo al menos uno de los siguientes:

35 una imagen adicional del objeto representado en la imagen, la imagen adicional capturando el objeto desde un ángulo diferente de un ángulo desde el que se capturó la imagen;

o

un video del objeto contenido en la imagen.

9. El sistema de validación de imagen de acuerdo con cualquiera de las reivindicaciones 1-8, en donde al menos dos operaciones además incluyen:

comparar al menos uno de los siguientes:

características de la imagen con las características de una imagen almacenada; o
metadatos de la imagen con los metadatos de la imagen almacenada.

10. El sistema de validación de imagen de acuerdo con cualquiera de las reivindicaciones 1-9, en donde la probabilidad de que la imagen ha sido modificada incluye una probabilidad de que un objeto representado en la imagen ha sido modificado.

11. Un método implementado por computadora, que comprende:
obtener, a través de un dispositivo de cómputo, una imagen que será verificada;
enviar, por el dispositivo de cómputo, la imagen a un servicio de verificación de imagen para determinar si la imagen ha sido alterada o no basándose en un análisis multifactorial;
recibir, en el dispositivo de cómputo y desde el servicio de verificación de imagen, una indicación de la probabilidad de que la imagen ha sido alterada; y
generar, por el dispositivo de cómputo, la indicación de la probabilidad de que la imagen ha sido alterada.

12. El método implementado por computadora de acuerdo con la reivindicación 11, que además comprende:

recibir metadatos asociados con la imagen y el análisis realizado por el servicio de verificación de la imagen; y

hacer que la imagen, la probabilidad, los metadatos y el análisis sean almacenados en un almacenamiento de datos.

13. El método implementado por computadora de acuerdo con la reivindicación 11 o reivindicación 12, que además comprende:

identificar información adicional asociada con la imagen, la información adicional incluyendo al menos uno de una identificación de dispositivo (ID) de un dispositivo de cómputo de consumidor asociado con la imagen, una dirección de Protocolo de Internet (IP) asociada con el dispositivo de cómputo de consumidor, o una ubicación geográfica asociada con el consumidor dispositivo de cómputo; y

enviar la información adicional al servicio de verificación de la imagen.

14. El método implementado por computadora de acuerdo con cualquiera de las reivindicaciones 11-13, en donde la indicación de la probabilidad de que la imagen ha sido alterada comprende una indicación de que la alteración es probable, y en donde el método implementado por computadora comprende además generar, por el dispositivo de cómputo, una solicitud de información adicional para determinar si la imagen ha sido alterada o no.

15. Un método implementado por computadora, que comprende:
obtener, a través de un dispositivo de cómputo, una imagen digital para su verificación;
en respuesta a la obtención de la imagen digital, analizar la imagen digital para determinar la probabilidad de que al menos una de la imagen digital o un objeto representado en la imagen digital ha sido modificado, el análisis comprende al menos dos de las siguientes operaciones:

analizar la imagen digital para detectar un cambio en la densidad de píxeles de una

primera porción de la imagen digital a una segunda porción de la imagen digital;

comparar la imagen digital con una miniatura de la imagen digital para detectar una diferencia entre la imagen digital y la miniatura de la imagen digital;

analizar los metadatos de la imagen digital para determinar si se ha utilizado el *software* de edición en la imagen digital; y

analizar una comparación entre la imagen digital y una imagen digital almacenada para identificar similitudes entre la imagen digital y la imagen digital almacenada; y

generar una indicación, basándose al menos en parte en el análisis de la imagen digital, de la probabilidad de que al menos uno de la imagen digital o el objeto representado en la imagen digital ha sido modificado.

RESUMEN

Un proceso automatizado para determinar si una imagen ha sido modificada incluye recibir una imagen (por ejemplo, a través de un portal web), solicitar un servicio de validación de imagen para
5 analizar la imagen para determinar si la imagen y/o un objeto representado en la imagen ha sido
modificado de su forma original y, basándose en el análisis del servicio de validación de imagen, generar
la probabilidad de que la imagen ha sido modificada. El servicio de validación de imagen puede analizar
la imagen utilizando una o más operaciones para determinar la probabilidad de que la imagen ha sido
modificada y proporcionar una indicación de que la probabilidad de que la imagen ha sido modificada al
10 portal web. La indicación de la probabilidad de que la imagen ha sido modificada se puede presentar en
una pantalla a través del portal web y se pueden sugerir o tomar varias acciones con base en la
probabilidad de que la imagen ha sido modificada.

15

20

25

30

35

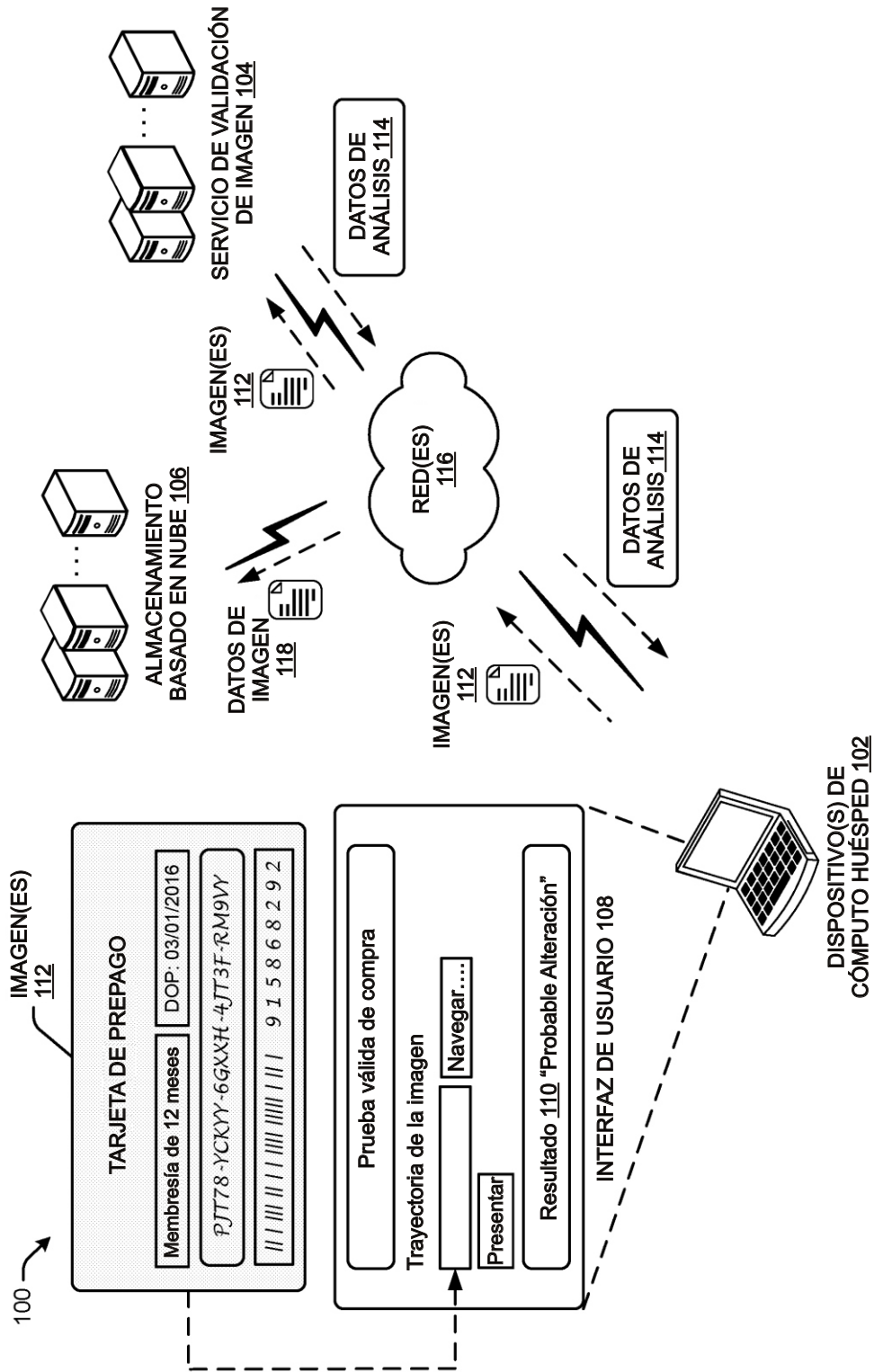


FIG. 1

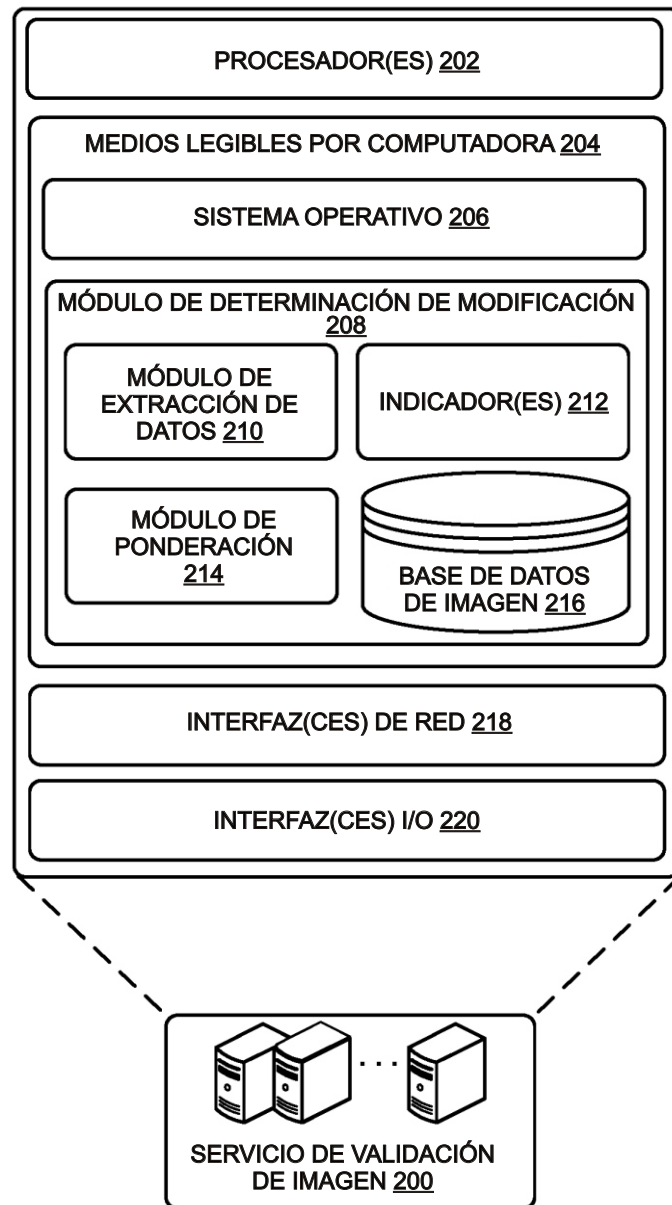


FIG. 2

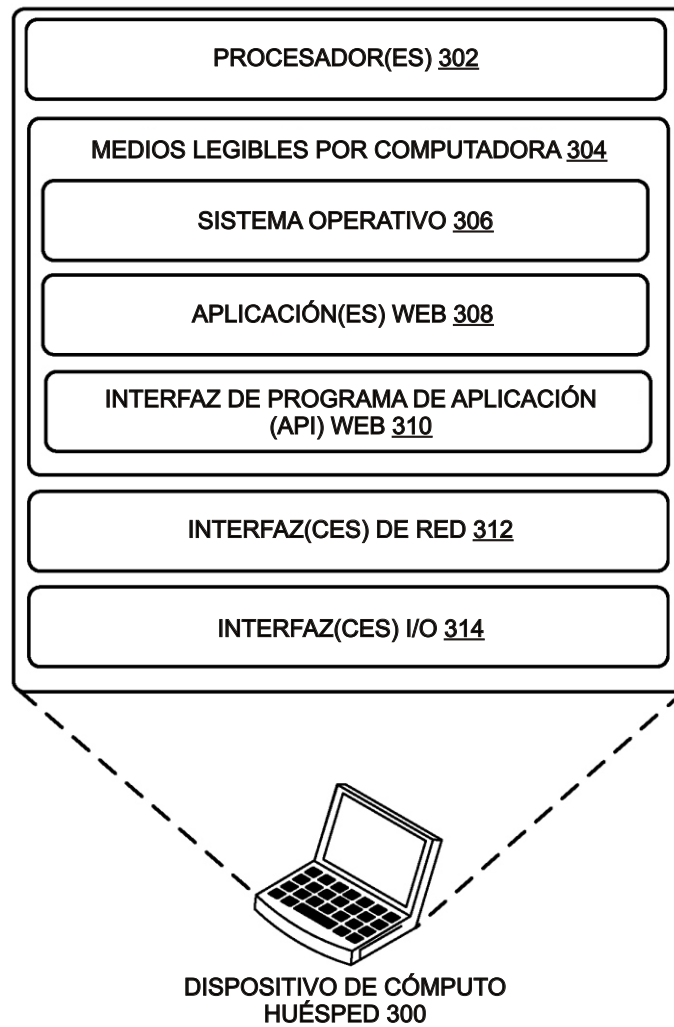


FIG. 3

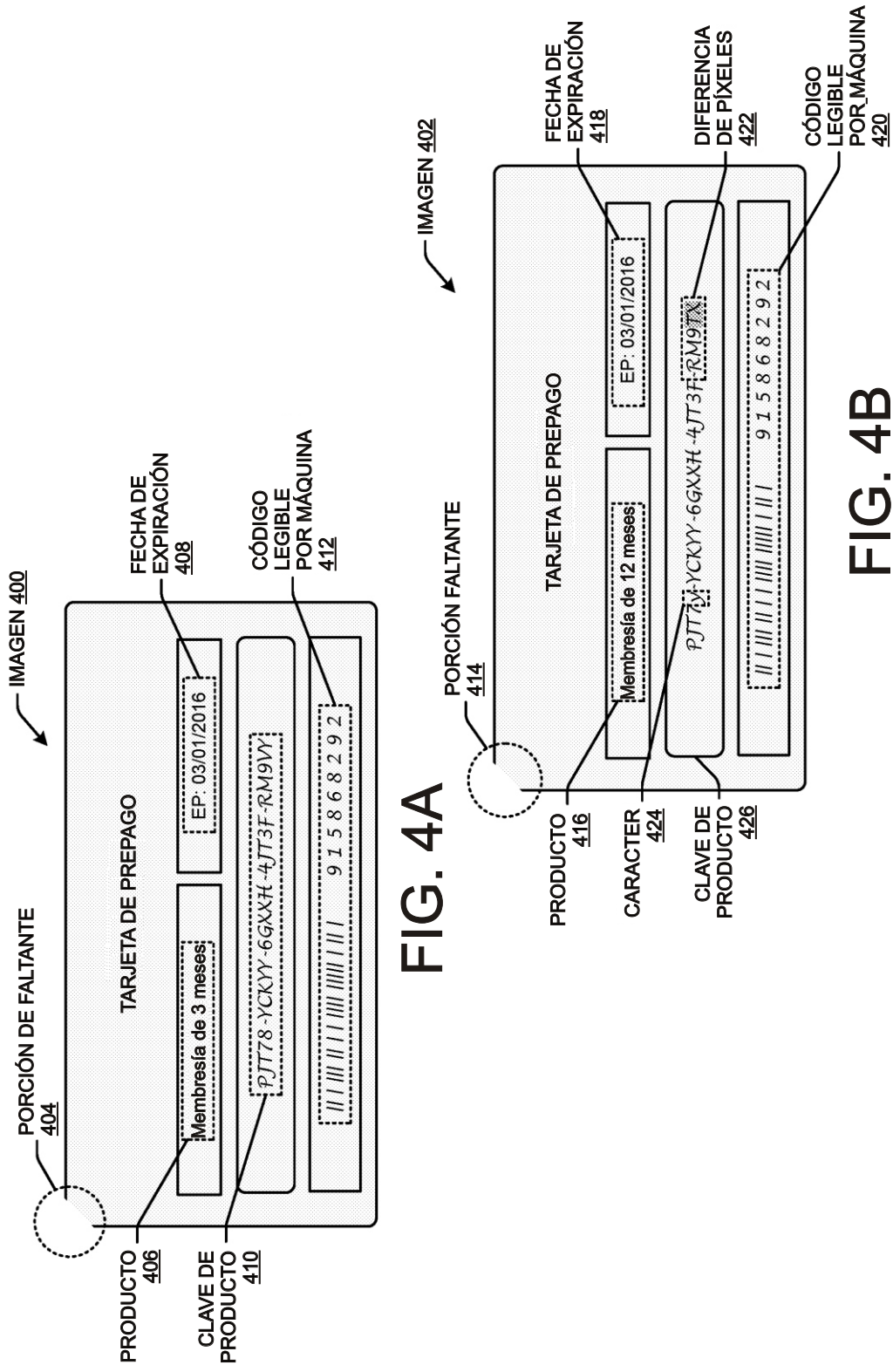


FIG. 4B

500

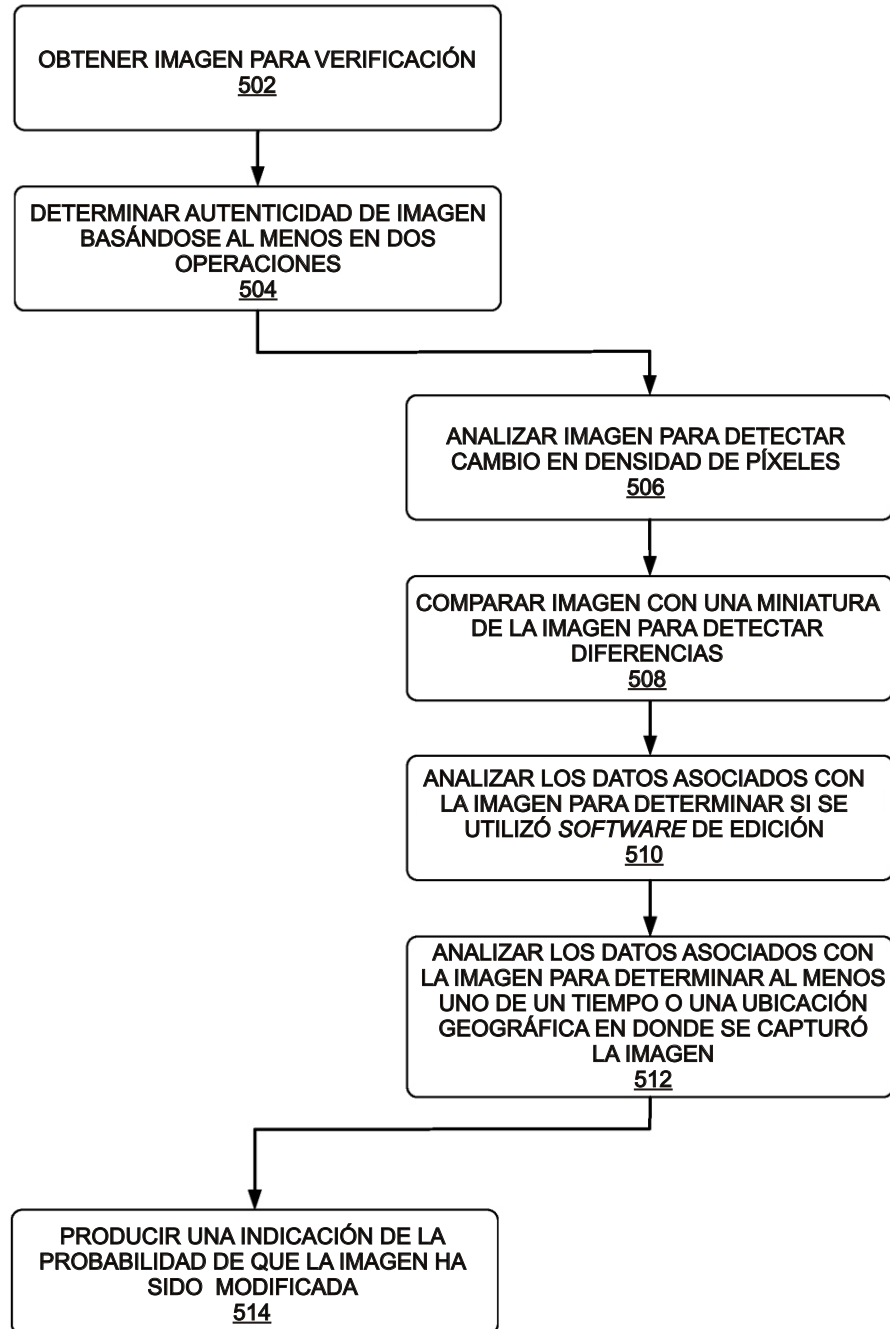


FIG. 5

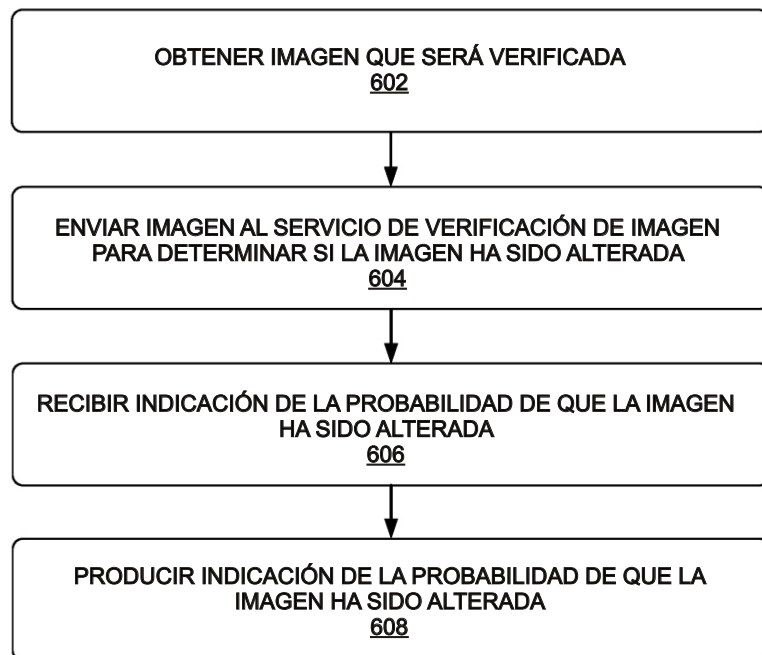
600 

FIG. 6

700

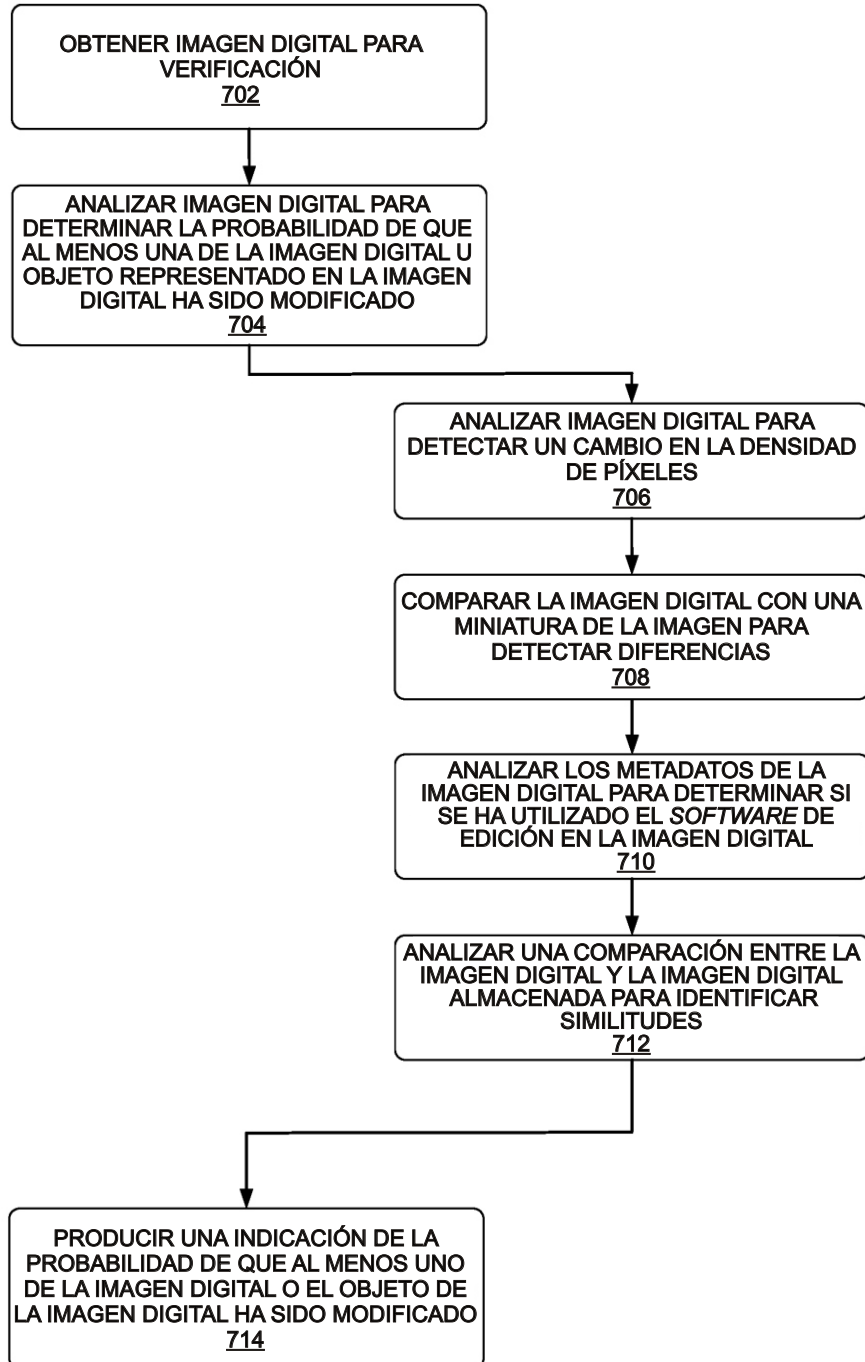


FIG. 7