(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 723 698**

(51) Int. CI.:

G06F 21/36 (2013.01)
H04L 29/06 (2006.01)
H04W 12/06 (2009.01)
H04L 9/06 (2006.01)
H04L 9/08 (2006.01)
H04L 9/14 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.04.2016 PCT/CN2016/080561**

(87) Fecha y número de publicación internacional: **16.03.2017 WO17041494**

(96) Fecha de presentación y número de la solicitud europea: **28.04.2016 E 16843433 (0)**

(97) Fecha y número de publicación de la concesión europea: **27.03.2019 EP 3264309**

(54) Título: **Método de procesamiento de la información y terminal, y medio de almacenamiento informático**

(30) Prioridad:

08.09.2015 CN 201510567786

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.08.2019

(73) Titular/es:

TENCENT TECHNOLOGY SHENZHEN COMPANY LIMITED (100.0%)
Room 403 East Block 2 SEG Park Zhenxing Road Futian District
Shenzhen, Guangdong 518044, CN

(72) Inventor/es:

QIU, ZHIGUANG y
HOU, XIN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método de procesamiento de la información y terminal, y medio de almacenamiento informático

Campo técnico

La descripción se relaciona con el campo técnico de las comunicaciones, y en concreto, con un método de procesamiento de la información, un terminal y un medio de almacenamiento informático.

Antecedentes

Una contraseña convencional es una contraseña creada mediante una cadena de caracteres alfanuméricos, y el usuario es requerido a recordar esta contraseña de cadena de caracteres, e introducir esta contraseña cuando se requiere verificación.

Adoptar una manera existente de verificación por contraseña puede no proporcionar una buena experiencia de usuario, y no es muy conveniente. Una contraseña que es demasiado complicada es difícil de memorizar e introducir. Una contraseña que es demasiado simple es inferior en cuanto a seguridad y fácil de imitar, y un pirata informático puede hacer una contraseña idéntica para la verificación sin coste después de adquirir la contraseña como una cadena de caracteres de un usuario. Por lo tanto, proporcionar una solución de procesamiento de la información para permitir a un usuario memorizar de manera conveniente y precisa una contraseña y mejorar la seguridad de la comprobación de las contraseñas ha resultado ser un problema técnico urgente a solucionar. El Documento D1 (US2013269013) describe un método para la autenticación de usuario comparando una imagen y los datos contextuales recibidos con las imágenes de referencia y los datos contextuales almacenados en una base de datos.

Compendio

En vista de esto, las realizaciones de la descripción están destinadas a proporcionar un método de procesamiento de la información, un terminal y un medio de almacenamiento informático, que puedan al menos solucionar el problema de la técnica convencional y mejorar las experiencias de usuario.

Las soluciones técnicas de las realizaciones de la descripción se implementan como sigue.

Las realizaciones de la descripción proporcionan un método de procesamiento de la información, que puede incluir que: la información de una primera imagen se pre-adquiera y se genere y almacene una primera clave de cifrado, incluyendo además el método que:

se adquiera la información de una segunda imagen;

se extraiga una primera característica de imagen y una segunda característica de imagen de la información de la segunda imagen, en donde la primera característica de imagen puede representar la información de fondo de la primera imagen, y la segunda característica de imagen puede representar información de primer plano de la primera imagen;

se obtiene una tercera característica de imagen en base a la primera característica de imagen y la segunda característica de imagen, y se determina la tercera característica de imagen como una segunda clave de cifrado; y

de manera similar se realiza una coincidencia sobre la segunda clave de cifrado y la primera clave de cifrado pre-almacenada, y se autentica la segunda imagen según el resultado de la coincidencia.

Las realizaciones de la descripción proporcionan además un terminal, que puede incluir una unidad de adquisición, una primera unidad de procesamiento, una segunda unidad de procesamiento y una unidad de correspondencia, en donde

la unidad de adquisición se puede configurar para pre-adquirir la información de una primera imagen y adquirir información de una segunda imagen;

la primera unidad de procesamiento se puede configurar para generar y almacenar una primera clave de cifrado en base a la información de la primera imagen;

la segunda unidad de procesamiento se puede configurar para extraer una primera característica de imagen y una segunda característica de imagen de la información de la segunda imagen, obtener una tercera característica de imagen en base a la primera característica de imagen y a la segunda característica de imagen, y determinar la tercera característica de imagen como la segunda clave de cifrado, en donde la primera característica de imagen puede representar la información de fondo de la primera imagen, y la segunda característica de imagen puede representar la información de primer plano de la primera imagen; y

la unidad de coincidencia se puede configurar para realizar una coincidencia de similitud sobre la segunda clave de cifrado y la primera clave de cifrado pre-almacenada, y autenticar una segunda imagen según el resultado de la correspondencia.

Las realizaciones de la descripción proporcionan además un medio de almacenamiento informático, en el que se pueden almacenar instrucciones ejecutables por ordenador, estando la instrucción ejecutable por ordenador configurada para ejecutar el método de procesamiento anteriormente mencionado.

Según las realizaciones de la descripción, la información de la primera imagen se adquiere de manera previa, y se genera y almacena la primera clave de cifrado; durante la autenticación, se adquiere la información de la segunda imagen, y se extraen la primera característica de imagen y la segunda característica de imagen de la información de la segunda imagen, en donde la primera característica de imagen representa la información de fondo de la primera imagen, y la segunda característica de imagen representa la información de primer plano de la primera imagen; la tercera característica de imagen se obtiene en base a la primera característica de imagen y a la segunda característica de imagen, y la tercera característica de imagen se determina como la segunda clave de cifrado; y se realiza la coincidencia de similitud sobre la segunda clave de cifrado y la primera clave de cifrado pre-almacenada, y se autentica la segunda imagen según el resultado de coincidencia. De tal manera, la primera clave de cifrado es generada mediante la información de la primera imagen, para que el usuario pueda memorizar de manera conveniente y precisa una contraseña de imagen, y se mejoran las experiencias de usuario, y durante la autenticación, se adquiere de nuevo la información de la imagen, y la autenticación a través de la clave de cifrado generada por la información de imagen adquirida puede mejorar la seguridad de comprobación de la contraseña.

Breve descripción de los dibujos

La Fig. 1 es un diagrama esquemático de diversas entidades de hardware involucradas en la interacción de información según una realización de la descripción.

La Fig. 2 es un diagrama de flujo de la implementación de una primera realización de la descripción.

La Fig. 3 es un diagrama esquemático de una primera imagen según una realización de la descripción.

La Fig. 4 es un diagrama de flujo de la implementación de una segunda realización de la descripción.

La Fig. 5 es un diagrama de flujo de la implementación de una tercera realización de la descripción.

La Fig. 6 es un diagrama de flujo de la implementación de una cuarta realización de la descripción.

La Fig. 7 es un diagrama de estructura de una quinta realización de la descripción.

La Fig. 8 es un diagrama de una entidad de hardware de un terminal según una realización de la descripción.

La Fig. 9 es un diagrama de estructura de la sexta realización de la descripción.

Descripción detallada

La implementación de las soluciones técnicas se describirá a continuación en más detalle con referencia a los dibujos.

La Fig. 1 es un diagrama esquemático de diversas entidades de hardware involucradas en la interacción de la información según una realización de la descripción. En la Fig. 1, se incluyen tres tipos de entidades de hardware, esto es un servidor 11, un terminal 21 y los terminales 31-33. El terminal 21 puede ser un terminal de teléfono móvil, y los terminales 31-33 pueden incluir ordenadores personales. Ordenadores Personales (PC), ordenadores todo en uno y similares. El terminal 21 y los terminales 31-33 pueden realizar una interacción de información con el servidor 11 a través de una red.

En base al diagrama de arquitectura de las diversas entidades de hardware de la Fig. 1, las realizaciones de la descripción se implementan principalmente como sigue: un terminal (tal como el terminal 21 y los terminales 31-33) pre-adquiere la información de una primera imagen, genera una primera clave de cifrado, y envía la primera clave de cifrado a un servidor, tal como el servidor 11, para su almacenamiento a través de la red o almacena la primera clave de cifrado en el terminal en sí; el terminal adquiere la información de una segunda imagen, y extrae una primera característica de imagen y una segunda característica de imagen de la información de la segunda imagen, en donde la primera característica de imagen representa la información de fondo de la primera imagen, y la segunda característica de imagen representa la información de primer plano de la primera imagen; se obtiene una tercera característica de imagen en base a la primera característica de imagen y a la segunda característica de imagen, y se determina la tercera característica de imagen como una segunda clave de cifrado; y la segunda clave de cifrado se envía al servidor, y el servidor realiza la coincidencia de similitud sobre la segunda clave de cifrado y la primera clave de cifrado pre-almacenada a través del servidor y autentica la segunda imagen según un resultado de coincidencia , o el terminal realiza la coincidencia de similitud sobre la segunda clave de cifrado y la primera clave de cifrado pre-almacenada y autentica la segunda imagen según el resultado de coincidencia .

En la descripción, el terminal puede ser cualquiera de entre el terminal 21 y los terminales 31-33 en la Fig. 1. En base a la estructura en la Fig. 1, se proponen a continuación diversas realizaciones de la descripción.

Primera realización

La Fig. 2 muestra un método de procesamiento de la información según una realización de la descripción. Como se muestra en la Fig. 2, el método de procesamiento de la información incluye los siguientes pasos.

En el paso 200, un terminal pre-adquiere la información de una primera imagen, y genera y almacena una primera clave de cifrado.

Aquí, la operación en la que la información de la primera imagen se pre-adquiere y se genera la primera clave de cifrado incluye que:

el terminal adquiera la primera información de la solicitud desde una interfaz de usuario del terminal, adquiera la información de la primera imagen en respuesta a la primera información de entrada, y genere la primera clave de cifrado en base a la información de la primera imagen.

Aquí, la primera información de la solicitud puede ser la información de entrada que necesita fijar una clave de cifrado cuando un usuario se registra e inicia sesión en una aplicación (APP) determinada de un terminal o la información de entrada de la configuración de cifrado para una función de la APP local del terminal.

La información de la primera imagen se puede adquirir a través de una cámara en el terminal.

La información de la primera imagen puede incluir información de primer plano e información de fondo. En un ejemplo mostrado en la Fig.3, la información de fondo puede ser un cierto gesto, capturado por la cámara, del usuario, o cualquier objeto objetivo que es capturado, como una copa. La información de fondo puede ser información, excepto el objeto determinado como la información de primer plano, en toda la imagen. Por ejemplo, la información de primer plano es una copa específica, y la información de fondo es una mesa sobre la cual se coloca la copa.

En base a la realización de la descripción, durante una aplicación práctica, después de que se adquiera la información de la primera imagen, el método incluye además que: la información de la primera imagen se almacene para permitir al usuario extraer directamente la información de imagen almacenada para su autenticación como la información de una segunda imagen en la autenticación posterior.

La operación para que la primera clave de cifrado se genere en base a la información de la primera imagen incluye que:

el terminal realice la extracción de características de Histograma de Gradientes Orientados (HOG) sobre la información de la primera imagen para adquirir el vector de características HOG correspondiente a la información de primer plano de la información de la primera imagen, adquiera un valor hash perceptual correspondiente a la información de fondo en la información de la primera imagen adoptando un Algoritmo Hash Perceptual (PHA) , y genere la primera clave de cifrado configurada para autenticar e identificar la información de la primera imagen en base al vector de características HOG y el valor hash perceptual.

Aquí, la operación de que la primera clave de cifrado configurada para autenticar e identificar la información de la primera imagen se genera en base al vector de característica HOG y el valor hash perceptual incluye que:

el terminal convierta el valor hash perceptual en un vector de características correspondiente, y una el vector de características y el vector de características HOG entre sí para obtener un vector de características configurado para identificar la información de la primera imagen, esto es la primera clave de cifrado configurada para autenticar e identificar la información de la primera imagen.

En base a la realización de la descripción, durante la aplicación práctica, cuando el terminal adquiere la información de la primera imagen, el método puede además incluir que: una solicitud de regulación de parámetros, que se configura para regular los parámetros de adquisición de imágenes, se genere para hacer una primera imagen adquirida clara y estable. Los parámetros de adquisición de imagen pueden ser la luz, la distancia focal y similares.

En base a la realización de la descripción, durante la aplicación práctica, después de la operación en la que se pre-adquiere la información de la primera imagen, el método incluye, además que:

el terminal sincronice la información adquirida de una primera imagen a un primer terminal para que el primer terminal almacene la información de la primera imagen. De esta manera, durante una operación de autenticación del usuario, el primer terminal pueda volver a sincronizar la información de la primera imagen al terminal como la información de la segunda imagen, para que se omita el proceso en el que el terminal adquiere la información de la segunda imagen. De manera alternativa, la información de la primera imagen almacenada en el primer terminal es directamente usada para la adquisición de imágenes del terminal como la información de la segunda imagen. De manera alternativa, la información de la primera imagen almacenada en el primer terminal se imprime/desarrolla

como una imagen clara como la información de la segunda imagen para la adquisición de imágenes del terminal, para que no se requiera construir la segunda imagen.

Aquí, el primer terminal es otro terminal de usuario diferente del terminal, o un ordenador de sobremesa, un PC, un ordenador todo en uno o similar.

En base a la realización de la descripción, durante la aplicación práctica, después de la operación en la que se pre-adquiere la información de la primera imagen, el método además incluye que:

se extraen N piezas de información de la imagen dentro de N regiones de imagen de la información de la primera imagen, y se determinan y almacenan las N piezas de información de la imagen como información de entrada de autenticación.

Aquí, N es un número entero positivo. Un valor numérico específico de N se puede fijar según un requisito práctico. Por ejemplo, el valor de N puede ser 2, 3 o similar.

Las N regiones de imagen pueden ser N regiones de imagen fijas preestablecidas. Por ejemplo, el valor de N es 2. Dos regiones de imagen fijas son una primera región en una esquina superior izquierda de la primera imagen y una segunda región en una esquina inferior derecha de la primera imagen respectivamente. Tanto la primera región como la segunda región son cuadradas con longitudes laterales a. El valor de a se puede establecer según un requisito. Por supuesto, la primera región y la segunda región pueden ser también rectángulos o cualquier otra forma para la cual las longitudes laterales son valores específicos.

De manera alternativa, las N regiones de imagen pueden ser también N regiones de imagen, determinadas de manera aleatoria por el terminal, en la primera imagen. Las formas, tamaños y similares de las N regiones de imagen pueden ser las mismas o diferentes.

La información de la solicitud de autenticación se configura para solicitar al usuario de un contenido la información de la primera imagen en un proceso de autenticación. La información de la solicitud de autenticación puede incluir parte de la información de primer plano y/o parte de la información de fondo en la información de la primera imagen.

Se ha de observar que sólo se requiere que se ejecute el Paso 200 cuando el método de la realización de la descripción se aplica por primera vez y la primera clave de cifrado se puede aplicar de manera directa posteriormente.

En el paso 201, se adquiere la información de una segunda imagen.

Antes del paso, el método además incluye que:

el terminal adquiera la información de la solicitud de autenticación, y por consiguiente presente la información de la solicitud de autenticación en la interfaz de usuario del terminal según una región, donde se ubica la información de la solicitud de autenticación, en la primera imagen. Por lo tanto, el usuario puede recordar rápidamente la información correspondiente de una primera imagen cuando se establece la primera clave de cifrado.

Aquí, la operación de que se adquiera la información de la solicitud de autenticación incluye que: el terminal adquiera la información de la solicitud de autenticación almacenada de manera local en el terminal.

La información de la segunda imagen es una información de imagen requerida cuando el usuario realiza la verificación de la clave de cifrado para una operación de desbloqueo, inicio de sesión o similar. En un proceso de aplicación práctica, la segunda imagen es un escenario reproducido del contenido de la primera imagen. Por ejemplo, la primera imagen es un gesto con forma de V hecho por el usuario en una mesa de oficina, como se muestra en la Fig.3, y la segunda imagen es un escenario reproducido del contenido de la imagen, esto es, el usuario vuelve a hacer el gesto con forma de V en la mesa de la oficina.

En el paso 202, se extraen una primera característica de imagen y una segunda característica de imagen de la información de la segunda imagen.

Aquí, la primera característica de imagen representa la información de fondo de la primera imagen, y la segunda característica de imagen representa la información de primer plano de la primera imagen.

El paso específicamente incluye que: el terminal adquiera un valor hash correspondiente a la información de la segunda imagen, determine el valor hash como la primera característica de imagen, realice la extracción de la información sobre la información de la segunda imagen para obtener un primer vector de características correspondiente a la información de la segunda imagen, y determine el primer vector de características como la segunda característica de imagen.

Aquí, la operación de que se adquiera el valor hash correspondiente a la información de la segunda imagen incluye que: el terminal adquiera un valor hash correspondiente a la segunda imagen adoptando el PHA, incluyendo específicamente: 1) la reducción de la segunda imagen: a partir de un método para eliminar las altas frecuencia y los

detalles más rápidos y sólo reservar las luces y sombras estructurales es la reducción de la segunda imagen, la segunda imagen se reduce a un tamaño 8 X 8, incluyendo en total 64 píxeles, para eliminar las diferencias de imagen provocadas por los diferentes tamaños y escalas; 2) la simplificación del color: la segunda imagen reducida se convierte en una imagen gris de 64 niveles, esto es, todos los píxeles tienen en total 64 colores; 3) el cálculo del valor de gris promedio: se calcula un valor de gris promedio de entre todos los 64 píxeles; 4) la comparación de gris de píxel: el gris de cada píxel en la práctica se compara con el valor de gris promedio, se registra como 1 si es mayor que o igual al valor de gris promedio, y se registra como 0 si es menor que el valor de gris promedio; y 5) el cálculo del valor de hash: los resultados de la comparación de gris de los píxeles se combinan para formar una cadena de caracteres de 64 bits, siendo la cadena de caracteres el valor de hash correspondiente a la información de la segunda imagen, esto es la primera característica de imagen de la segunda imagen, en donde se puede establecer una secuencia de combinación según un requisito práctico, por ejemplo, desde la izquierda a la derecha y desde la parte superior a la parte inferior.

La operación de que la extracción de la información se realice sobre la información de la segunda imagen para obtener el primer vector de características correspondiente a la información de la segunda imagen incluye que:

el terminal realice la extracción de característica HOG sobre la información de la segunda imagen para obtener el primer vector de características correspondiente a la información de la segunda imagen, incluyendo específicamente que: 1) se realice el procesamiento del gris en la segunda imagen, y la segunda imagen se considere como una imagen en tres dimensiones de x, y y z (gris); 2) el procesamiento de normalización del espacio de color se realiza en la segunda imagen adoptando un método de corrección Gamma, para regular el contraste de la segunda imagen, reducir la influencia de los cambios de luz y sombra locales de la segunda imagen y de manera simultánea suprimir la interferencia de ruido; 3) se calcula un gradiente, incluyendo de tamaño y dirección, de cada píxel de la segunda imagen para capturar la información de contorno de la segunda imagen y de manera simultánea debilitar la interferencia de la luz; 4) la segunda imagen se divide en pequeñas celdas, tales como 6*6 píxeles/celda; 5) se hacen las estadísticas sobre el histograma de gradiente de cada celda para formar un descriptor de cada celda; 6) cada n celdas se forma un bloque, y los descriptores de característica de todas las celdas en cada bloque se conectan en serie para obtener un descriptor de características HOG del bloque, en donde n se puede establecer según un requisito práctico, por ejemplo, n es 9, esto es 3*3 celdas/bloque; y 7) los descriptores de características HOG de todos los bloques en la segunda imagen se conectan en serie para obtener un descriptor de características HOG de la segunda imagen, esto es el primer vector de características correspondiente a la información de la segunda imagen.

En el paso 203, se obtiene una tercera característica de imagen en base a la primera característica de imagen y la segunda característica de imagen, y la tercera característica de imagen se determina como una segunda clave de cifrado.

Aquí, la operación de que se obtenga la tercera característica de imagen en base a la primera característica de imagen y la segunda característica de imagen incluye que:

el terminal convierta el valor hash correspondiente a la información de la segunda imagen en un segundo vector de características, uniendo el segundo vector de características y el primer vector de características entre sí para obtener un vector de características exhaustivo para identificar la información de la segunda imagen, y determina el vector de característica exhaustivo como la tercera característica de imagen.

Aquí, la operación de que se convierta el valor hash correspondiente a la información de la segunda imagen en el segundo vector de características incluye que:

el terminal represente el valor hash correspondiente a la información de la segunda imagen en forma de vector, y determine un vector obtenido como el segundo vector de características.

Unir el segundo vector de características y el primer vector de características entre sí es conectar un vector de cola del segundo vector de características con un vector cabecera del primer vector de características para formar el vector de características exhaustivo. Por ejemplo, el segundo vector de características es f2 = {x1, x2, x3}, el primer vector de características es f1 = {x4, x5, x6}, y el vector de características exhaustivo obtenido uniendo los dos entre si es f = {x1, x2, x3, x4, x5, x6}.

En el paso 204, se realiza una coincidencia de similitud sobre la segunda clave de cifrado y la primera clave de cifrado almacenada previamente, y la segunda imagen se autentica según un resultado de coincidencia.

El paso específicamente incluye que: se realice el cálculo del coeficiente de similitud sobre la segunda clave de cifrado y la primera clave de cifrado pre-almacenada para obtener un primer coeficiente, y el primer coeficiente se compara con un valor de umbral preestablecido del coeficiente; cuando el primer coeficiente es mayor que el valor de umbral preestablecido del coeficiente, se determina que la segunda imagen pasa la autenticación; y cuando el primer coeficiente es menor que el valor de umbral preestablecido del coeficiente, se determina que la segunda imagen falla al pasar la autenticación.

Aquí, el cálculo del coeficiente de similitud puede ser el cálculo de un coeficiente de correlación de Pearson. El primer coeficiente puede ser un coeficiente de correlación de Pearson. La magnitud del valor de umbral preestablecido del coeficiente se puede establecer según un requisito práctico. El valor de umbral preestablecido del coeficiente es preferiblemente 0,8.

La operación del cálculo del coeficiente de correlación de Pearson que se realiza sobre la segunda clave de cifrado y la primera clave de cifrado pre-almacenada incluye que:

se establezca que la primera clave de cifrado sea X y la segunda clave de cifrado sea Y, y el coeficiente de correlación de Pearson $\rho_{X, Y}$ de la segunda clave de cifrado y de la primera clave de cifrado pre-almacenada se obtiene según una de las siguientes fórmulas:

$$\rho_{X,Y} = \frac{\operatorname{cov}(X, Y)}{\sigma_X \sigma_Y} = \frac{E((X - \mu_X)(Y - \mu_Y))}{\sigma_X \sigma_Y} = \frac{E(XY) - E(X)E(Y)}{\sqrt{E(X^2) - E^2(X)}\sqrt{E(Y^2) - E^2(Y)}} \quad (1);$$

$$\rho_{X,Y} = \frac{N\sum XY - \sum X \sum Y}{\sqrt{N\sum X^2 - (\sum X)^2}\sqrt{N\sum Y^2 - (\sum Y)^2}} \quad (2); \text{ y}$$

$$\rho_{X,Y} = \frac{\sum XY - \frac{\sum X \sum Y}{N}}{\sqrt{(\sum X^2 - \frac{(\sum X)^2}{N})(\sum Y^2 - \frac{(\sum Y)^2}{N})}} \quad (3),$$

Donde cov (X, Y) en la fórmula (1) representa la covarianza de X e Y, σ_X representa la desviación estándar de X, σ_Y representa la desviación estándar de Y, E(i) representa una operación de promedio sobre i, μ_X representa un valor promedio de X y μ_Y representa un valor promedio de Y; y N en la fórmula (2) y la fórmula (3) representa una dimensión de vector de X e Y.

Segunda realización

La Fig. 4 muestra un método de procesamiento de la información según una realización de la descripción. Como se muestra en la Fig. 4, el método de procesamiento de la información incluye los siguientes pasos.

En el paso 401, un terminal pre-adquiere la información de una primera imagen, y genera una primera clave de cifrado.

El paso incluye específicamente que: el terminal adquiera la primera información de la solicitud de la interfaz de usuario del terminal, adquiera la información de la primera imagen en respuesta a la primera información de la solicitud, y genere la primera clave de cifrado en base a la información de la primera imagen.

Aquí, la primera información de la solicitud puede ser la información para solicitar establecer una clave de cifrado cuando un usuario se registra e inicia sesión en una APP determinada o la información de la solicitud de establecimiento de cifrado para una función de la APP local del terminal.

La información de la primera imagen se puede adquirir a través de la cámara en el terminal.

La información de la primera imagen puede incluir información de primer plano e información de fondo. En un ejemplo, la información de primer plano puede ser una expresión facial determinada, capturada por la cámara, del usuario, tal como llorando, riendo y frunciendo el ceño, o cualquier objeto objetivo específico que se captura, tal como un cierto miembro de la familia. De manera alternativa, la información de primer plano puede ser una foto de grupo del usuario y el miembro de la familia o una foto de grupo del usuario y otro objeto, tal como una copa y un libro favorito. Cualquier información, que pertenezca al usuario o está asociada con un grupo específico y un objeto específico en una relación con el usuario y que no puede ser conocida por otro usuario, se puede determinar como la información de primer plano.

La operación en la que se genera la primera clave de cifrado en base a la información de la primera imagen incluye que:

el terminal realiza la extracción de características HOG sobre la información de la primera imagen para adquirir un vector de características HOG correspondiente a la información de primer plano en la información de la primera imagen, adquiere un valor hash perceptual correspondiente a la información de fondo en la información de la primera imagen adoptando un PHA, y genera la primera clave de cifrado configurada para autenticar e identificar la información de la primera imagen en base al vector de características HOG y el valor hash perceptual.

Aquí, se genera la operación en la que la primera clave de cifrado configurada para autenticar e identificar la información de la primera imagen en base al vector de características HOG y el valor hash perceptual incluye que:

el terminal convierte el valor hash perceptual en un vector de características correspondiente, y une el vector de características y el vector de características HOG entre sí para obtener un vector de características configurado para identificar la información de la primera imagen, esto es la primera clave de cifrado configurada para autenticar e identificar la información de la primera imagen.

En base a la realización de la descripción, durante una aplicación práctica, cuando el terminal adquiere la información de la primera imagen, el método puede incluir además que: se genere una solicitud de regulación de parámetros configurada para regular los parámetros de adquisición de imágenes para hacer una primera imagen adquirida clara y estable. Los parámetros de adquisición de imágenes pueden ser la luz, la distancia focal y similares.

En base a la realización de la descripción, durante la aplicación práctica, después de la operación en la que se adquiere de manera previa la información de la primera imagen, el método incluye además que:

el terminal sincronice la información adquirida de una primera imagen a un primer terminal para que el primer terminal almacene la información de la primera imagen. De dicha manera, en una operación de autenticación del usuario, el primer terminal puede volver a sincronizar la información de la primera imagen al terminal como información de una segunda imagen, para que se omita el proceso en que el terminal adquiere la información de la segunda imagen. De manera alternativa, la información de la primera imagen almacenada en el primer terminal se usa directamente para la adquisición de imágenes del terminal como la información de la segunda imagen. De manera alternativa, la información de la primera imagen almacenada en el primer terminal se imprime/desarrolla en una imagen clara como la información de la segunda imagen para la adquisición de imágenes del terminal, para que no se requiera construir una segunda imagen.

Aquí, el primer terminal es otro terminal de usuario diferente del terminal, o un ordenador de sobremesa, un PC, un ordenador todo en uno y similar.

En base a la realización de la descripción, durante la aplicación práctica, después de la operación en la que se pre-adquiere la información de la primera imagen, el método además incluye que:

se extraen N piezas de información de imagen dentro de las N regiones de imagen de la información de la primera imagen, y se determinan y almacenan N piezas de información de imagen como la información de la solicitud de autenticación.

Aquí, N es un número entero positivo, y se puede establecer un valor numérico específico de N según un requisito práctico. Por ejemplo, el valor de N puede ser 2, 3 o similar.

Las N regiones de imagen pueden ser N regiones de imagen fijas preestablecidas. El valor de N es 2. Las dos regiones de imagen fijas son una primera región en una esquina superior izquierda de la primera imagen y una segunda región en la esquina inferior derecha de la primera imagen respectivamente. Tanto la primera región como la segunda región son cuadradas con longitudes laterales a. El valor de a se puede establecer según un requisito. Por supuesto, la primera región y la segunda región pueden ser también rectángulos o cualquier otra forma de las que se especifiquen los valores de las longitudes laterales.

De manera alternativa, las N regiones de imagen pueden ser también N regiones de imagen, determinadas de manera aleatoria por el terminal, en la primera imagen. Las formas, tamaños y similares de las N regiones de imagen pueden ser las mismas o diferentes.

La información de la solicitud de autenticación se configura para solicitar al usuario el contenido de la información de la primera imagen en un proceso de autenticación. La información de la solicitud de autenticación puede incluir parte de la información de primer plano y/o parte de la información de fondo en la información de la primera imagen.

En el paso 402, el terminal envía la primera clave de cifrado a un servidor para que el servidor almacene la primera clave de cifrado.

Se ha de observar aquí que los pasos 401-402 sólo se requieren que sean ejecutados cuando el método de la realización de la descripción se aplica por primera vez y la primera clave de cifrado se puede aplicar de manera directa posteriormente.

En el paso 403, el terminal adquiere la información de la solicitud de autenticación, y por consiguiente presenta la información de la solicitud de autenticación en una interfaz de usuario según una región, donde se ubica la información de la solicitud de autenticación, en una primera imagen.

Aquí, la información de la solicitud de autenticación se presenta en la interfaz de usuario, para que el usuario pueda memorizar rápidamente la información correspondiente de la primera imagen cuando se establece la primera clave de cifrado.

En el paso 404, el terminal adquiere la información de una segunda imagen.

Aquí, la información de la segunda imagen es información de imagen requerida cuando el usuario realiza la verificación de la clave de cifrado para una operación de desbloqueo, inicio de sesión o similar. En un proceso de aplicación práctica, la segunda imagen es un escenario reproducido del contenido de la primera imagen. Por ejemplo, la primera imagen es un gesto de V hecho por el usuario en una mesa de oficina, como se muestra en la Fig. 3, y la segunda imagen es un escenario reproducido del contenido de la imagen, esto es, el usuario vuelve a hacer el gesto de la V en la mesa de oficina.

En el paso 405, el terminal extrae una primera característica de imagen y una segunda característica de imagen de la información de la segunda imagen, obtiene una tercera característica de imagen en base a la primera característica de imagen y la segunda característica de imagen, y determina la tercera característica de imagen como una segunda clave de cifrado.

Aquí, la primera característica de imagen representa la información de fondo de la primera imagen, y la segunda característica de imagen representa la información de primer plano de la primera imagen.

El paso incluye de manera específica que: el termina adquiera un valor hash correspondiente a la información de la segunda imagen, determine el valor hash como la primera característica de imagen, realice la extracción de información sobre la información de la segunda imagen para obtener un primer vector de características correspondiente a la información de la segunda imagen, y determine el primer vector de características como la segunda característica de imagen.

Aquí, la operación en la que se adquiere el valor hash correspondiente a la información de la segunda imagen incluye que: el terminal adquiera un valor hash correspondiente a la segunda imagen adoptando el PHA.

La operación en la que se realiza la extracción de la información sobre la información de la segunda imagen para obtener el primer vector de características correspondiente a la información de la segunda imagen incluye que:

el terminal realice la extracción de características HOG sobre la información de la segunda imagen para obtener el primer vector de características correspondiente a la información de la segunda imagen.

La operación en la que se obtiene la tercera característica de imagen en base a la primera característica de imagen y la segunda característica de imagen incluye que:

el terminal convierta el valor hash correspondiente a la información de la segunda imagen en un segundo vector de características, una el segundo vector de características y el primer vector de características entre sí para obtener un vector de características exhaustivo para identificar la información de la segunda imagen, y determine el vector de características exhaustivo como la tercera característica de imagen.

En el paso 406, el terminal envía la segunda clave de cifrado al servidor.

En el paso 407, el servidor realiza el cálculo del coeficiente de correlación de Pearson sobre la segunda clave de cifrado y la primera clave de cifrado pre-almacenada para obtener un primer coeficiente, juzga si el primer coeficiente excede un valor de umbral preestablecido del coeficiente o no. Si el primer coeficiente excede el valor de umbral preestablecido del coeficiente, se realizará el paso 408. Si el primer coeficiente no excede el valor de umbral preestablecido del coeficiente, se realizará el paso 409.

Aquí, el primer coeficiente puede ser un coeficiente de correlación de Pearson.

Se puede establecer la magnitud del valor de umbral del coeficiente según un requisito práctico, y el valor de umbral del coeficiente es preferiblemente 0,8.

En el paso 408, se determina que la segunda imagen pase la autenticación.

En el paso 409, se determina que la segunda imagen falle al pasar la autenticación.

Tercera realización

La Fig. 5 muestra un método de procesamiento de la información según una realización de la descripción. El método de procesamiento de la información se aplica a una APP, y como se muestra en la Fig. 5, incluye los siguientes pasos.

En el paso 501, el terminal adquiere la información de una primera imagen, y sincroniza la información de la primera imagen a un primer terminal.

El paso específicamente incluye que: el terminal adquiera la primera información de la solicitud desde la interfaz de usuario del terminal, adquiera la información de la primera imagen en respuesta a la primera información de la solicitud, y genere una primera clave de cifrado en base a la información de la primera imagen.

En la realización de la descripción, la primera información de la solicitud es información para solicitar establecer una clave de cifrado cuando se registra un usuario en un casillero de la APP. Aquí, la clave de cifrado es una clave de cifrado configurada para desbloquear una APP.

La información de la primera imagen se puede adquirir a través de una cámara en el terminal.

La información de la primera imagen incluye información de primer plano e información de fondo. En la realización de la descripción, la información de primer plano es un cierto gesto, capturado por la cámara, del usuario, como se muestra en la Fig. 3. Por supuesto, la información de primer plano puede ser un objeto objetivo que es capturado, tal como una copa.

El terminal sincroniza la información adquirida de una primera imagen al primer terminal para que el primer terminal almacene la información de la primera imagen. De esta manera, durante la operación de autenticación del usuario, el primer terminal puede sincronizar la información de la primera imagen con el terminal de nuevo como información de una segunda imagen, para que se omita el proceso en el que el terminal adquiere la información de la primera imagen. De manera alternativa, la información de la primera imagen almacenada en el primer terminal es directamente usada para la adquisición de imágenes del terminal como la información de la segunda imagen. De manera alternativa, la información de la primera imagen almacenada en el primer terminal se imprime/desarrolla en una imagen clara como la información de la segunda imagen para la adquisición de imágenes del terminal, para que no se requiera construir una segunda imagen.

Aquí, el primer terminal es otro terminal de usuario diferente del terminal, o un ordenador de sobremesa, un PC, un ordenador todo en uno y similar.

En base a la realización de la descripción, durante una aplicación práctica, cuando el terminal adquiere la información de la primera imagen, el método puede incluir además que: el terminal genere una solicitud de regulación de parámetros configurada para regular los parámetros de adquisición de imágenes para hacer una primera imagen adquirida clara y estable. Los parámetros de adquisición de imágenes pueden ser la luz, la distancia focal y similar.

En base a la realización de la descripción, durante la aplicación práctica, después de la operación en la que se adquiere la información de la primera imagen, el método incluye además que:

el terminal extraiga N piezas de información de imagen dentro de N regiones de imagen de la información de la primera imagen, y determine y almacene las N piezas de información de imagen como información de la solicitud de autenticación.

Aquí, N es un número entero positivo, y un valor numérico específico de N se puede establecer según un requisito práctico. Por ejemplo, el valor de N puede ser 2, 3 o similar.

Las N regiones de imagen pueden ser N regiones de imagen preestablecidas. En la realización de la descripción, las N regiones de imagen se fijan para ser una primera región en la esquina superior izquierda de la primera imagen y una segunda región en la esquina inferior derecha de la primera imagen respectivamente. Tanto la primera región como la segunda región son cuadrados con longitudes laterales a. El valor de a se puede establecer según un requisito. Por supuesto, la primera región y la segunda región pueden ser también rectángulos o cualesquiera otras formas de las cuales las longitudes laterales son valores específicos.

De manera alternativa, las N regiones de imagen pueden ser también N regiones de imagen, determinadas de manera aleatoria por el terminal, en la primera imagen. Las formas, tamaños y similares de las N regiones de imagen pueden ser la misma o diferentes.

La información de la solicitud de autenticación se configura para solicitar al usuario el contenido de la información de la primera imagen en un proceso de autenticación. La información de la solicitud de autenticación puede incluir parte de la información de primer plano y/o parte de la información de fondo en la información de la primera imagen.

En el paso 502, el terminal genera una primera clave de cifrado según la información de la primera imagen, y bloquea una APP seleccionada en base a la primera clave de cifrado.

El paso incluye específicamente que: el terminal realice la extracción de característica HOG sobre la información de la primera imagen para adquirir el vector de características HOG correspondiente a la información de primer plano en la información de la primera imagen, adquiera un valor hash perceptual correspondiente a la información de fondo en la información de la primera imagen adoptando un PHA, y genera le primera clave de cifrado configurada para autenticar e identificar la información de la primera imagen en base al vector de características HOG y el valor hash perceptual.

Aquí, la operación de que se genere la primera clave de cifrado configurada para autenticar e identificar la información de la primera imagen en base al vector de características HOG y el valor hash perceptual incluye que:

el terminal convierta el valor hash perceptual en un vector de características correspondiente, y una el vector de características y el vector de características HOG entre sí para obtener un vector de características configurado para identificar la información de la primera imagen, esto es la primera clave de cifrado configurada para autenticar e identificar la información de la primera imagen.

Se ha de observar que la generación de la primera clave de cifrado sólo se requiere que se ejecute cuando el método de la realización de la descripción se aplica por primera vez y la primera clave de cifrado se puede aplicar directamente de manera posterior a bloquear la APP.

En el paso 503, el terminal adquiere información de una segunda imagen.

Antes del paso, el método incluye además que: el terminal adquiera la información de la solicitud de autenticación, y por consiguiente presente la información de la solicitud de autenticación en la interfaz de usuario del terminal según una región, donde se ubica la información de la solicitud de autenticación, en la primera imagen. Por lo tanto, el usuario puede recordar rápidamente la información correspondiente de la primera imagen cuando se establece la primera clave de cifrado.

Aquí, la operación en la que se adquiere la información de la solicitud de autenticación incluye que: el terminal adquiera la información de la solicitud de autenticación localmente almacenada en el terminal.

La información de la segunda imagen es información de imagen requerida cuando el usuario realiza la verificación de la clave de cifrado para el desbloqueo de la APP.

El paso incluye específicamente que: el terminal adquiera la información de la segunda imagen presentada en una pantalla de presentación del primer terminal. Aquí, la información de la segunda imagen es realmente la información de la primera imagen almacenada en el primer terminal. En el proceso de operación práctico, el primer terminal puede ser sostenido por el usuario, y el primer terminal presenta la información de la primera imagen para la adquisición de imágenes del terminal.

De manera alternativa, el terminal adquiere la información de la primera imagen enviada por el primer terminal, y determina la información de la primera imagen como la información de la segunda imagen.

De manera alternativa, el usuario reproduce el escenario del contenido de la primera imagen, y el terminal adquiere la información del escenario reproducido como la información de la segunda imagen.

En el paso 504, el terminal extrae una primera característica de imagen y una segunda característica de imagen de la información de la segunda imagen.

Aquí, la primera característica de imagen representa la información de fondo de la primera imagen, y la segunda característica de imagen representa la información de primer plano de la primera imagen.

El paso específicamente incluye que: el terminal adquiera un valor hash correspondiente a la información de la segunda imagen, determine el valor hash como la primera característica de imagen, realice la extracción de la información sobre la información de la segunda imagen para obtener un primer vector de características correspondiente a la información de la segunda imagen, y determine el primer vector de características como la segunda característica de imagen.

Aquí, la operación en la que se adquiere el valor hash correspondiente a la información de la segunda imagen incluye que: el terminal adquiera un valor hash correspondiente a la segunda imagen adoptando el PHA.

La operación en la que se realiza la extracción de la información se realiza sobre la información de la segunda imagen para obtener el primer vector de características correspondiente a la información incluye que:

el terminal realice la extracción de características HOG sobre la información de la segunda imagen para obtener el primer vector de características correspondiente a la información de la segunda imagen.

En el paso 505, el terminal obtiene una tercera característica de imagen en base a la primera característica de imagen y la segunda característica de imagen, y determina la tercera característica de imagen como una segunda clave de cifrado.

Aquí, la operación en la que se obtiene la tercera característica de imagen en base a la primera característica de imagen y la segunda característica de imagen incluye que:

el terminal convierta el valor hash correspondiente a la información de la segunda imagen en un segundo vector de características, una el segundo vector de características y el primer vector de características entre sí para obtener un vector de características exhaustivo para identificar la información de la segunda imagen, y determine el vector de características exhaustivo como la tercera característica de imagen.

Aquí, la operación en la que el valor hash correspondiente a la información de la segunda imagen se convierte en el segundo vector de características incluye que:

el terminal represente el valor hash correspondiente a la información de la segunda imagen en forma de vector, y determine un vector obtenido como el segundo vector de características.

Unir el segundo vector de características y el primer vector de características entre sí es conectar el vector de cola del segundo vector de características con el vector cabecera del primer vector de características para formar el vector de características exhaustivo.

En el paso 506, el terminal realiza el cálculo del coeficiente de correlación de Pearson sobre la segunda clave de cifrado y la primera clave de cifrado para obtener un primer coeficiente, juzga si el primer coeficiente excede un valor de umbral preestablecido del coeficiente o no. Si el primer coeficiente excede un valor de umbral preestablecido del coeficiente, se realizará el paso 507. Si el primer coeficiente no excede un valor de umbral preestablecido del coeficiente, se realizará el paso 508.

Aquí, el primer coeficiente puede ser un coeficiente de correlación de Pearson.

La magnitud del valor de umbral del coeficiente se puede establecer según un requisito práctico, y en la realización de la descripción, el valor de umbral del coeficiente es 0,8.

En el paso 507, se desbloquea la APP.

En el paso 508, se indica que la APP ha fallado al ser desbloqueada.

Cuarta realización

La Fig. 6 muestra un método de procesamiento de la información según una realización de la descripción. El método de procesamiento de la información se aplica a la autenticación de inicio de sesión de software de conversación tal como el QQ y el WeChat. Como se muestra en la Fig. 6, el método incluye los siguientes pasos.

En el paso 601, el terminal adquiere la información de una primera imagen, y genera la primera clave de cifrado en base a la información de la primera imagen.

El paso específicamente incluye que: el terminal adquiera primero la información de la solicitud desde la interfaz de usuario del terminal, adquiera la información de la primera imagen en respuesta a la primera información de la solicitud, y genere la primera clave de cifrado en base a la información de la primera imagen.

En la realización de la descripción, la primera información de la solicitud es información para solicitar establecer una clave de cifrado cuando un usuario se registra en el software de conversación tal como el QQ y el WeChat, y la primera clave de cifrado es una clave de cifrado usada cuando el usuario inicia sesión en el software de conversación tal como el QQ y el WeChat de nuevo.

La información de la primera imagen puede ser adquirida a través de una cámara en el terminal.

La información de la primera imagen incluye la información de primer plano y la información de fondo. En la realización de la descripción, la información de primer plano es un cierto gesto, capturado por la cámara, del usuario, como se muestra en la Fig. 3. Por supuesto, la información de primer plano puede ser cualquier objeto objetivo que sea capturado, tal como una copa.

En base a la realización de la descripción, durante una aplicación práctica, después de que el terminal adquiera la información de la primera imagen, el método además incluye que:

el terminal sincronice la información adquirida de una primera imagen a un primer terminal para que el primer terminal almacene la información de la primera imagen. De esta manera, durante una operación de autenticación del usuario, el primer terminal puede volver a sincronizar la información de la primera imagen al terminal como información de una segunda imagen, para que se omita el proceso en el que el terminal adquiere la información de la segunda imagen. De manera alternativa, la información de la primera imagen almacenada en el primer terminal es directamente usada para la adquisición de imágenes del terminal como la información de la segunda imagen. De manera alternativa, la información de la primera imagen almacenada en el primer terminal se imprime/desarrolla en una imagen clara como la información de la segunda imagen para la adquisición de imágenes del terminal, para que no se requiera construir una segunda imagen.

Aquí, el primer terminal es otro terminal de usuario diferente del terminal, o un ordenador de escritorio, un PC, un ordenador todo en uno y similar.

En base a la realización de la descripción, durante la aplicación práctica, cuando el terminal adquiere la información de la primera imagen, el método puede además incluir que: el terminal genere una solicitud de regulación de parámetros configurada para regular los parámetros de adquisición de imágenes para hacer una primera imagen

adquirida clara y estable. Los parámetros de adquisición de imágenes pueden ser la luz, la distancia focal y similares.

En base a la realización de la descripción, durante la aplicación práctica, después de la operación en la que se adquiere la información de la primera imagen, el método además incluye que:

el terminal extraiga N piezas de información de imagen dentro de N regiones de imagen de la información de la primera imagen, y determine y almacene las N piezas de información de imagen como la información de la solicitud de autenticación.

Aquí, N es un número entero positivo, y el valor numérico específico de N se puede establecer según un requisito práctico. Por ejemplo, el valor de N puede ser 2, 3 o similar.

Las N regiones de imagen pueden ser N regiones de imagen fijas preestablecidas. Por ejemplo, las N regiones de imagen se fijan para ser una primera región en una esquina superior izquierda de la primera imagen y una segunda región en la esquina inferior derecha de la primera imagen respectivamente. Tanto la primera región como la segunda región son cuadrados con longitudes laterales a. El valor de a se puede establecer según un requisito. Por supuesto, la primera región y la segunda región pueden ser también rectángulos o cualesquiera otras formas para las cuales las longitudes laterales son valores específicos.

De manera alternativa, las N regiones de imagen pueden ser también N regiones de imagen, determinadas de manera aleatoria por el terminal, en la primera imagen. Las formas, tamaños y similares de las N regiones de imagen pueden ser las mismas o diferentes. En la realización de la descripción, las N regiones de imagen son dos regiones de imagen, que son determinadas de manera aleatoria por el terminal y tienen la misma área, en la primera imagen.

La información de la solicitud de autenticación se configura para solicitar al usuario el contenido de la información de la primera imagen en un proceso de autenticación de inicio de sesión. La información de la solicitud de autenticación puede incluir parte de la información de primer plano y/o parte de la información de fondo en la información de la primera imagen.

En base a la realización de la descripción, durante la aplicación práctica, la operación en la que se genera la primera clave de cifrado en base a la información de la primera imagen incluye que:

el terminal realice la extracción de características HOG sobre la información de la primera imagen para adquirir un vector de características HOG correspondiente a la información de primer plano en la información de la primera imagen, adquiera un valor hash perceptual correspondiente a la información de fondo en la información de la primera imagen adoptando un PHA, y genere la primera clave de cifrado configurada para autenticar e identificar la información de la primera imagen en base al vector de características HOG y el valor hash perceptual.

Aquí, la operación en la que se genera la primera clave de cifrado configurada para autenticar e identificar la información de la primera imagen en base al vector de características HOG y el valor hash perceptual incluye que:

el terminal convierta el valor hash perceptual en un vector de características correspondiente, y una el vector de características y el vector de características HOG entre sí para obtener un vector de características configurado para identificar la información de la primera imagen.

En el paso 602, el terminal envía la primera clave de cifrado a un servidor para que el servidor almacene la primera clave de cifrado, y solicita el registro con éxito.

Se ha de observar que sólo se requiere que se ejecuten los Pasos 601-602 cuando el método de la realización de la descripción se aplica por primera vez y la primera clave de cifrado se puede aplicar de manera directa posteriormente.

En el paso 603, el terminal adquiere información de una segunda imagen.

Antes del paso, el método incluye además que: el terminal adquiera la información de la solicitud de autenticación, y por consiguiente presente la información de la solicitud de autenticación en la interfaz de usuario del terminal según una región, donde se ubica la información de la solicitud de autenticación, en la primera imagen.

Aquí, la información de la solicitud de información se presenta en la interfaz de usuario, para que el usuario pueda recordar rápidamente la información correspondiente de una primera imagen cuando se establece la primera clave de cifrado.

En la realización de la descripción, la segunda imagen es un escenario reproducido del contenido de la primera imagen. Por ejemplo, la primera imagen es un gesto en forma de V hecho por el usuario en una mesa de oficina, como se muestra en la Fig. 3, y la segunda imagen es un escenario reproducido del contenido de la imagen, esto es, el usuario vuelve a hacer el gesto en forma de V en la mesa de oficina.

En el paso 604, el terminal extrae una primera característica de imagen y una segunda característica de imagen de la información de la segunda imagen, obtiene una tercera característica de imagen en base a la primera característica de imagen y a la segunda característica de imagen, y determina la tercera característica de imagen como una segunda clave de cifrado.

Aquí, la primera característica de imagen representa la información de fondo de la primera imagen, y la segunda característica de imagen representa la información de primer plano de la primera imagen.

El paso específicamente incluye que: el terminal adquiera un valor hash correspondiente a la información de la segunda imagen, determine el valor hash como la primera característica de imagen, realice la extracción de información sobre la información de la segunda imagen para obtener un primer vector de características correspondiente a la información de la segunda imagen, y determine el primer vector de características como la segunda característica de imagen.

Aquí, la operación en la que se adquiere el valor hash correspondiente a la información de la segunda imagen incluye que: el terminal adquiera un valor hash correspondiente a la segunda imagen adoptando el PHA.

La operación en la que la extracción de información es realizada sobre la información de la segunda imagen para obtener el primer vector de características correspondiente a la información de la segunda imagen incluye que:

el terminal realice la extracción de características HOG sobre la información de la segunda imagen para obtener el primer vector de características correspondiente a la información de la segunda imagen.

La operación en la que se obtiene la tercera característica de imagen en base a la primera característica de imagen y la segunda característica de imagen incluye que:

el terminal convierta el valor hash correspondiente a la información de la segunda imagen en un segundo vector de características, una el segundo vector de características y el primer vector de características entre sí para obtener un vector de características exhaustivo para identificar la información de la segunda imagen, y determine el vector de características exhaustivo como la tercera característica de imagen.

En el paso 605, el terminal envía la segunda clave de cifrado al servidor.

En el paso 606, el servidor realiza el cálculo del coeficiente de correlación de Pearson sobre la segunda clave de cifrado y la primera clave de cifrado para obtener un primer coeficiente, juzga si el primer coeficiente excede un valor de umbral preestablecido del coeficiente o no. Si el primer coeficiente excede el valor de umbral preestablecido del coeficiente, se realizará el paso 607. Si el primer coeficiente no excede el valor de umbral preestablecido del coeficiente, se realizará el paso 608.

Aquí, el primer coeficiente puede ser el coeficiente de correlación de Pearson.

La magnitud del coeficiente de valor de umbral se puede establecer según un requisito práctico, y el valor de umbral del coeficiente es preferiblemente 0,8.

En el paso 607, se determina que una segunda imagen pasa la autenticación, y se indica al usuario que ha tenido éxito en el inicio de sesión.

En el paso 608, se determina que una segunda imagen falla la autenticación, y se indica al usuario que ha fallado en el inicio de sesión.

Quinta realización

La Fig. 7 es un diagrama de estructura del terminal de la primera realización de la descripción. Como se muestra en la Fig. 7, un terminal de la realización de la descripción incluye: una unidad 71 de adquisición, una primera unidad 72 de procesamiento, una segunda unidad 73 de procesamiento y una unidad 74 de coincidencia.

La unidad 71 de adquisición se configura para pre-adquirir la información de una primera imagen, y adquirir información de una segunda imagen.

La primera unidad 72 de procesamiento se configura para generar y almacenar una primera clave de cifrado en base a la información de la primera imagen.

La segunda unidad 73 de procesamiento se configura para extraer una primera característica de imagen y una segunda característica de imagen de la información de la segunda imagen, obtener una tercera característica de imagen en base a la primera característica de imagen y la segunda característica de imagen, y determinar la tercera característica de imagen como una segunda clave de cifrado, en donde la primera característica de imagen representa la información de fondo de la primera imagen, y la segunda característica de imagen representa la información de primer plano de la primera imagen.

La unidad 74 de coincidencia se configura para realizar la coincidencia de similitud sobre la segunda clave de cifrado y la primera clave de cifrado pre-almacenada, y autentica una segunda imagen según un resultado de coincidencia.

En base a la realización de la descripción, durante una aplicación práctica, la unidad 71 de adquisición se configura específicamente para adquirir la primera información de la solicitud desde una interfaz de usuario del terminal, y adquirir la información de la primera imagen en respuesta a la primera información de la solicitud.

Aquí, la primera información de la solicitud puede ser información para solicitar establecer una clave de cifrado cuando un usuario se registra e inicia sesión en una APP determinada o información de la solicitud de ajuste de cifrado para una función APP local del terminal.

La información de la primera imagen puede incluir información de primer plano e información de fondo. La información de primer plano puede ser un gesto determinado, capturado por una cámara, del usuario, como se muestra en la Fig. 3, o cualquier otro objeto objetivo que es capturado, tal como una copa.

En base a la realización de la descripción, durante la aplicación práctica, la primera unidad 72 de procesamiento se configura de manera específica para realizar la extracción de características HOG sobre la información de la primera imagen para adquirir un vector de características HOG correspondiente a la información de primer plano en la información de la primera imagen, adquirir un valor hash perceptual correspondiente a la información de fondo en la información de la primera imagen adoptando un PHA, y generar la primera clave de cifrado configurada para autenticar e identificar la información de la primera imagen en base al vector de características HOG y el valor hash perceptual.

En base a la realización de la descripción, durante la aplicación práctica, el terminal incluye además una unidad 75 de solicitud, configurada para generar una solicitud de regulación de parámetros configurada para regular los parámetros de adquisición de imágenes para tener una primera imagen adquirida clara y estable. Los parámetros de adquisición de imágenes pueden ser la luz, la distancia focal y similares.

En base a la realización de la descripción, durante la aplicación práctica, la primera unidad 72 de procesamiento se configura además para sincronizar la información adquirida de una primera imagen a un primer terminal para que el primer terminal almacene la información de la primera imagen.

En base a la realización de la descripción, durante la aplicación práctica, la primera unidad 72 de procesamiento se configura además para extraer N piezas de información de imagen dentro de N regiones de imagen de la información de la primera imagen, y determinar y almacenar las N piezas de información de imagen como información de la solicitud de autenticación. N es un número entero positivo, y se puede establecer un valor numérico específico de N según un requisito práctico. Por ejemplo, el valor de N puede ser 2, 3 o similar.

Las N regiones de imagen pueden ser N regiones de imagen fijas preestablecidas. El valor de N es 2. Dos regiones de imagen fijas son una primera región en la esquina superior izquierda de la primera imagen y una segunda región en la esquina inferior derecha de la primera imagen respectivamente. Tanto la primera región como la segunda región son cuadrados con longitudes laterales a. El valor de a se puede establecer según un requisito. Por supuesto, la primera región y la segunda región pueden ser también rectángulos o cualesquiera otras formas de las cuales las longitudes laterales son valores específicos.

De manera alternativa, las N regiones de imagen pueden ser también N regiones de imagen, determinadas de manera aleatoria por el terminal, en la primera imagen. Las formas, tamaños, y similares de las N regiones de imagen pueden ser las mismas o diferentes.

La información de la solicitud de autenticación se configura para solicitar al usuario el contenido de la información de la primera imagen en un proceso de autenticación. La información de la solicitud de autenticación puede incluir parte de la información de primer plano y/o parte de la información de fondo en la información de la primera imagen.

En base a la realización de la descripción, durante la aplicación práctica, la primera unidad 72 de procesamiento se configura además para adquirir la información de la solicitud de autenticación, y por consiguiente presentar la información de la solicitud de autenticación en la interfaz de usuario del terminal según una región, donde se ubica la información de la solicitud de autenticación, en la primera imagen.

En base a la realización de la descripción, durante la aplicación práctica, la segunda unidad 73 de procesamiento se configura específicamente para adquirir un valor hash correspondiente a la información de la segunda imagen, y determinar el valor hash como la primera característica de imagen.

La segunda unidad 73 de procesamiento se configura además para realizar la extracción de información sobre la información de la segunda imagen para obtener un primer vector de características correspondiente a la información de la segunda imagen, y determinar el primer vector de características como la característica de la segunda imagen.

En base a la realización de la descripción, durante la aplicación práctica, la segunda unidad 73 de procesamiento se configura de manera específica para convertir el valor hash en un segundo vector de características, unir el segundo

vector de características y el primer vector de características entre sí para obtener un vector de características exhaustivo para identificar la información de la segunda imagen, y determinar el vector de características exhaustivo como la tercera característica de imagen.

En base a la realización de la descripción, durante la aplicación práctica, la unidad 74 de coincidencia se configura de manera específica para realizar el cálculo del coeficiente de similitud sobre la segunda clave de cifrado y la primera clave de cifrado pre-almacenada para obtener un primer coeficiente, y comparar el primer coeficiente con un valor de umbral preestablecido del coeficiente.

cuando el primer coeficiente es mayor que el valor de umbral preestablecido del coeficiente, determinar que la segunda imagen pasa la autenticación; y

cuando el primer coeficiente es menor que el valor de umbral preestablecido del coeficiente, determinar que la segunda imagen falla al pasar la autenticación; en donde el cálculo del coeficiente de similitud puede ser el cálculo del coeficiente de correlación de Pearson, el primer coeficiente puede ser un coeficiente de correlación de Pearson, la magnitud del valor de umbral del coeficiente se puede establecer según un requisito práctico, y el valor de umbral del coeficiente l es preferiblemente 0,8.

Se ha de observar aquí que el terminal puede ser un PC, un ordenador portátil, un ordenador de sobremesa, un ordenador todo en uno, y el terminal que combina cada unidad para la realización de las funciones de cada unidad o las funciones en las que al menos se divide cada unidad al menos incluye una base de datos configurada para almacenar datos y un procesador configurado para el procesamiento de datos, o incluye un medio de almacenamiento dispuesto en el terminal o un medio de almacenamiento independiente.

Aquí, el procesador configurado para el procesamiento de datos puede ser implementado mediante un microprocesador, una Unidad Central de Procesamiento (CPU), un Procesador Digital de Señales (DSP) o una Matriz de Puertas Programables en Campo (FPGA) al ejecutar el procesamiento; y el medio de almacenamiento incluye una instrucción de operación, la instrucción de operación puede ser un código ejecutable por un ordenador, y cada paso en el flujo del método de procesamiento de la información de la realización de la descripción se implementa a través de la instrucción de operación.

Un ejemplo del terminal de la realización de la descripción que sirve como una entidad S11 de hardware se muestra en la Fig. 8. El terminal incluye un procesador 81, un medio 82 de almacenamiento y al menos una interfaz 83 de comunicación externa. El procesador 81, el medio 82 de almacenamiento y la interfaz 83 de comunicación externa están todos conectados a través de un bus 84.

Es importante apuntar aquí que: las descripciones anteriores sobre el terminal son similares a las descripciones sobre el método, y las descripciones sobre los efectos beneficiosos que sean las mismas que aquellas del método no se elaborarán. Los detalles técnicos no descritos en la realización terminal de la descripción se refieren a las descripciones en las realizaciones anteriormente mencionadas de la descripción.

Sexta realización

La Fig. 9 es un diagrama de estructura del terminal de la segunda realización de la descripción. Como se muestra en la Fig. 9, un terminal de la realización de la descripción incluye: una unidad 91 de adquisición, una primera unidad 92 de procesamiento, una segunda unidad 93 de procesamiento y una unidad 94 de envío.

La unidad 91 de adquisición se configura para pre-adquirir la información de una primera imagen y adquirir la información de una segunda imagen.

La primera unidad 92 de procesamiento se configura para generar una primera clave de cifrado en base a la información de la primera imagen.

La segunda unidad 93 de procesamiento se configura para extraer una primera característica de imagen y una segunda característica de imagen de la información de la segunda imagen, obtener una tercera característica de imagen en base a la primera característica de imagen y la segunda característica de imagen, y determinar la tercera característica de imagen como una segunda clave de cifrado, en donde la primera característica de imagen representa la información de fondo de la primera imagen, y la segunda característica de imagen representa la información de primer plano de la primera imagen.

La unidad 94 de envío se configura para enviar la primera clave de cifrado y la segunda clave de cifrado a un servidor para que el servidor realice la coincidencia de similitud en la segunda clave de cifrado y la primera clave de cifrado y autentique una segunda imagen según un resultado de coincidencia.

En base a la realización de la descripción, durante una aplicación práctica, la unidad 91 de adquisición se configura de manera específica para adquirir la primera información de la solicitud desde una interfaz de usuario del terminal, adquirir la información de la primera imagen en respuesta a la primera información de la solicitud, y generar la primera clave de cifrado en base a la información de la primera imagen.

Aquí, la primera información de la solicitud puede ser información para solicitar establecer una clave de cifrado cuando un usuario se registra e inicia sesión en una APP determinada o información de la solicitud de ajuste de cifrado para una función APP local del terminal.

La información de la primera imagen puede incluir información de primer plano e información de fondo, en donde la información de primer plano puede ser un gesto determinado, capturado por una cámara, del usuario, como se muestra en la Fig. 3, o cualquier objeto objetivo que se capture, tal como una copa.

En base a la realización de la descripción, durante la aplicación práctica, la primera unidad 92 de procesamiento se configura específicamente para realizar la extracción de características HOG sobre la información de la primera imagen para adquirir un vector de características HOG correspondiente a la información de primer plano en la información de la primera imagen, adquirir un valor hash perceptual correspondiente a la información de fondo en la información de la primera imagen adoptando un PHA, y generar la primera clave de cifrado configurada para autenticar e identificar la información de la primera imagen en base al vector de características HOG y el valor hash perceptual.

En base a la realización de la descripción, durante la aplicación práctica, el terminal además incluye una unidad 95 de solicitud, configurada para generar una solicitud de regulación de parámetros configurada para regular los parámetros de adquisición de imágenes para hacer una primera imagen adquirida clara y estable. Los parámetros de adquisición de imágenes pueden ser la luz, la distancia focal y similares.

En base a la realización de la descripción, durante la aplicación práctica, la primera unidad 92 de procesamiento se configura además para sincronizar la información adquirida de una primera imagen con un primer terminal para que el primer terminal almacene la información de la primera imagen.

En base a la realización de la descripción, durante la aplicación práctica, la primera unidad 92 de procesamiento se configura además para extraer N piezas de información de imagen dentro de N regiones de imagen de la información de la primera imagen, y determinar y almacenar las N piezas de información de imagen como la información de la solicitud de información. N es un número entero positivo, y se puede establecer el valor numérico de N según un requisito práctico. Por ejemplo, el valor de N puede ser 2, 3 o similar.

Las N regiones de imagen pueden ser N regiones de imagen fijas preestablecidas. El valor de N es 2. Las dos regiones de imagen fijas son una primera región en una esquina superior izquierda de la primera imagen y una segunda región en la esquina inferior derecha de la primera imagen respectivamente. Tanto la primera región como la segunda región son cuadrados con longitudes laterales a. El valor de a se puede establecer según un requisito. Por supuesto, la primera región y la segunda región pueden ser también rectángulos o cualesquiera otras formas para las cuales las longitudes laterales son valores específicos.

De manera alternativa, las N regiones de imagen pueden ser también N regiones de imagen, determinadas de manera aleatoria por el terminal, en la primera imagen. Las formas, tamaños y similares de las N regiones de imagen pueden ser las mismas o diferentes.

La información de la solicitud de autenticación se configura para solicitar al usuario de un contenido la información de la primera imagen en un proceso de autenticación. La información de la solicitud de autenticación puede incluir parte de la información de primer plano y/o parte de la información de fondo en la información de la primera imagen.

En base a la realización de la descripción, durante la aplicación práctica, la primera unidad 92 de procesamiento se configura además para adquirir la información de la solicitud de autenticación y por consiguiente presentar la información de la solicitud de autenticación en la interfaz de usuario del terminal según una región, donde se ubica la información de la solicitud de autenticación, en la primera imagen.

En base a la realización de la descripción, durante la aplicación práctica, la segunda unidad 93 de procesamiento se configura específicamente para adquirir un valor hash correspondiente a la información de la segunda imagen, y determinar el valor hash como la primera característica de imagen.

La segunda unidad 93 de procesamiento se configura además para realizar la extracción sobre la información de la segunda imagen para obtener un primer vector de características correspondiente a la información de la segunda imagen, y determinar el primer vector de características como la segunda característica de imagen.

En base a la realización de la descripción, durante la aplicación práctica, la segunda unidad 93 de procesamiento se configura específicamente para convertir el valor hash en un segundo vector de características, unir el segundo vector de características y el primer vector de características entre sí para obtener un vector de características exhaustivo para identificar la información de la segunda imagen, y determinar el vector de características exhaustivo como las tercera característica de imagen.

Por consiguiente, la realización de la descripción proporciona además un medio de almacenamiento informático, en el cual se almacena una instrucción ejecutable por un ordenador, estando la instrucción ejecutable por un ordenador configurada para ejecutar el método de procesamiento de la información anteriormente mencionado.

En algunas realizaciones proporcionadas por la descripción, se debería entender que el equipo y el método descritos se pueden implementar de otra manera. La realización de equipo descrita anteriormente es sólo esquemática, y por ejemplo, la división de las unidades es sólo una división de funciones lógica, y se pueden adoptar otras maneras de división durante la implementación práctica. Por ejemplo, se pueden combinar o integrar múltiples unidades o componentes en otro sistema, o se pueden abandonar o no ejecutar algunas características. Además, el acoplamiento, o el acoplamiento directo o la conexión de comunicación entre cada componente presentado o discutido pueden ser un acoplamiento o comunicación de conexión indirecta, implementada a través de algunas interfaces del equipo o las unidades, y puede ser eléctrico y mecánico o adoptar otras formas.

Las unidades anteriormente mencionadas descritas como partes separadas pueden estar o no separadas, y partes presentadas como unidades pueden ser o no unidades físicas, y principalmente se pueden ubicar en el mismo lugar, o se pueden distribuir en múltiples unidades de red. Parte o todas estas unidades se pueden seleccionar para alcanzar el propósito de las soluciones de las realizaciones según un requisito práctico.

Además, cada unidad de función en cada realización de la descripción se puede integrar en una unidad de procesamiento, cada unidad puede existir también independientemente, y dos o más de dos unidades se pueden integrar también en una unidad. La unidad integrada anteriormente mencionada se puede implementar en forma de hardware, y también se puede implementar en forma de unidad funcional de hardware y software.

Aquellos expertos en la técnica deberían saber que: todos o parte de los pasos de la realización anteriormente mencionada pueden ser implementados dando instrucciones al hardware relacionadas a través de un programa, el programa anteriormente mencionado se puede almacenar en un medio de almacenamiento legible por un ordenador, y el programa se ejecuta para ejecutar los pasos de la realización anteriormente mencionada; y el medio de almacenamiento incluye: diversos medios capaces de almacenar códigos de programa tales como un equipo de almacenamiento móvil, una Memoria de Sólo Lectura (ROM), una Memoria de Acceso Aleatorio (RAM), un disco magnético o un disco óptico.

De manera alternativa, al ser implementado en forma de módulo de función de software y ser vendido o usado como un producto independiente, la unidad integrada de la descripción se puede almacenar también en un medio de almacenamiento legible por un ordenador. En base a dicho conocimiento, sustancialmente se pueden realizar las soluciones técnicas de las realizaciones de la descripción o las partes que hacen contribuciones a la técnica convencional en forma de producto de software, y el producto de software informático se almacena en un medio de almacenamiento (que puede ser un PC, un servidor, un equipo de red o similar) para ejecutar todo o parte del método en cada realización de la descripción. El medio de almacenamiento anteriormente mencionado incluye: diversos medios capaces de almacenar códigos de programa tales como un equipo de almacenamiento móvil, una ROM, una RAM, un disco magnético o un disco óptico.

Lo anterior es sólo el modo de implementación específico de la descripción y no está destinado a limitar el alcance de protección de la descripción. Cualesquiera variaciones o reemplazos evidentes para aquellos expertos en la técnica dentro del alcance técnico descrito por la descripción deben caer dentro del alcance de protección de la descripción. Por lo tanto, el alcance de protección de la descripción se debe someter al alcance de protección de las reivindicaciones.

Aplicabilidad industrial

Según las realizaciones de la descripción, la información de la primera imagen se pre-adquiere, y se genera y almacena la primera clave de cifrado; durante la autenticación, se adquiere la información de la segunda imagen, y se extraen la primera característica de imagen y la segunda característica de imagen de la información de la segunda imagen, en donde la primera característica de imagen representa la información de fondo de la primera imagen, y la segunda característica de imagen representa la información de primer plano de la primera imagen; la tercera característica de imagen se obtiene en base a la primera característica de imagen y la segunda característica de imagen, y la tercera característica de imagen se determina como la segunda clave de cifrado; y se realiza la coincidencia de similitud sobre la segunda clave de cifrado y la primera clave de cifrado pre-almacenada, y la segunda imagen se autentica según el resultado de coincidencia . De esta manera, la primera clave de cifrado es generada mediante la información de la primera imagen, para que el usuario pueda memorizar de manera conveniente y precisa una contraseña de imagen, y se mejoran las experiencias de usuario; y durante la autenticación, se adquiere de nuevo la información de imagen, y la autenticación a través de la clave de cifrado generada mediante la información de imagen adquirida puede mejorar la seguridad de la comprobación de la contraseña.

REIVINDICACIONES

1. Un método de procesamiento de la información, comprendiendo el método: pre-adquirir la información de una primera imagen y generar y almacenar una primera clave de cifrado, comprendiendo además el método:

adquirir información de una segunda imagen;

extraer una primera característica de imagen y una segunda característica de imagen de la información de la segunda imagen, en donde la primera característica de imagen representa la información de fondo de la primera imagen, y la segunda característica de imagen representa la información de primer plano de la primera imagen.

obtener una tercera característica de imagen en base a la primera característica de imagen y la segunda característica de imagen, y determinar la tercera característica de imagen como una segunda clave de cifrado; y

realizar la coincidencia de similitud sobre la segunda clave de cifrado y la primera clave de cifrado pre-almacenada, y autenticar la segunda imagen según un resultado de coincidencia.

2. El método según la reivindicación 1, en donde la pre-adquisición de la información de la primera imagen comprende:

adquirir la primera información de la solicitud desde una interfaz de usuario de un terminal; y

adquirir la información de la primera imagen en respuesta a la primera información de la solicitud, y generar la primera clave de cifrado en base a la información de la primera imagen.

3. El método según la reivindicación 2, en donde antes de adquirir la información de la segunda imagen, el método comprende además:

extraer N piezas de información de imagen dentro de N regiones de imagen de la información de la primera imagen, y determinar y almacenar las N piezas de información de imagen como información de la solicitud de autenticación, siendo N un número entero positivo.

4. El método según la reivindicación 3, en donde antes de adquirir la información de la segunda imagen, el método comprende además:

adquirir la información de la solicitud de autenticación, y por consiguiente presentar la información de la solicitud de autenticación en la interfaz de usuario del terminal según una región, donde la información de la solicitud de autenticación se ubica, en la primera imagen.

5. El método según la reivindicación 1 o 2, en donde la extracción de la primera característica de imagen y de la segunda característica de imagen de la información de la segunda imagen comprende:

adquirir un valor hash correspondiente a la información de la segunda imagen, y determinar el valor hash como la primera característica de imagen; y

realizar la extracción de la información sobre la información de la segunda imagen para obtener un primer vector de características correspondiente a la información de la segunda imagen, y determinar el primer vector de características como la segunda característica de imagen.

6. El método según la reivindicación 5, en donde obtener la tercera característica de imagen en base a la primera característica de imagen y la segunda característica de imagen comprende:

convertir el valor hash en un segundo vector de características, unir el segundo vector de características y el primer vector de características entre sí para obtener un vector de características exhaustivo para identificar la información de la segunda imagen, y determinar el vector de características exhaustivo como la tercera característica de imagen.

7. El método según la reivindicación 1 o 2, en donde realizar la coincidencia de similitud sobre la segunda clave de cifrado y la primera clave de cifrado pre-almacenada y autenticar la segunda imagen según el resultado de coincidencia comprende:

realizar el cálculo del coeficiente de similitud sobre la segunda clave de cifrado y la primera clave de cifrado pre-almacenada para obtener un primer coeficiente, y comparar el primer coeficiente con un valor de umbral preestablecido del coeficiente; y

cuando el primer coeficiente es mayor que el valor de umbral preestablecido del coeficiente, determinar que la segunda imagen pasa la autenticación; y

cuando el primer coeficiente es menor que el valor de umbral preestablecido del coeficiente, determinar que la segunda imagen falla al pasar la autenticación.

8. El método según la reivindicación 1 o 2, en donde la información de primer plano de la primera imagen es un gesto de un usuario durante la adquisición de la información de la primera imagen.

9. Un terminal, comprendiendo el terminal una unidad de adquisición, una primera unidad de procesamiento, una segunda unidad de procesamiento y una unidad de coincidencia, en donde

la unidad de adquisición se configura para pre-adquirir la información de una primera imagen, y adquirir la información de una segunda imagen;

la primera unidad de procesamiento se configura para generar y almacenar una primera clave de cifrado en base a la información de la primera imagen;

la segunda unidad de procesamiento se configura para extraer una primera característica de imagen y una segunda característica de imagen de la información de la segunda imagen, obtener una tercera característica de imagen en base a la primera característica de imagen y a la segunda característica de imagen, y determinar la tercera característica de imagen como una segunda clave de cifrado, en donde la primera característica de imagen representa la información de fondo de la primera imagen, y la segunda característica de imagen representa la información de primer plano de la primera imagen; y

la unidad de coincidencia se configura para realizar la coincidencia de similitud sobre la segunda clave de cifrado y la primera clave de cifrado pre-almacenada, y autenticar una segunda imagen según el resultado de coincidencia.

10. El terminal según la reivindicación 9, en donde la unidad de adquisición se configura además para adquirir la primera información de la solicitud desde una interfaz de usuario de un terminal, y adquirir la información de la primera imagen en respuesta a la primera información de la solicitud.

11. El terminal según la reivindicación 10, en donde la primera unidad de procesamiento se configura además para extraer N piezas de información de imagen dentro de N regiones de imagen de la información de la primera imagen, y determinar y almacenar las N piezas de información de imagen como la información de la solicitud de autenticación, siendo N un número entero positivo.

12. El terminal según la reivindicación 11, en donde la primera unidad de procesamiento se configura además para adquirir la información de la solicitud de autenticación, y por consiguiente presentar la información de la solicitud de autenticación en la interfaz de usuario del terminal según una región, donde se ubica la información de la solicitud de información, en la primera imagen.

13. El terminal según la reivindicación 9 o 10, en donde la segunda unidad de procesamiento se configura además para adquirir un valor hash correspondiente a la información de la segunda imagen, y determinar el valor hash como la primera característica de imagen;

y realizar la extracción de información sobre la información de la segunda imagen para obtener un primer vector de características correspondiente a la información de la segunda imagen, y determinar el primer vector de características como la segunda característica de imagen.

14. El terminal según la reivindicación 13, en donde la segunda unidad de procesamiento se configura además para convertir el valor hash en un segundo vector de características, unir el segundo vector de características y el primer vector de características entre sí para obtener un vector de características exhaustivo para identificar la información de la segunda imagen, y determinar el vector de características exhaustivo como la tercera característica de imagen.

15. El terminal según la reivindicación 9 o 10, en donde la unidad de coincidencia se configura además para realizar el cálculo del coeficiente de similitud sobre la segunda clave de cifrado y la primera clave de cifrado pre-almacenada para obtener un primer coeficiente, y comparar el primer coeficiente con un valor de umbral preestablecido del coeficiente;

cuando el primer coeficiente es mayor que el valor de umbral preestablecido del coeficiente, determinar que la segunda imagen pasa la autenticación; y

cuando el primer coeficiente es menor que el valor de umbral preestablecido del coeficiente, determinar que la segunda imagen falla al pasar la autenticación.

16. Un medio de almacenamiento informático que tiene almacenado en éste instrucciones ejecutables por un ordenador para ejecutar el método de procesamiento de la información según cualquiera de las reivindicaciones 1-8.

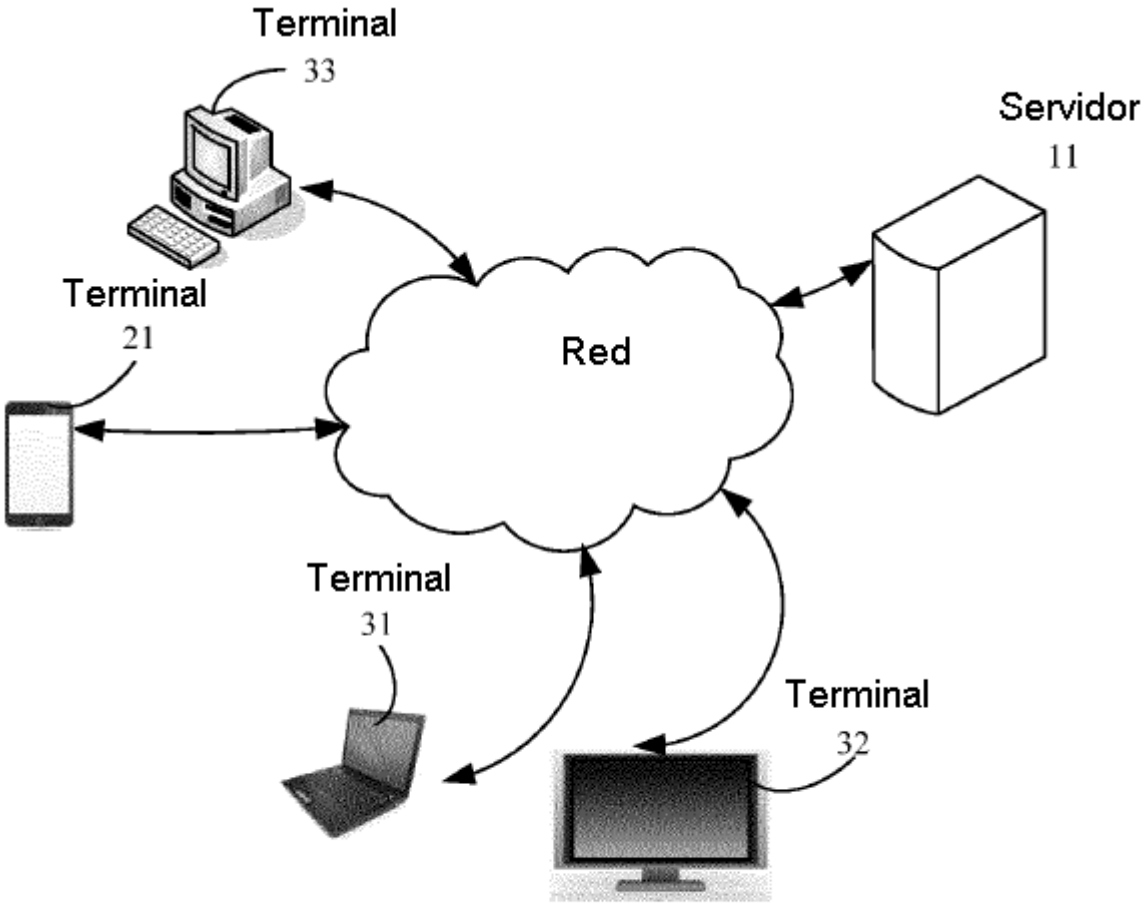
Terminal
33
Servidor
11
Terminal
21
Red
Terminal
31
Terminal
32

FIG. 1

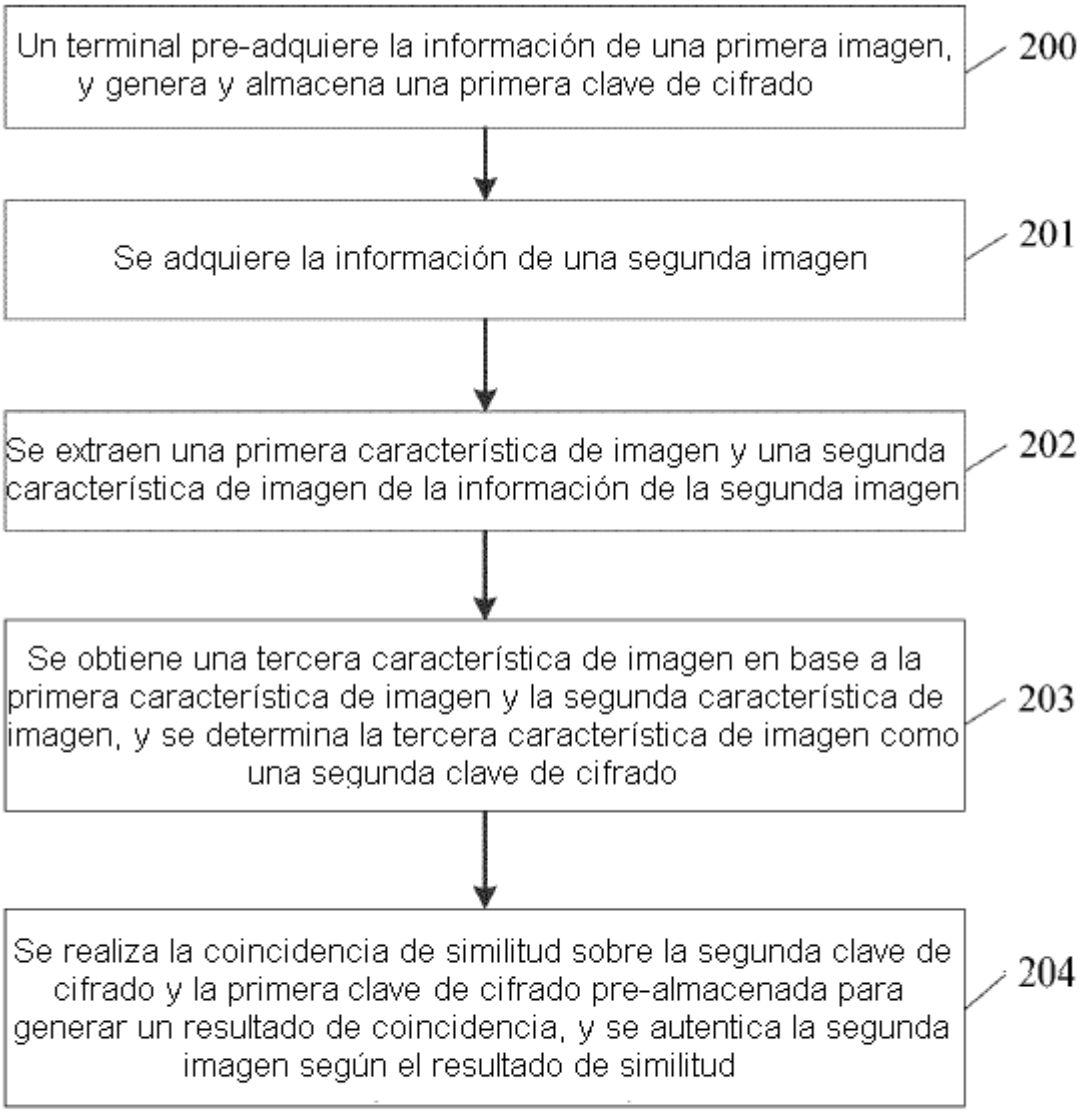
Un terminal pre-adquiere la información de una primera imagen, y genera y almacena una primera clave de cifrado
200
Se adquiere la información de una segunda imagen
201
Se extraen una primera característica de imagen y una segunda característica de imagen de la información de la segunda imagen
202
Se obtiene una tercera característica de imagen en base a la primera característica de imagen y la segunda característica de imagen, y se determina la tercera característica de imagen como una segunda clave de cifrado
203
Se realiza la coincidencia de similitud sobre la segunda clave de cifrado y la primera clave de cifrado pre-almacenada para generar un resultado de coincidencia, y se autentica la segunda imagen según el resultado de similitud
204

FIG. 2

FIG. 3

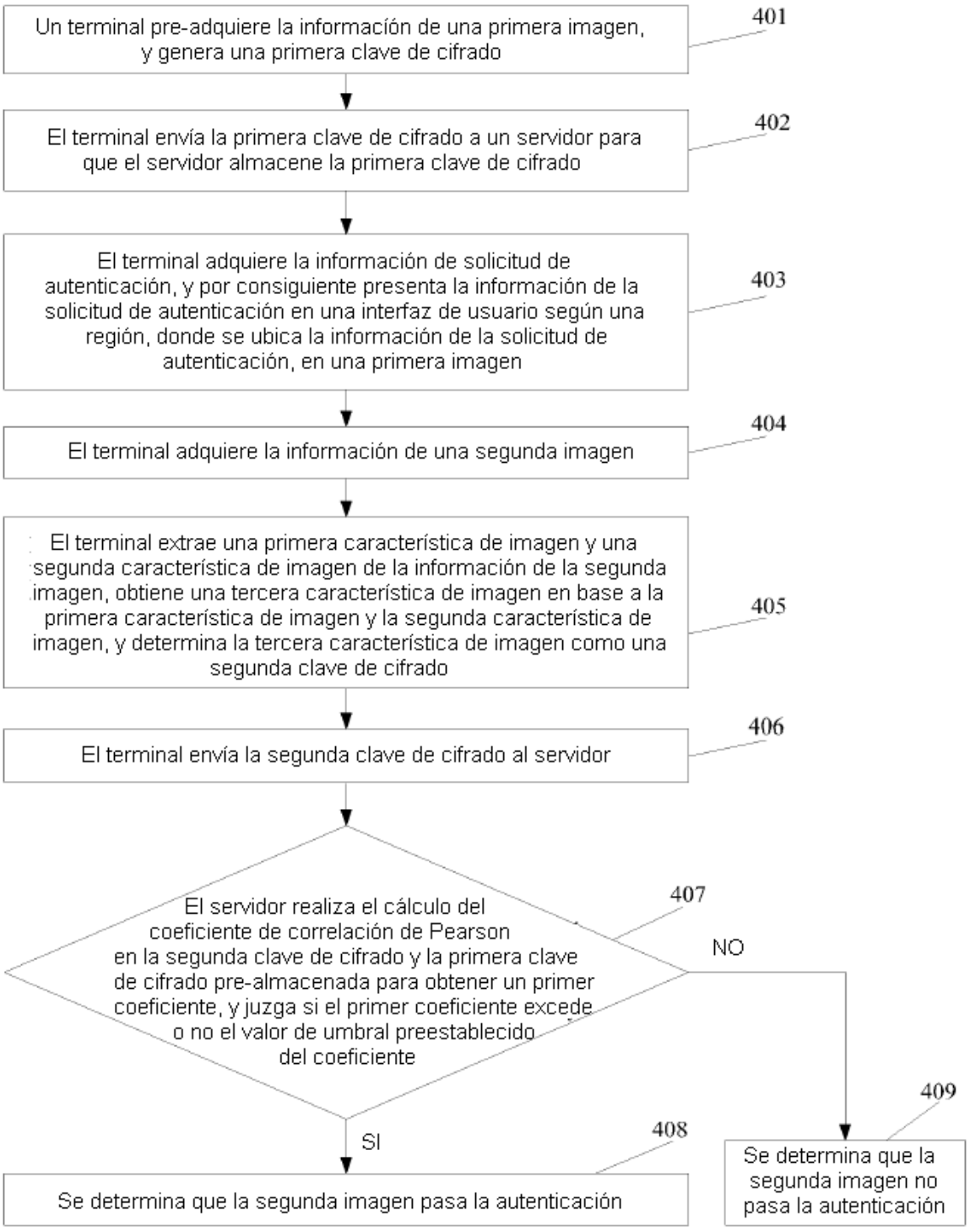
Un terminal pre-adquiere la información de una primera imagen, y genera una primera clave de cifrado
401
El terminal envía la primera clave de cifrado a un servidor para que el servidor almacene la primera clave de cifrado
402
El terminal adquiere la información de solicitud de autenticación, y por consiguiente presenta la información de la solicitud de autenticación en una interfaz de usuario según una región, donde se ubica la información de la solicitud de autenticación, en una primera imagen
403
El terminal adquiere la información de una segunda imagen
404
El terminal extrae una primera característica de imagen y una segunda característica de imagen de la información de la segunda imagen, obtiene una tercera característica de imagen en base a la primera característica de imagen y la segunda característica de imagen, y determina la tercera característica de imagen como una segunda clave de cifrado
405
El terminal envía la segunda clave de cifrado al servidor
406
El servidor realiza el cálculo del coeficiente de correlación de Pearson en la segunda clave de cifrado y la primera clave de cifrado pre-almacenada para obtener un primer coeficiente, y juzga si el primer coeficiente excede o no el valor de umbral preestablecido del coeficiente
407
NO
SI
408
Se determina que la segunda imagen pasa la autenticación
409
Se determina que la segunda imagen no pasa la autenticación

FIG. 4

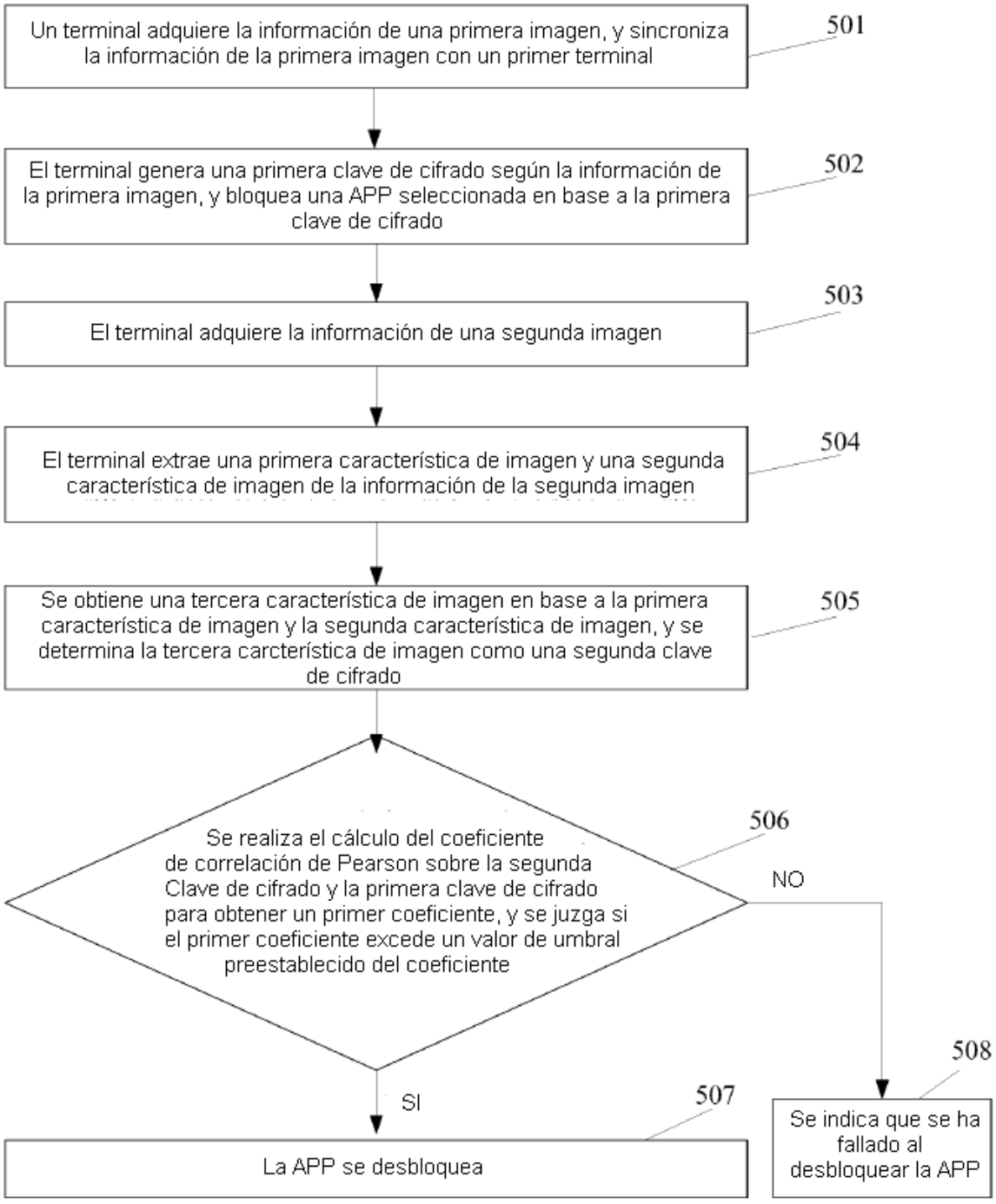
Un terminal adquiere la información de una primera imagen, y sincroniza la información de la primera imagen con un primer terminal
501
El terminal genera una primera clave de cifrado según la información de la primera imagen, y bloquea una APP seleccionada en base a la primera clave de cifrado
502
El terminal adquiere la información de una segunda imagen
503
El terminal extrae una primera característica de imagen y una segunda característica de imagen de la información de la segunda imagen
504
Se obtiene una tercera característica de imagen en base a la primera característica de imagen y la segunda característica de imagen, y se determina la tercera carcterística de imagen como una segunda clave de cifrado
505
Se realiza el cálculo del coeficiente de correlación de Pearson sobre la segunda Clave de cifrado y la primera clave de cifrado para obtener un primer coeficiente, y se juzga si el primer coeficiente excede un valor de umbral preestablecido del coeficiente
506
NO
SI
507
La APP se desbloquea
508
Se indica que se ha fallado al desbloquear la APP

FIG. 5

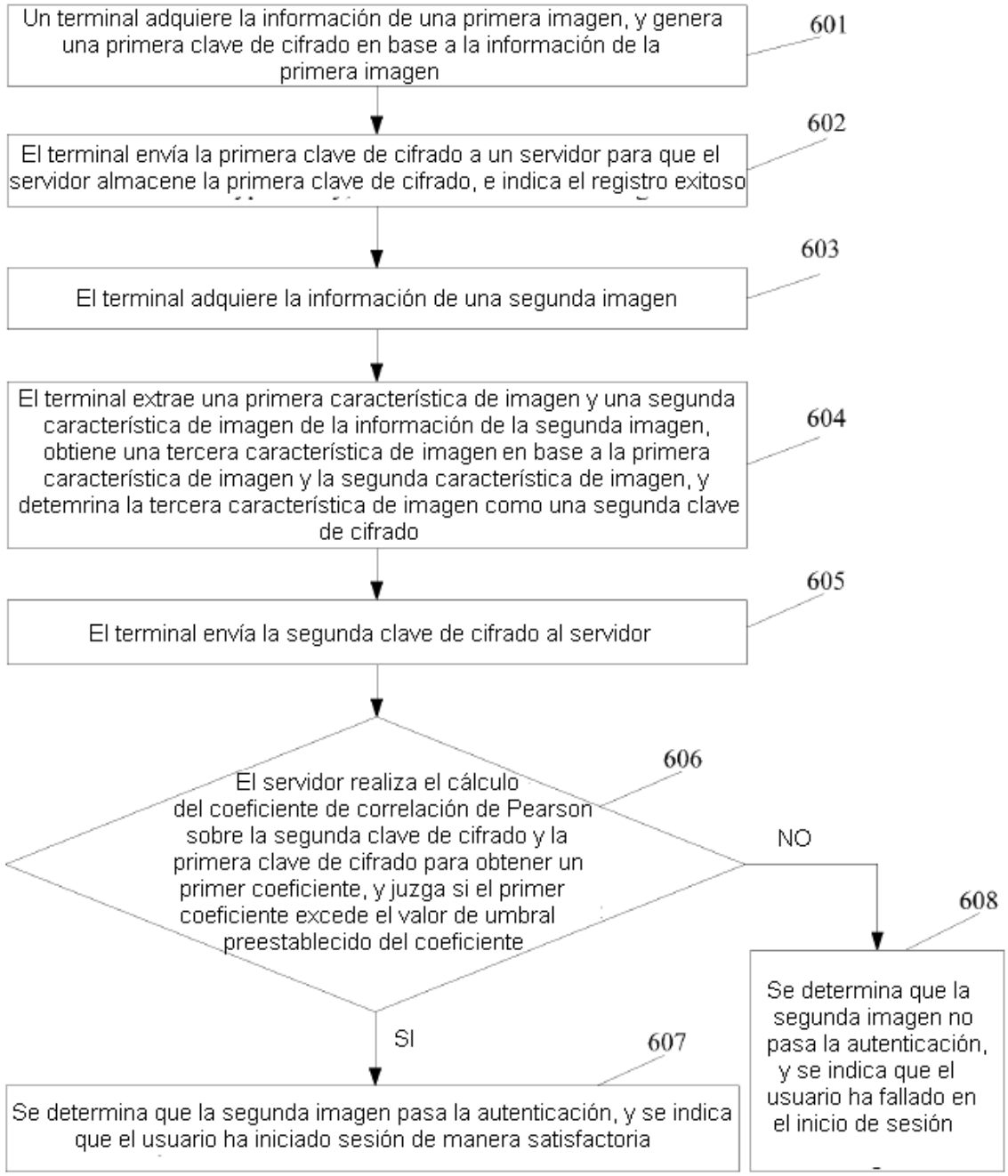
Un terminal adquiere la información de una primera imagen, y genera una primera clave de cifrado en base a la información de la primera imagen
601
El terminal envía la primera clave de cifrado a un servidor para que el servidor almacene la primera clave de cifrado, e indica el registro exitoso
602
El terminal adquiere la información de una segunda imagen
603
El terminal extrae una primera característica de imagen y una segunda característica de imagen de la información de la segunda imagen, obtiene una tercera característica de imagen en base a la primera característica de imagen y la segunda característica de imagen, y detemrina la tercera característica de imagen como una segunda clave de cifrado
604
El terminal envía la segunda clave de cifrado al servidor
605
El servidor realiza el cálculo del coeficiente de correlación de Pearson sobre la segunda clave de cifrado y la primera clave de cifrado para obtener un primer coeficiente, y juzga si el primer coeficiente excede el valor de umbral preestablecido del coeficiente
606
NO
608
Se determina que la segunda imagen no pasa la autenticación, y se indica que el usuario ha fallado en el inicio de sesión
SI
607
Se determina que la segunda imagen pasa la autenticación, y se indica que el usuario ha iniciado sesión de manera satisfactoria

FIG. 6

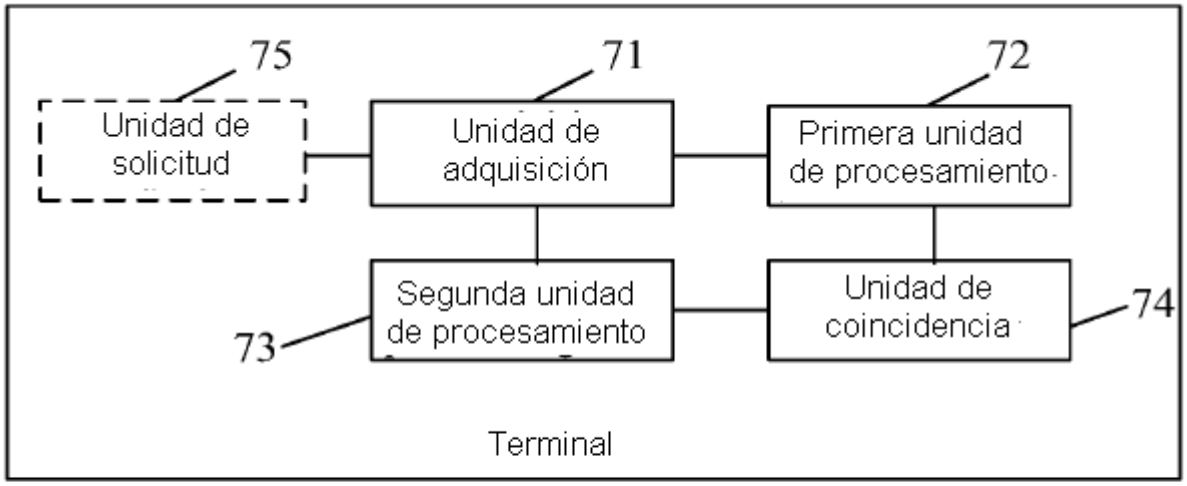
75
71
72
Unidad de solicitud
Unidad de adquisición
Primera unidad de procesamiento
Segunda unidad de procesamiento
Unidad de coincidencia
73
74
Terminal

FIG. 7

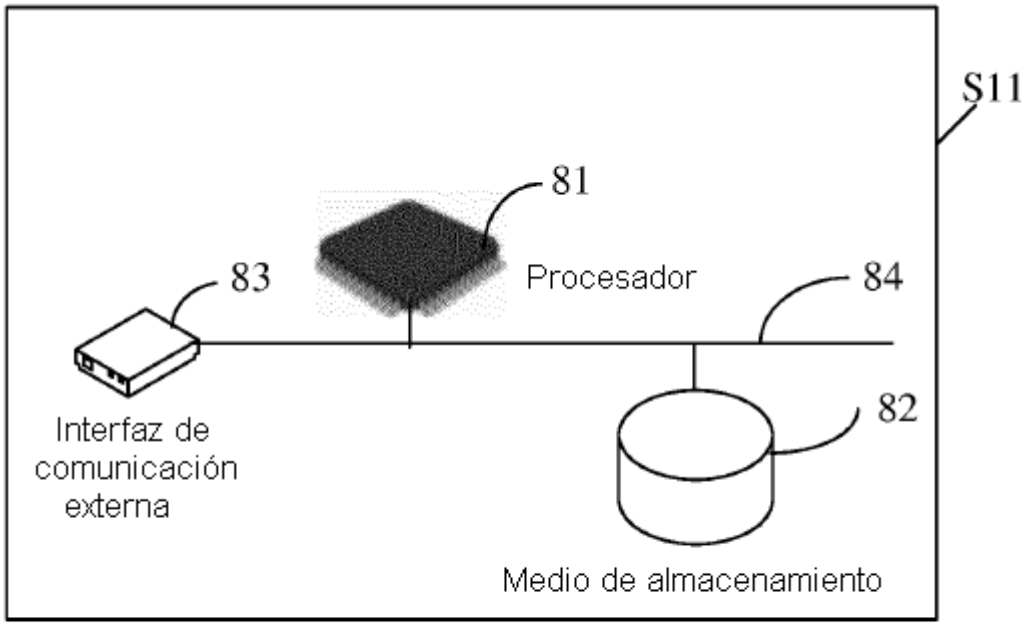
S11
81
Procesador
83
84
82
Interfaz de comunicación externa
Medio de almacenamiento

FIG. 8

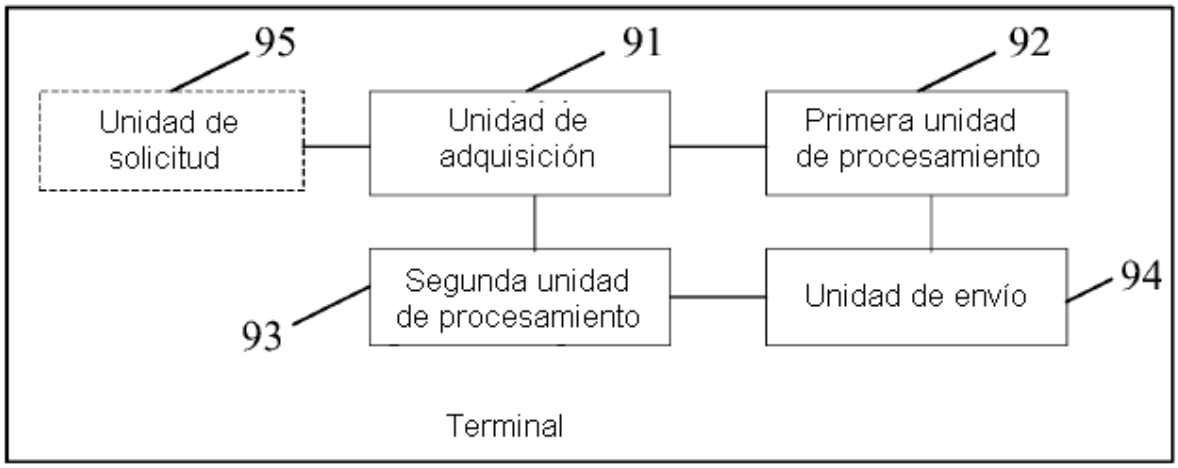
95
91
92
Unidad de solicitud
Unidad de adquisición
Primera unidad de procesamiento
Segunda unidad de procesamiento
Unidad de envío
93
94
Terminal

FIG. 9