(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 427 163**

(51) Int. CI.:

G07D 7/00 (2006.01)
H04L 9/32 (2006.01)
G07B 15/06 (2011.01)
G06F 21/00 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.03.2011 E 11450041 (6)**

(97) Fecha y número de publicación de la concesión europea: **19.06.2013 EP 2503518**

(54) Título: **Procedimiento para validar una transacción de peaje**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.10.2013

(73) Titular/es:

KAPSCH TRAFFICCOM AG (100.0%)
Am Europlatz 2
1120 Wien, AT

(72) Inventor/es:

HAFENSCHER, ALBERT

(74) Agente/Representante:

ZEA CHECA, Bernabé

PROCEDIMIENTO PARA VALIDAR UNA TRANSACCIÓN DE PEAJE

DESCRIPCIÓN

La presente invención se refiere a un procedimiento para validar una transacción de control de tráfico por carretera que se genera mediante la grabación de una imagen de un vehículo en una estación de control de un sistema de control de tráfico por carretera y la lectura OCR (reconocimiento óptico de caracteres) de una matrícula del vehículo en la imagen grabada y que se envía a un receptor de transacción del sistema de control de tráfico por carretera.

Este tipo de sistemas de control de tráfico por carretera se identifica también como “sistemas de control por vídeo”, ya que las transacciones de control se basan en grabaciones de vídeos de tráfico en una estación de control. Los sistemas se pueden usar con múltiples fines de control, por ejemplo, para controlar la presencia de un vehículo en un lugar determinado a fin de facturar el uso de este lugar en forma de peaje viario, peaje por zonas o peaje de aparcamiento, como prueba en caso de controles de velocidad u otras infracciones de tráfico, para supervisar el cumplimiento de las normas relativas al transporte de mercancías peligrosas, la ejecución adecuada de recorridos de quitanieves o de limpieza de carreteras, la entrada y salida de vehículos de flota en recintos industriales o de vehículos de alquiler en oficinas de alquiler o similar.

En este caso, los vehículos se identifican sobre la base de un reconocimiento óptico de caracteres (Optical Character Recognition, OCR) de sus matrículas de vehículo en las imágenes grabadas. En la práctica, el operador del sistema de control de tráfico por carretera (en un sistema de peaje viario, el “Toll Charger”, TC, perceptor de peajes) no es la misma entidad que el receptor y procesador de las transacciones de control que, por lo general, es el propietario del sistema de control de tráfico por carretera o una autoridad estatal (“Contract Issuer”, CI, emisor de contrato). Para estos últimos tiene una importancia decisiva validar la autenticidad de las transacciones de control, enviadas por el operador, a fin de impedir que a los usuarios o a las personas sometidas a control se les facturen, atribuyan o carguen en cuenta transacciones que no han tenido lugar.

Por el documento EP2088568 es conocida una estación de control que en caso de una infracción prepara un documento electrónico con otras grabaciones de vehículo y con otros datos, como la matrícula leída por OCR o la clase de vehículo detectada. Antes de enviarse el documento elaborado a la central mediante una vía de comunicación, dado el caso, insegura, este documento se firma de acuerdo con un procedimiento convencional de private-public-key (clave pública-privada). Esto permite detectar una manipulación en la vía de transmisión, pero no es posible, sin embargo, una validación o autentificación de toda la transacción de control, incluida la elaboración del documento, por lo que cada una de las estaciones de control se ha de proteger de manera costosa con sistemas sensores adicionales.

Hasta el momento no hay ninguna posibilidad para realizar tal validación o autentificación de transacciones. La invención tiene el objetivo de proporcionar una solución de este tipo.

Este objetivo se consigue según la invención mediante un procedimiento del tipo mencionado al inicio con las características de la reivindicación 1.

Con ayuda del procedimiento según la invención, el receptor de transacción (Contract Issuer) puede comprobar transacciones de peaje directamente en la interfaz con el operador del sistema de control, por ejemplo, un operador del sistema de peaje (Toll Charger), y rechazar transacciones de control no autentificadas. La invención se basa aquí en el uso de un elemento de procesamiento separado en la estación de control, que goza de la confianza del receptor de transacción y que con este fin se provee de una clave criptográfica del receptor de transacción. En combinación con una clave aleatoria de la estación de control, que es única para cada transacción o imagen grabada, se generan datos de autentificación para el receptor de transacción que le permiten validar la transacción de control original sobre la base de la imagen grabada originalmente mediante la comprobación autárquica, por su parte, de los datos de autentificación.

La estación de control mencionada puede ser tanto fija como móvil y comprender una o varias cámaras, así como componentes repartidos geográficamente, por ejemplo, un ordenador remoto proxy para evaluar la matrícula por OCR.

Según una realización preferida de la invención, en el elemento de procesamiento se almacenan varias claves criptográficas asignadas a distintos receptores de transacción, y la clave criptográfica, que se va a usar respectivamente, se selecciona en función de la matrícula leída por OCR. De este modo se pueden autentificar por separado directamente en su origen y validar a continuación transacciones de control para distintos receptores de transacción, por ejemplo, diferentes autoridades, policía, bomberos, servicios de mantenimiento de carreteras, etc.

Los datos de autentificación y la clave aleatoria se envían preferentemente junto con la transacción de control al receptor de transacción, de manera que la transacción de control contiene de manera directa los datos que posibilitan su validación. Alternativamente, los datos de autentificación y la clave aleatoria se pueden enviar también junto con la imagen grabada al receptor de transacción, previéndose referencias correspondientes a la transacción de control.

Como se establece en la reivindicación 1, la clave aleatoria define según la invención una sección de imagen en la imagen grabada y la codificación mencionada de la imagen grabada con la clave aleatoria comprende el paso de extraer la sección de imagen de la imagen grabada y el paso de formar un primer valor hash de la sección de imagen. Por tanto, una capacidad de cálculo extremadamente pequeña en el elemento de procesamiento es suficiente para conseguir el objetivo deseado, ya que la codificación, que tiene lugar aquí, siempre que esté relacionada con la clave aleatoria, se limita a extraer una sección de imagen aleatoria de la imagen grabada y a formar un valor hash de la misma. La selección de una sección de imagen reduce en gran medida el volumen de datos, y la formación de un valor hash es una operación informática muy simple. De este modo, al realizarse la codificación ulterior con la clave criptográfica, el valor hash mencionado está disponible como juego de datos inicial, fuertemente reducido, y es posible usar cualquier procedimiento de codificación conocido en la técnica con un pequeño coste.

La sección de imagen extraída contiene preferentemente también la matrícula del vehículo, lo que aumenta la seguridad de la validación.

Es particularmente favorable que también esta segunda codificación se lleve a cabo con ayuda de la formación de un valor hash, es decir, la codificación mencionada de la imagen grabada con la clave criptográfica comprende el paso de formar un segundo valor hash a partir del primer valor hash y de la clave criptográfica, constituyendo a continuación este segundo valor hash los datos de autentificación.

La sección de imagen mencionada puede ser cualquier parte de la imagen grabada que se puede definir mediante la clave aleatoria. Así, por ejemplo, la clave aleatoria define los puntos angulares de un contorno periférico que encierra una sección de imagen plana. Alternativamente, la clave aleatoria podría predefinir valores de color de píxeles, y todos los píxeles con estos valores de color formarían conjuntamente la sección de imagen mencionada.

En la presente descripción se entiende por “formación de un valor hash” la aplicación de una función de representación n:1 prácticamente irreversible al valor de entrada, es decir, una función que es reversible sólo de manera (extremadamente) multiforme, por lo que a partir del valor hash conocido ya no se puede inferir prácticamente el valor inicial (en este caso, la sección de imagen). Como ejemplos de este tipo de funciones hash se pueden mencionar la función de suma horizontal, la función módulo, etc.

En otras configuraciones ventajosas de la invención se pueden integrar en los datos de autentificación un sello de tiempo, una identificación de la estación de control, una identificación del elemento de procesamiento y/o un valor de conteo continuo. Cada uno de estos datos se puede usar para pruebas de plausibilidad posteriores, lo que permite aumentar la seguridad de la validación.

Es posible además almacenar varias claves criptográficas con identificaciones de clave asignadas en el receptor de transacción y en el elemento de procesamiento, integrar la identificación de clave de la clave usada en los datos de autentificación y usarla en el receptor de transacción para determinar la clave asignada. Esto permite aumentar también la seguridad del sistema.

El elemento de procesamiento, que sirve como unidad de autentificación, puede ser tanto un elemento de software como un elemento de hardware. Se usa preferentemente un elemento de hardware que se conecta mediante una interfaz física a la estación de control, por ejemplo, en forma de un módulo de hardware protegido criptográficamente (Secure Access Module, SAM, módulo de acceso seguro), un token USB, etc. A este respecto, se puede prever también preferentemente que la separación de la interfaz inutilice el elemento de hardware para impedir manipulaciones y proporcionar una alta protección de confianza al receptor de transacción.

Según otra característica preferida de la invención, la transacción de control complementada es enviada por la estación de control al receptor de transacción a través de un primer canal y la imagen grabada es enviada por la estación de control al receptor de transacción a través de un segundo canal, asignándose entre sí la transacción de control complementada y la imagen grabada correspondiente en el receptor de transacción por medio de al menos una referencia mutua. Por consiguiente, no es imprescindible que las transacciones de control y las imágenes grabadas lleguen simultáneamente al receptor de transacción; por ejemplo, las imágenes grabadas, acumuladas en bases de datos, se podrían poner a disposición del receptor de transacción para la validación.

La invención se explica detalladamente a continuación por medio de un ejemplo de realización representado en los dibujos adjuntos. En los dibujos muestran:

Fig. 1 un esquema de bloques de un sistema de peaje viario interoperable como sistema de control de tráfico por carretera, a modo de ejemplo, según la invención;
Fig. 2 esquemáticamente, una de las estaciones de control del sistema de peaje viario de la figura 1; y
Fig. 3 un diagrama de flujo de señales del procedimiento, según la invención, para validar transacciones de control en el marco del sistema de peaje viario de la figura 1.

Según la figura 1, en un sistema de control de tráfico por carretera interoperable, en este caso un sistema de peaje viario 1, se generan transacciones de control tr mediante una pluralidad de estaciones de control diferentes (en este caso: Tolling Entities, entidades de peaje) TE y estas transacciones de control se envían a través de centrales específicas del operador (en este caso: Toll Charger) TC a receptores de transacción CI (Contract Issuer) para el procesamiento y/o la facturación. Los receptores de transacción CI pueden recibir transacciones de control tr de distintas centrales de operador TC y éstas se pueden conectar a su vez a una pluralidad de estaciones de control TE diferentes, de las que se muestra una a modo de ejemplo en la figura 2.

La estación de control TE de la figura 2 comprende una radiobaliza 2 opcional, por ejemplo, según el estándar DSRC (Dedicated Short Range Communication, comunicación dedicada de corto alcance) o el estándar WAVE (Wireless Access in a Vehicle Environment, conexión inalámbrica en entorno vehicular), y una cámara fotográfica o cámara de vídeo 3 que están conectadas a un ordenador de estación 4 que a su vez está conectado a la central TC (figura 1). La radiobaliza 2 permite generar, por ejemplo, transacciones de peaje basadas en el estándar DSRC, mediante la radiocomunicación 5 con aparatos de vehículo (Onboard Units, OBUs, unidades de a bordo) 6 que son transportados por vehículos 7 que pasan por la estación TE en una carretera 8.

Con ayuda de la cámara 3 se pueden generar transacciones de control, basadas en vídeos, al grabar la cámara 3 una imagen pic del vehículo 7, en la que se lee a continuación la matrícula de vehículo 9 en una placa de matrícula del vehículo 7 mediante el reconocimiento óptico de caracteres (Optical Character Recognition, OCR). La matrícula de vehículo 9 como resultado de la evaluación por OCR de la imagen grabada pic representa, por ejemplo, tras complementarse con un sello de tiempo actual, un valor de medición de velocidad del vehículo y/o una identificación de la estación de control TE o la cámara 3, la base de una transacción de control tr basada en vídeos que se envía al receptor de transacción CI a través de una central TC.

En el caso de la matrícula de vehículo 9 leída por OCR se puede tratar del número de matriculación del vehículo, pero también de otras matrículas del vehículo posibles de leer por OCR, por ejemplo, una matrícula de mercancía peligrosa, una matrícula de flota, etc.

A fin de posibilitar al receptor de transacción CI una validación (autentificación) de tales transacciones tr basadas en vídeos, las estaciones de control TE basadas en vídeos están equipadas con un elemento de procesamiento separado (Authentication Entity, entidad de autentificación) AE que se puede asignar individualmente a toda la estación de control TE o a una o cada cámara 3 de la misma.

En un primer paso 11, una clave criptográfica (Trusted Key, clave confiable) tk, que está asignada de manera única a un receptor de transacción CI y que es de su confianza, se almacena, por una parte, en el receptor de transacción CI y, por la otra parte, en cada estación de control tr, de la que se debe recibir la transacción de control TR, más exactamente en el respectivo elemento de procesamiento AE de la estación de control TE (figura 1).

La figura 3 muestra a continuación los pasos de procesamiento o flujos de señales durante el paso de un vehículo 7 por una estación de control TE que está equipada con tal elemento de procesamiento AE y genera una transacción de control tr que se envía, a modo de ejemplo, a un receptor de transacción CI a través de la central de operador TC. Las claves criptográficas tk de los distintos receptores de transacción CI, a los que la estación de control TE puede enviar las transacciones de control tr, ya se encuentran almacenadas en el elemento de procesamiento AE, véase el juego de datos tk 12.

La cámara 3 graba una imagen pic del vehículo 7 al pasar por la estación de control TE y a partir de esta imagen genera en un proceso OCR 13 una transacción de control tr sobre la base del resultado de la lectura de matrícula por OCR de la matrícula de vehículo 9. La transacción de control tr puede contener otros datos, como un sello de tiempo, una identificación de la estación de control TE y/o de la cámara 3, una identificación del elemento de procesamiento AE, un valor de conteo incrementado de manera continua (contador de transacción), etc. Se entiende que el proceso OCR 13 se podría calcular también en un ordenador proxy (no mostrado), distante geográficamente, que se ha de asignar a la estación de control TE.

El elemento de procesamiento AE recibe la imagen grabada pic y genera una clave aleatoria rd para la misma. Sobre la base de la clave aleatoria rd se extrae en un proceso 14 una sección de imagen aleatoria p a partir de la imagen grabada pic y se genera un valor hash h(p) de la sección de imagen p, por ejemplo, mediante adición modular de los píxeles en la sección de imagen p. La clave aleatoria rd indica, por ejemplo, directamente las coordenadas de imagen de al menos tres píxeles en la imagen grabada pic que generan o definen la sección de imagen p. Alternativamente, la clave aleatoria rd podría predefinir determinadas propiedades de píxeles, por ejemplo, valores de color, y todos los píxeles con estas propiedades forman la sección de imagen p.

La extracción de una sección de imagen aleatoria p de la imagen grabada pic y la formación de un valor hash h de la sección de imagen p necesitan sólo una capacidad de cálculo pequeña y, por tanto, se pueden llevar a cabo también en tiempo real, por ejemplo, con medios procesadores simples en el documento de procesamiento AE, como los procesadores existentes, por ejemplo, en tarjetas chip o tarjetas SIM.

En un proceso 15, el valor hash h, formado de esta manera, se vuelve a codificar a continuación con la clave criptográfica tk del respectivo receptor de transacción TE, hacia el que está dirigida la transacción de control tr. El proceso de codificación 15 se puede realizar también mediante una nueva formación de un valor hash a partir del valor hash h mencionado antes y la clave criptográfica tk.

La clave tk correcta se puede seleccionar, por ejemplo, sobre la base de las listas de asignación (“white lists”, listas blancas), almacenadas en la estación de control TE, de matrículas de vehículo 9 y receptores de transacción CI correspondientes, es decir, el resultado de la lectura de matrícula del proceso OCR 13 controla la selección de la clave criptográfica tk a partir del juego 12 (flecha 16).

A la salida o al final del proceso 15 se obtienen datos de autentificación au que se adicionan junto con la clave aleatoria rd a la transacción de control tr para su ampliación en forma de una transacción de control complementada {tr,rd,au} 17. En este caso, a los datos de autentificación au se pueden añadir también otros datos, como un sello de tiempo, una identificación de la estación de control TE y/o de la cámara 3, una identificación del elemento de procesamiento AE, un valor de conteo incrementado de manera continua (contador de transacción), etc., o estos datos pueden estar integrados en los datos de autentificación.

La transacción de control complementada 17 se envía a continuación al receptor de transacción CI a través de un primer canal de transmisión 18 que comprende también, por ejemplo, una central de operador TC en su recorrido. La imagen grabada pic, en la que se basa la transacción de control tr, se envía también al receptor de transacción CI a través de un segundo canal de transmisión 19. El envío a través del primer y del segundo canal de transmisión 18, 19 no se tiene que realizar simultáneamente. Así, por ejemplo, tanto las transacciones de control complementadas 17 como preferentemente también las imágenes grabadas pic se podrían almacenar de manera temporal, por ejemplo, en bases de datos 20 de la central de operador TC, y poner a disposición a solicitud del receptor de transacción CI. Esto entra asimismo en el concepto de “enviar”. Otra posibilidad consiste en no añadir los datos de autentificación au y la clave aleatoria rd a la transacción de control tr, sino a los datos de imagen pic. Todos los datos tr, rd, au, pic se pueden enviar también a través del mismo canal de transmisión.

Se entiende que en realizaciones simplificadas puede tener lugar también, en vez de los procesos preferidos mostrados 14, 15, sólo un único proceso de codificación o paso de codificación en el elemento de procesamiento AE, en el que la imagen grabada pic se codifica en un paso con la clave aleatoria rd y la clave criptográfica tk para obtener los datos de autentificación au. Así, por ejemplo, la clave aleatoria rd y la clave criptográfica tk se podrían combinar en una clave común que se aplica a la imagen grabada pic para obtener así los datos de autentificación au.

En el receptor de transacción CI se combinan a continuación las transacciones de control complementadas 17 recibidas y las imágenes grabadas pic recibidas que sirven de base a éstas, es decir, se asignan una a otra, por ejemplo, por medio de al menos una referencia mutua en uno de estos datos, por ejemplo, una referencia a una identificación única de una imagen grabada pic en la transacción de control tr o una referencia a una identificación única de una transacción de control tr en una imagen grabada pic o ambas. El receptor de transacción CI podría validar también sólo aleatoriamente transacciones de control tr al procesar o recibir, únicamente en caso necesario, la imagen grabada asignada pic correspondiente, por ejemplo, al solicitarla a la base de datos 20 de la central de operador TC. Si la imagen grabada pic se recibe junto con la transacción de control complementada 17, no es necesario hacer una asignación.

En un primer paso 21, la clave aleatoria rd se extrae ahora de la transacción de control complementada 17 en el receptor de transacción CI y se aplica en la imagen grabada pic asignada recibida en un proceso 22, similar al proceso 14 en el elemento de procesamiento AE, para volver a obtener la sección de imagen aleatoria p y formar el valor hash h para la misma. Este valor hash se codifica nuevamente con la clave criptográfica tk del receptor de transacción CI en un proceso 23, similar al proceso 15 del elemento de procesamiento AE, para obtener datos de

referencia o autentificación nominales au_r. Estos datos se comparan a continuación en un paso o proceso 24 con los datos de autentificación au, extraídos de la transacción de control complementada 17 y, si son iguales, se valida la transacción tr, es decir, se considera que está autentificada y queda libre para el procesamiento y/o la facturación ulteriores en el receptor de transacción CI. Si no son iguales, se ha producido un error o una manipulación y la transacción tr no está validada (sin validez) y se descarta. Se puede emitir y registrar entonces un mensaje correspondiente de alarma.

Para cada receptor de transacción CI se pueden almacenar opcionalmente varias claves criptográficas tk_i diferentes, en cada caso con una identificación de clave tkID asignada, en el juego de datos 12 del elemento de procesamiento AE y en el receptor de transacción CI (no representado). En el elemento de procesamiento AE se selecciona a continuación una clave tk_i del respectivo receptor de transacción CI con su identificación de clave tkID y se usa para la codificación. La identificación de clave tkID de la clave tk_i usada se añade ahora a los datos de autentificación au y se usa en el receptor de transacción CI para identificar la clave tk_i correcta.

El elemento de procesamiento AE se puede diseñar tanto como módulo de software protegido de manera criptográfica como también, preferentemente, como elemento de hardware protegido de manera física. El elemento de procesamiento AE se puede conectar en particular mediante una interfaz física 25 a la estación de control TE que en el caso más simple puede ser también sólo la cámara 3. Se toman medidas para que una separación no autorizada de la interfaz 25 inutilice el elemento de procesamiento AE diseñado como elemento de hardware, por ejemplo, una separación de la interfaz 25 borra irremediablemente la memoria del elemento de procesamiento AE o bloquea de forma permanente al menos cada acceso a la clave criptográfica rd, tk.

La invención no está limitada a las realizaciones representadas, sino que comprende todas las variantes y modificaciones que entran en el marco de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Procedimiento para validar una transacción de control de tráfico por carretera (tr), que es enviada por una estación de control (TE) de un sistema de control de tráfico por carretera (1) a un receptor de transacción (CI) del sistema de control de tráfico por carretera (1), en el receptor de transacción (CI), que comprende los siguientes pasos:

almacenar una clave criptográfica (tk), asignada al receptor de transacción (CI), en el receptor de transacción (CI) y en un elemento de procesamiento (AE) separado de la estación de control (TE);
grabar una imagen (pic) de un vehículo (7), leer por OCR una matrícula (9) del vehículo (7) en la imagen grabada (pic) y generar una transacción de control (tr) a partir de esto en la estación de control (TE);
generar una clave aleatoria (rd) que define una sección de imagen (p) en la imagen grabada (pic), y codificar la imagen grabada (pic) con la clave aleatoria (rd) y con la clave criptográfica (tk) para obtener datos de autentificación (au) en el elemento de procesamiento separado (AE) mediante los siguientes procesos:

- extraer la sección de imagen (p) de la imagen grabada (pic),
- formar un primer valor hash (h) de la sección de imagen (p) y
- codificar el primer valor hash (h) con la clave criptográfica (tk) para obtener los datos de autentificación (au);

enviar la imagen grabada (pic), la transacción de control (tr), la clave aleatoria (rd) y los datos de autentificación (au) al receptor de transacción (CI);
codificar en el receptor de transacción la imagen grabada (pic) recibida con la clave aleatoria (rd) recibida y con la clave criptográfica (tk) almacenada para obtener datos de autentificación nominales (au_r), específicamente mediante los mismos procesos que en el elemento de procesamiento (AE), y
comparar los datos de autentificación (au) recibidos con los datos de autentificación nominales (au_r),
validándose la transacción de control (tr) recibida en caso de igualdad.

2. Procedimiento según la reivindicación 1, **caracterizado porque** la codificación mencionada del primer valor hash (h) con la clave criptográfica (tk) comprende el paso de formar un segundo valor hash a partir del primer valor hash (h) y de la clave criptográfica (tk), constituyendo este segundo valor hash los datos de autentificación (au).

3. Procedimiento según la reivindicación 1 ó 2, **caracterizado porque** en el elemento de procesamiento se almacenan varias claves criptográficas (tk), asignadas a distintos receptores de transacción (CI), y la clave criptográfica (tk), que se va a usar respectivamente, se selecciona en función de la matrícula (9) leída por OCR.

4. Procedimiento según una de las reivindicaciones 1 a 3, **caracterizado porque** los datos de autentificación (au) y la clave aleatoria (rd) se envían junto con la transacción de control (tr) al receptor de transacción (CI).

5. Procedimiento según una de las reivindicaciones 1 a 3, **caracterizado porque** los datos de autentificación (au) y la clave aleatoria (rd) se envían junto con la imagen grabada (pic) al receptor de transacción (CI).

6. Procedimiento según una de las reivindicaciones 1 a 5, **caracterizado porque** en los datos de autentificación (au) se integran un sello de tiempo, una identificación de la estación de control (TE), una identificación del elemento de procesamiento (AE) y/o un valor de conteo continuo.

7. Procedimiento según una de las reivindicaciones 1 a 6, **caracterizado porque** en el receptor de transacción (CI) y en el elemento de procesamiento (AE) se almacenan varias claves criptográficas (tk_i) con identificaciones de clave (tkID) asignadas, integrándose la identificación de clave (tkID) de la clave (tk_i) usada en los datos de autentificación (au) y usándose esta identificación de clave en el receptor de transacción (CI) para determinar la clave (tk_i) asignada.

8. Procedimiento según una de las reivindicaciones 1 a 7, **caracterizado porque** como elemento de procesamiento (AE) mencionado se usa un elemento de hardware que se conecta a la estación de control (TE) mediante una interfaz física (25).

9. Procedimiento según la reivindicación 8, **caracterizado porque** la separación de la interfaz (25) inutiliza el elemento de hardware (AE).

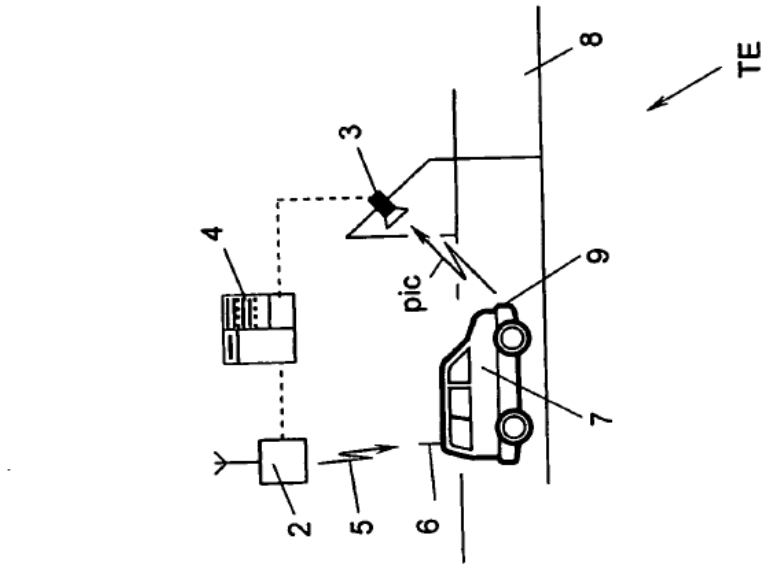
8
TE
3
4
pic
9
7
2
5
6

Fig. 2

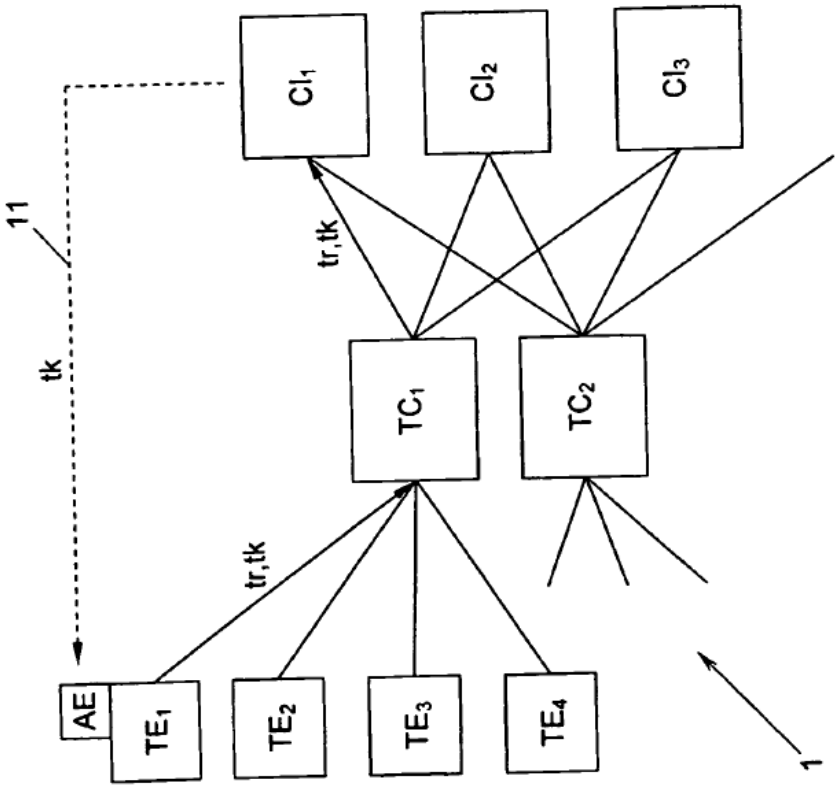
11
tk
Cl1
Cl2
Cl3
tr,tk
TC1
TC2
tr,tk
AE
TE1
TE2
TE3
TE4
1

Fig. 1

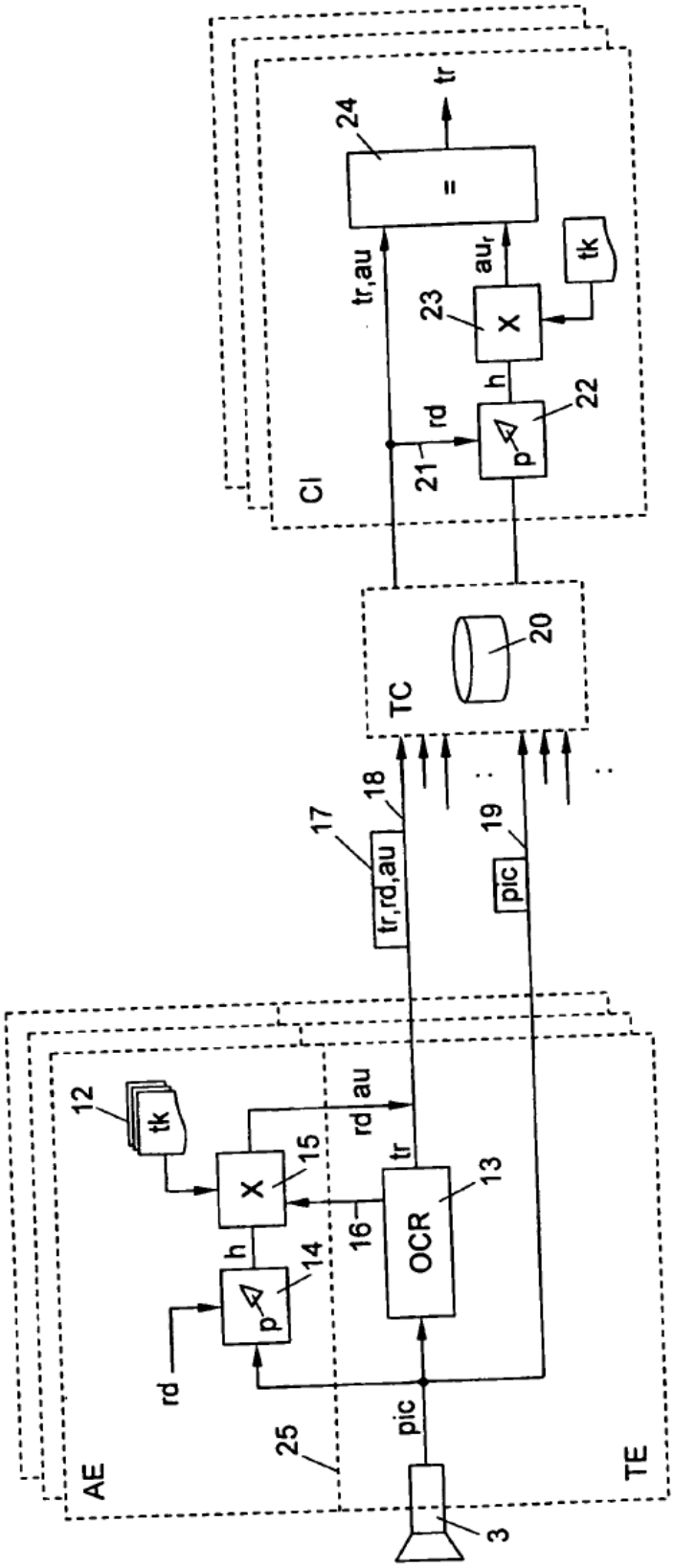
AE
TE
CI
TC
tk
X
p
h
rd
au
tr
OCR
pic
=
tr,au
tr,rd,au
au_r
12
13
14
15
16
17
18
19
20
21
22
23
24
25
3

Fig. 3

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

Esta lista de referencias citadas por el solicitante es únicamente para la comodidad del lector. No forma parte del documento de la patente europea. A pesar del cuidado tenido en la recopilación de las referencias, no se pueden excluir errores u omisiones y la EPO niega toda responsabilidad en este sentido.

Documentos de patente citados en la descripción

• EP2088568A **[0004]**