(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 393 014**

(21) Número de solicitud: 201031412

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 9/08 (2006.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

23.09.2010

(43) Fecha de publicación de la solicitud:

17.12.2012

(43) Fecha de publicación del folleto de la solicitud:

17.12.2012

(71) Solicitantes:

UNIVERSIDAD DE ALCALÁ (100.0%)
Plaza de San Diego, s/n
28801 Alcalá de Henares, Madrid, ES

(72) Inventor/es:

MALDONADO BASCÓN, Saturnino;
ACEVEDO RODRÍGUEZ, Francisco Javier;
GIL JIMÉNEZ, Pedro;
LAFUENTE ARROYO, Sergio;
GÓMEZ MORENO, Hilario;
MALLOL POYATO, Ricardo;
SÁNCHEZ GOLMAYO, Jesús y
LÓPEZ SASTRE, Roberto Javier

(74) Agente/Representante:

GUTIÉRREZ DE MESA, José Antonio

(54) Título: **EQUIPO DE AUTENTICACIÓN DE FECHA Y HORA PARA VIDEO ESCENAS.**

(57) Resumen:

Equipo de autenticación de fecha y hora para vídeo.
El equipo objeto de esta invención tiene como objetivo la autenticación de la fecha y la hora proporcionadas en una secuencia de vídeo de una escena vigilada. Para ello se emplea un panel de autenticación (1) presente en la escena a auditar que mostrará un código (2) encriptado con la fecha y la hora. El panel estará dotado de información al usuario (3) y marcas de referencia (4) y estará gobernado por un sistema de control (5). La información del panel es capturada por una cámara (8) y llevada a un servidor (9) donde un software analizará las distintas imágenes y desencriptará el código proporcionado por el panel. El panel propuesto tendrá un sistema de alimentación (7) que puede ser autónomo y alimentado por un placa solar (6).

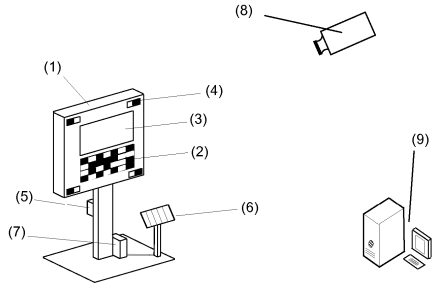

Figura 1

ES 2 393 014 A1

EQUIPO DE AUTENTICACIÓN DE FECHAY HORA PARA VÍDEO ESCENAS

DESCRIPCIÓN

SECTOR DE LA TÉCNICA

La presente invención se encuentra dentro de las tecnologías de la información y las comunicaciones y en concreto dentro del campo de la auditoría de video secuencias.

ESTADO DE LA TÉCNICA

La autenticación de los sistemas de video vigilancia comprende el proceso de preservar la integridad del vídeo original así como los datos asociados de la escena. Este proceso, en el que se asegura que las imágenes no han sido manipuladas, tiene especial importancia para la presentación de secuencias de vídeo como una evidencia en procesos penales o en auditorías. Además de la preservación del contenido es importante validar la fecha y la hora asociadas a la secuencia considerada. Un ejemplo concreto donde se requiere éstos datos asociados a la video-secuencia es en los sistemas de peaje a la sombra, en los que una empresa concesionaria de una autopista factura al gobierno dependiendo del número de vehículos y tamaño de los mismos que circulan por dicha autopista. Para que el gobierno pueda validar los datos se le proporcionan las secuencias de vídeo, pero sería necesario validar que las fechas correspondientes a dichas secuencias son las reales y no corresponden a secuencias tomadas en fechas u horas diferentes.

Las técnicas actuales de autenticación del contenido del vídeo se pueden dividir en dos grandes grupos: criptografía de los datos digitales obtenidos y añadir marcas de agua (watermarking) a las imágenes de la secuencia. El primer grupo se basa en codificar la secuencia digitalizada de la escena mediante algún tipo de algoritmo criptográfico [1], de forma que se imposibilita la manipulación de los datos si no se tiene la clave correspondiente. En los sistemas basados en watermarking se enmascara dentro de cada imagen una marca no visible, de forma que si se manipulan las imágenes se pierde la

marca, constatando que el vídeo ha sido manipulado. Algunos trabajos que describen la inclusión de este tipo de marcas son [2-5]. Además de estos dos grupos de técnicas existen también algunas propuestas en forma experimental que tratan de verificar la manipulación del contenido del video mediante técnicas de reconocimiento de patrones [6]. En la actualidad existen cámaras que pueden incorporar técnicas de criptografía, así como de watermarking.

Sin embargo, al auditar las escenas, además de verificar que no han sido manipuladas, se debe asegurar que la fecha y la hora corresponden con la realidad y que la secuencia no corresponde con lo sucedido en otra franja de tiempo. Si bien este problema puede ser resuelto mediante la encriptación de esos datos en la secuencia de vídeo, esto requiere tener cámaras que sean capaces de realizar tal encriptación, por lo que se haría necesario sustituir todo el sistema de video vigilancia. Por otro lado, el usuario que requiere la autenticación de la fecha y la hora no tiene por qué ser el propietario del sistema de video vigilancia, como se da en el ejemplo del peaje a la sombra, por lo que la manipulación de las mismas puede ser realizada antes de que se produzca el cifrado del mismo.

DESCRIPCIÓN DE LA INVENCIÓN

Descripción General

El equipo que se describe en esta invención consta de un panel de autenticación (1) que mostrará en un área de código (2) la fecha y la hora encriptadas consistiendo la representación de dicho código en la iluminación por medio de diferentes colores de una serie de LEDs o panel de LEDs. El panel también puede contener un área de información al usuario (3) destinado a mostrar mensajes o imágenes que no tiene por qué estar relacionada con la aplicación. El panel mostrará también unas marcas de referencia (4) necesarias para localizar dicho panel en un sistema de análisis de las secuencias cuando la cámara tiene cierto movimiento debido a oscilaciones físicas. El sistema de control del panel (5) estará encargado de obtener la fecha y la hora,

sincronizarlas, almacenar las claves criptográficas, ejecutar el algoritmo de encriptación, además de controlar posibles funciones adicionales de monitorización del propio panel y de la alimentación recibida, así como de controlar la comunicación con el servidor de análisis (9). La energía necesaria para alimentar el panel puede ser obtenida mediante una placa solar (6) conectada a un sistema de regulación de carga inteligente y de acumulación de batería (7), contemplando también la posibilidad de utilizar una batería simple.

La escena vigilada, en la que se incluye el panel de autenticación, es captada por una cámara (8) y digitalizada junto con la información de fecha y hora proporcionada por la cámara, de forma que la información se envía a un servidor con los algoritmos necesarios para localizar el panel de autenticación en la imagen, leer correctamente el código reflejado en la escena real y desencriptarlo para verificar que la fecha y hora de la escena reales coinciden con la información proporcionada junto con la secuencia de vídeo.

Descripción Detallada.

El equipo de autenticación de fecha y hora en escena que se preconiza incluye un panel de autenticación que contendrá, al menos, un área de código donde será mostrado el resultado de encriptar la fecha y la hora mediante una relación entre el código de cada bit o conjunto de bits con un determinado grupo de LEDs. La codificación para representar cada bit puede consistir en apagar o encender un LED asociado para representar un cero o un uno. Sin embargo, se prefiere la codificación en colores distintos para garantizar que, en caso de mal funcionamiento de un grupo de LEDs, pueda ser detectado el fallo y no se asocie con código alguno. Las dimensiones del área de código dependerán de la longitud del mismo y del tamaño de LED asociado a cada bit, debiendo ocupar éste tamaño un mínimo de 8 píxels en la imagen digitalizada. Además del área de código el panel contendrá un área de información de usuario (3), que puede destinarse tanto a la información de individuos o vehículos que transiten por la escena bajo vigilancia, como a publicidad.

La parte visible del panel se completa con unas marcas situadas en zonas concretas del panel, denominadas marcas de referencia (4), y que estarán iluminadas de forma que sean fácilmente identificables por un sistema de visión artificial. Dado que las cámaras destinadas a video vigilancia o monitorización del tráfico pueden tener fuertes oscilaciones, es importante poder identificar en cada momento en qué lugar de la imagen se encuentra el panel. Mediante estas marcas de posicionamiento se facilita la labor de localización del panel y su interpretación posterior para contrastar la información codificada.

Respecto al algoritmo de encriptación de la fecha y de la hora puede ser tanto simétrico, en cuyo caso el servidor de autenticación (9) debe conocer la clave de cada panel, como asimétrico, en cuyo caso el servidor solo contendrá la clave pública del panel, siendo la clave privada solo conocida al programar el panel. La mínima longitud de clave propuesta es de 32 bits para garantizar que no pueda ser rota la seguridad y manipular una escena con los códigos correspondientes a otra fecha. El intervalo de cambio de mensaje de cifrado puede ser programado, con un intervalo mínimo de un minuto y un intervalo máximo de diez minutos.

Como medida de seguridad adicional se puede incorporar una célula de proximidad que detecte cuando un objeto está en el entorno del panel, de manera que cuando se produzca esta situación, se codifica la fecha y la hora utilizando una clave alternativa. Esta funcionalidad permite relacionar la información proporcionada por el panel con parte de la acción que está sucediendo en la escena, siendo fácilmente comprobable esta situación por un algoritmo de visión artificial.

Adicionalmente, el sistema de control del panel puede tener un módulo de comunicación con el servidor de autenticación, de forma que puedan intercambiar información. Dado que las posibles aplicaciones del equipo propuesto condicionan que los mismos puedan localizarse en sitios donde no exista cableado, este módulo debe estar basado en la transmisión de mensajes por tecnología móvil (GSM, GPRS o UMTS). En este sentido, es posible establecer un protocolo de comunicaciones para el cambio consensuado de clave cada cierto tiempo, de manera que las claves son

dinámicas, resultando más difícil la encriptación. Además, este módulo de comunicaciones puede ser utilizado para notificar situaciones de alerta como la detección de un LED fundido, batería baja o un posible intento de saboteo del panel.

Para asegurar el sincronismo de fecha y hora, y que no se produzcan errores de autenticación debidos a un desajuste de estos datos, se contempla un receptor de señal RDS a partir del cuál se pueden obtener los datos de fecha y hora y compararlos con los del propio sistema para corregir los desajustes.

La alimentación del panel se realizará de forma preferente pero no limitativa mediante un sistema de placa solar, regulador de carga y batería de acumulación. La potencia a considerar debe contar con la potencia requerida por los paneles LED (código, información y marcas de referencia), el sistema de comunicación, el receptor RDS y el sistema de control global.

DESCRIPCIÓN DE LAS FIGURAS

Para completar la descripción de la invención y con objeto de ayudar a una mejor comprensión de las características del invento, se acompaña como parte integrante de dicha descripción, con carácter ilustrativo y no limitativo, un juego único de esquemas donde se ha representado un panel de autenticación (1) con sus diferentes elementos, la cámara (8) de captación de la escena y un servidor donde se ejecutará el software (9). La disposición de los elementos no obedece a escala alguna, pudiendo estar el servidor en cualquier localización remota.

MODO DE REALIZACIÓN

Atendiendo a la descripción aportada y la Figura 1 que se adjunta se detalla una realización donde el panel de LEDs está empotrado en una carcasa galvanizada. El panel deberá iluminar cuatro marcas de referencia en color rojo para la correcta situación por parte de los algoritmos de visión artificial del software. El código es encriptado mediante un algoritmo de encriptación simétrica AES (Advanced Encryption Standard) y en concreto en su modalidad Rijndael con un bloque de cifrado de 128 bits.

La clave simétrica se almacena en memoria EEPROM del sistema del control del panel y se comunica al servidor central de control de ese panel para la posterior desencriptación del código por parte del software de procesado. El tamaño del panel se diseña para que, una vez calibrada la cámara, cada bit ocupe en la imagen al menos 8 píxels de forma que pueda ser identificado sin problemas el código. Los LEDs correspondientes a 0 y 1 se realizarán en colores diferentes al negro y rojo para evitar la confusión al fundirse una zona de LEDs y no dificultar la búsqueda de marcas de referencia por parte del algoritmo de visión artificial.

El panel se complementa con un mástil también galvanizado donde irá alojada la placa microcontroladora que se encargará de leer la fecha y hora de un dispositivo RDS cada dos minutos, encriptará la información de acuerdo con la clave almacenada y actuará sobre cada conjunto de LEDs asociados a los códigos 0 ó 1 de los bits que comprenden el mensaje cifrado.

La alimentación es obtenida mediante un sistema compuesto por una batería, una placa solar con acumulador de tensión y un equipo de regulación de carga inteligente, de manera que cuando se detecta que la alimentación solar acumulada es insuficiente se alimentará el panel mediante la batería descrita.

El servidor en el que se procederá a la autenticación de la fecha y hora está dotado de una memoria RAM de 2 Gb, memoria en disco duro de 160 Gb y tarjeta gráfica entre otros elementos. En este servidor se ejecutan los algoritmos de visión artificial para localizar el panel en la imagen mediante las marcas de referencia, leer el código encriptado a partir de los LEDs y, conociendo la clave simétrica, desencriptar el mismo para poder comprobar que la fecha y hora asociadas con la video secuencia se corresponden con la información que se quiere autenticar.

BIBLIOGRAFÍA

[1] F. Liu, H. Koenig, "A survey of video encryption algorithms", Computers & Security, 29, 1, 3-15, 2010.

[2] Q. Sun; D. He; Q. Tian; , "A Secure and Robust Authentication Scheme for Video Transcoding," *IEEE Transactions on Circuits and Systems for Video Technology,* 16, 10, 1232-1244, 2006.

[3] M. Barni, F. Bartolini, A. Piva, "Digital watermarking for the authentication of AVS data", *Proceeedings of the EUSIPCO 2000*, Tampere, Finland, 2000.

[4] X. Li, Y. Shoshar, A. Fish, G. Jullien, O. Yadid, "Hardware Implementations of video watermarking", *Proceedings of the VI Conference on Information Research and Applications*, Varna, Bulgaria, 2008.

[5] P. Su; C. Chen; H. Chang, "Towards Effective Content Authentication for Digital Videos by Employing Feature Extraction and Quantization," *IEEE Transactions on Circuits and Systems for Video Technology,* , 19, 5, 668-677, 2009.

[6] M. Vatsa, R. Singh, S. K. Singh, S. Upadhyay, "Video Authentication Using Relative Correlation Information and SVM", en Computational Intelligence in Multimedia Processing: Recent Advances, 511- 529, Springer, 2008.

REIVINDICACIONES

1- Equipo de autenticación de fecha y hora para vídeo escenas que se caracteriza porque comprende:

a) un panel (1) de LEDs que muestran un mensaje encriptado con la información de la fecha y la hora almacenados en el sistema mediante un código de encriptación. Dicho panel comprende también de una placa microcontroladora (5) que almacena el código de encriptación, ejecuta el algoritmo de encriptación y se encarga de activar las salidas pertinentes para que el panel pueda reflejar dicha información. El panel estará alimentado por red eléctrica o batería autónoma (7).

b) Una cámara fija incorporada en el sistema de video vigilancia (8) que se quiere autenticar y que vigilará la escena incluyendo en todo momento el panel descrito anteriormente y

c) el software necesario para autenticar en una vídeo secuencia grabada que la fecha y la hora referidas son las que corresponden a la decodificación de la fecha y hora a partir del código de LEDs leído. Este software estará alojado en un servidor central (9).

2- Equipo de autenticación de fecha y hora para vídeo escenas, según reivindicación 1, caracterizado porque el panel de LEDs incorpora unas marcas de referencia (4) con el objeto de facilitar su localización en el tratamiento de imagen que lleva a cabo el software de autenticación.

3- Equipo de autenticación de fecha y hora para vídeo escenas, según reivindicación 1, caracterizado por la correspondencia entre 0 y 1 para los distintos bits encriptados con zonas de LEDs de colores diferentes al negro, de forma que el software pueda proporcionar información a posteriori sobre zonas fundidas y actuar en consecuencia para la lectura del código.

4- Equipo de autenticación de fecha y hora para vídeo escenas, según reivindicación 1, caracterizado por estar dotado de un dispositivo de transmisión

de mensajes por tecnología móvil (GSM, GPRS o UMTS) para el intercambio de información con el servidor central.

5- Equipo de autenticación de fecha y hora para vídeo escenas, según reivindicación 1, caracterizado por estar dotado de un receptor RDS en el panel para que proporcione información a la placa microcontroladora y pueda sincronizar la fecha y la hora conforme a las necesidades recibidas.

6- Equipo de autenticación de fecha y hora para vídeo escenas, según reivindicación 1, caracterizado por estar alimentado mediante una placa de energía solar (6) con acumulación y sistema de conmutación inteligente a batería autónoma cuando la energía acumulada no sea suficiente.

7- Equipo de autenticación de fecha y hora para vídeo escenas, según reivindicación 1, caracterizado por estar dotado de una célula de proximidad y dos códigos de encriptación de forma que el mensaje encriptado de fecha y hora sea diferente en presencia de un objeto o de un sujeto cercano al panel que en ausencia del mismo.

8- Equipo de autenticación de fecha y hora para vídeo escenas, según reivindicación 1, caracterizado por estar dotado de un espacio adicional donde puedan reflejarse mensajes a los individuos presentes en la escena (3).

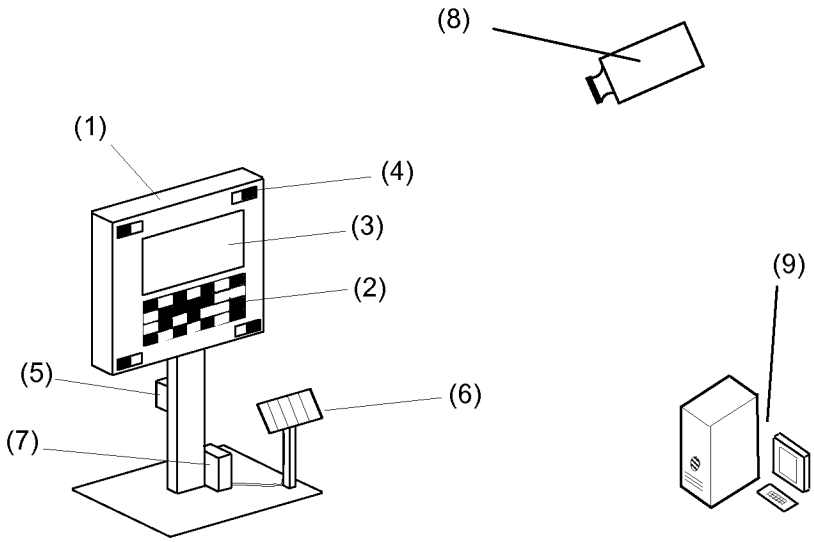

Figura 1

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201031412

(22) Fecha de presentación de la solicitud: 23.09.2010

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04L9/32*** (2006.01)
H04L9/08 (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) Documentos citados	Reivindicaciones afectadas
A	US 2009319769 A1 (BETOUIN PIERRE et al.) 24.12.2009	1
A	JP 2007150963 A (VICTOR COMPANY OF JAPAN) 14.06.2007	1
A	WO 03071737 A1 (MEASURECAST COM INC) 28.08.2003	1
A	WO 0141360 A2 (EORIGINAL INC et al.) 07.06.2001	1

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
29.11.2012	M. C. González Vasserot	1/4

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04L

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI

Fecha de Realización de la Opinión Escrita: 29.11.2012

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-8	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones	1-8	**SI**
	Reivindicaciones		**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	US 2009319769 A1 (BETOUIN PIERRE et al.)	24.12.2009
D02	JP 2007150963 A (VICTOR COMPANY OF JAPAN)	14.06.2007
D03	WO 03071737 A1 (MEASURECAST COM INC)	28.08.2003
D04	WO 0141360 A2 (EORIGINAL INC et al.)	07.06.2001

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

Los documentos citados solo muestran el estado general de la técnica, y no se consideran de particular relevancia. Así, la invención reivindicada se considera que cumple los requisitos de novedad, actividad inventiva y aplicación industrial.

1.- El objeto de la presente solicitud de patente consiste en un equipo que consta de un panel de autenticación que mostrará en un área de código la fecha y la hora encriptadas consistiendo la representación de dicho código en la iluminación por medio de diferentes colores de una serie de LEDs o panel de LEDs. El panel también puede contener un área de información al usuario destinado a mostrar mensajes o imágenes que no tiene por qué estar relacionada con la aplicación. El panel mostrará también unas marcas de referencia necesarias para localizar dicho panel en un sistema de análisis de las secuencias cuando la cámara tiene cierto movimiento debido a oscilaciones físicas. El sistema de control del panel estará encargado de obtener la fecha y la hora, sincronizarlas, almacenar las claves criptográficas, ejecutar el algoritmo de encriptación, además de controlar posibles funciones adicionales de monitorización del propio panel y de la alimentación recibida, así como de controlar la comunicación con el servidor de análisis. La energía necesaria para alimentar el panel puede ser obtenida mediante una placa solar conectada a un sistema de regulación de carga inteligente y de acumulación de batería, contemplando también la posibilidad de utilizar una batería simple. La escena vigilada, en la que se incluye el panel de autenticación, es captada por una cámara y digitalizada junto con la información de fecha y hora proporcionada por la cámara, de forma que la información se envía a un servidor con los algoritmos necesarios para localizar el panel de autenticación en la imagen, leer correctamente el código reflejado en la escena real y desencriptarlo para verificar que la fecha y hora de la escena reales coinciden con la información proporcionada junto con la secuencia de vídeo.

2.- El problema planteado por el solicitante es la autenticación de los sistemas de video vigilancia que comprende el proceso de preservar la integridad del vídeo original así como los datos asociados de la escena. Este proceso, en el que se asegura que las imágenes no han sido manipuladas, tiene especial importancia para la presentación de secuencias de vídeo como una evidencia en procesos penales o en auditorías. Además de la preservación del contenido es importante validar la fecha y la hora asociadas a la secuencia considerada. Sin embargo, al auditar las escenas, además de verificar que no han sido manipuladas, se debe asegurar que la fecha y la hora corresponden con la realidad y que la secuencia no corresponde con lo sucedido en otra franja de tiempo. Si bien este problema puede ser resuelto mediante la encriptación de esos datos en la secuencia de vídeo, esto requiere tener cámaras que sean capaces de realizar tal encriptación, por lo que se haría necesario sustituir todo el sistema de video vigilancia.

El documento D1 puede considerarse como el representante del estado de la técnica más cercano ya que en este documento confluyen la mayoría de las características técnicas reivindicadas.

Análisis de la reivindicación independiente 1

D1 se diferencia del documento de solicitud de patente en que el equipo de autenticación de fecha y hora para vídeo escenas no comprende un panel de LEDs que muestre un mensaje encriptado con la información de la fecha y la hora almacenados en el sistema mediante un código de encriptación.

La reivindicación 1 es nueva (Art. 6.1 LP 11/1986) y tiene actividad inventiva (Art. 8.1 LP11/1986).

Análisis del resto de los documentos

De este modo, ni el documento D1, ni ninguno del resto de los documentos citados en el Informe del Estado de la Técnica, tomados solos o en combinación, revelan la invención en estudio tal y como es definida en las reivindicaciones independientes, de modo que los documentos citados solo muestran el estado general de la técnica, y no se consideran de particular relevancia. Además, en los documentos citados no hay sugerencias que dirijan al experto en la materia a una combinación que pudiera hacer evidente la invención definida por estas reivindicaciones y no se considera obvio para una persona experta en la materia aplicar las características incluidas en los documentos citados y llegar a la invención como se revela en la misma.