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).