Diseño e implementación de un sistema de detección e identificación de aficionados violentos en estadios de futbol

Design and implementation of a system for detection and identification in violent amateur soccer stadiums

Ing. Miguel Nieto García*

M.C. René E. Cuevas Valencia**

M.C. José M. Martínez Castro***

Fecha de recepción: 2 de abril de 2013
Fecha de aceptación: 5 de mayo de 2013

Resumen

En este documento, se describe el proceso de diseño e implementación de un sistema avocado a la detección e identificación de aficionados violentos en estadios de futbol. Misma que describe la necesidad de implementar este tipo de tecnología en sectores concurridos, se pretende establecer un sistema que al ser combinado con diversas herramientas tecnológicas, permita tener el más completo sistema de identificador de rostros aplicado en estadios de futbol.

Palabras clave: Control de paso, autentificación biométrica, CCTV, huella digital, sistema, aficionado, violencia.

* Universidad Autónoma de Guerrero. Unidad Académica de Ingeniería. Av. Lázaro Cárdenas S/N, CU. Correo electrónico: mikael_blue@hotmail.com

** Universidad Autónoma de Guerrero. Unidad Académica de Ingeniería. Av. Lázaro Cárdenas S/N, CU. Correo electrónico: reneecuevas@gmail.com

*** Universidad Autónoma de Guerrero. Unidad Académica de Ingeniería. Av. Lázaro Cárdenas S/N, CU. Correo electrónico: jmmtzc@gmail.com

Abstract

In this paper, we describe the design process and implementation of an avocado system to detect and identify hooligans in football stadiums. Same describing the need to implement this technology in crowded areas, is to establish a system that when combined with various technology tools, allows to have the most complete system identifier applied faces football stadiums.

Key words: Pitch control, authentication, biometrics, CCTV, fingerprint, system fan, violence.

1. Introducción

El sistema de detección e identificación de aficionados violentos en estadios de futbol representa un salto hacia la modernización de la experiencia de asistir a los espectáculos deportivos en nuestro país. A través de la implementación de herramientas digitales y biométricas, los clubes de futbol podrán acceder a un mayor control de la organización de los eventos. Al mismo tiempo los organismos correspondientes del Estado tendrán una herramienta adicional para garantizar mayor seguridad dentro de los estadios.

2. Delimitación

2.1. Justificación

Muy pocos acontecimientos hoy en día tienen la cualidad de generar tanta ilusión como lo hace el fútbol. Lamentablemente, en ocasiones esto se ve manchado por la violencia en las tribunas, generada entre porras rivales o entre los mismos fans de un club.

En México no somos ajenos a estos problemas, lamentable sólo en muy pocos estadios sean tomadas las medidas necesarias para frenar estos tipos acontecimientos mientras que en la gran mayoría de los inmuebles no cuentan con los medios para evitar, detectar y castigar a quienes provocan estos hechos.

Es por ello que surge la necesidad de la planificación de un buen sistema de seguridad teniendo como prioridades la prevención, detección e identificación de cualquier sujeto sospechoso de querer participar en actos de violencia.

2.2. Alcances

Se pretende desarrollar un sistema de detección e identificación de aficionados involucrados en actos violentos en los estadios de futbol apoyándose en la tecnología existente de vigilancia por video, biométrica y de control de paso.

El sistema debe ser capaz de utilizar la información generada por el sistema de vigilancia de video, de registrar la información de los aficionados detenidos por actos violentos y de identificar a un aficionado registrado como violento de uno que no lo está en los accesos al estadio.

2.3. Objetivo General

Desarrollar un sistema de que permita la detección e identificación de fanáticos violentos

utilizando un sistema CCTV, autentificación biométrica y control de paso.

2.4. Objetivos Específicos

- Analizar 3 sistemas CCTV o video vigilancia
- Analizar 3 sistemas de control paso
- Analizar 3 sistemas de autentificación biométrica
- Diseñar la base de datos para el sistema de detección e identificación
- Diseñar el sistema de detección e identificación
- Programar el sistema de detección e identificación
- Implementación de una aplicación piloto del sistema de detección e identificación.

3. Marco teórico

3.1. Descripción

La seguridad cada vez es más necesaria en nuestra vida cotidiana. En lugares y ocasiones en que se da una concentración numerosa de personas, esta seguridad se ve amenazada. Es el caso de los estadios y canchas de deporte.

Algunos de los problemas identificados son, por ejemplo:

- Las gradas de los estadios son frecuentemente escenarios de acciones violentas, que además a menudo se penalizan imponiendo multas a los clubes.
- Los sistemas de reventa y la falsificación de boletos hacen fácil burlar los sistemas de seguridad.
- Ciertos usuarios pueden obtener sin control alguno un número elevado de abonos que obstaculizan el acceso de nuevos socios y que son utilizados para otros propósitos comerciales ajenos al club.

La FIFA, las Federaciones Nacionales y los Clubes piden soluciones a la violencia en los estadios.

Los clubs deportivos además, intentan aportar cada vez más una imagen innovadora, prestar los máximos servicios al cliente y velar por su comodidad y satisfacción.

Con este panorama, la tecnología juega un papel fundamental, siendo capaz de aportar una gestión ordenada y al mismo tiempo dar un grado de innovación que atrae al cliente.

Sin embargo, muchas veces, el uso de dicha tecnología implica dotar al usuario de elementos físicos que son necesarios para dichas funcionalidades.

A continuación se describen generalidades de la tecnología que utilizará el sistema de detección e identificación de fanáticos violentos.

3.1.1. CCTV y Sistemas de Video vigilancia

El Circuito Cerrado de Televisión o su acrónimo CCTV, que viene del inglés: Closed Circuit Television, es una tecnología de vídeo vigilancia visual diseñada para supervisar una diversidad de ambientes y actividades.

Se le denomina circuito cerrado ya que, al contrario de lo que pasa con la difusión, todos sus componentes están enlazados. Además, a diferencia de la televisión convencional, este es un sistema pensado para un número limitado de espectadores.

El circuito puede estar compuesto, simplemente, por una o más cámaras de vigilancia conectadas a uno o más monitores o televisores, que reproducen las imágenes capturadas por las cámaras. Aunque, para mejorar el sis-

tema, se suelen conectar directamente o enlazar por red otros componentes como vídeos u ordenadores.

En un sistema moderno las cámaras que se utilizan pueden estar controladas remotamente desde una sala de control, donde se puede configurar su panorámica, inclinación y zoom.

Estos sistemas incluyen visión nocturna, operaciones asistidas por ordenador y detección de movimiento, que facilita al sistema ponerse en estado de alerta cuando algo se mueve delante de las cámaras. La claridad de las imágenes debe ser excelente, ya que se puede transformar de niveles oscuros a claros.

3.1.2. Torniquetes y tornos de control de paso

Los torniquetes o tornos son una de las fórmulas más efectivas para realizar un Control de Paso de personas. Combinando la tecnología para la identificación y el control de accesos conjuntamente con los tornos y torniquetes, permitirá tener el control total para la gestión de personas en un recinto.

El control de paso se ha convertido, con el tiempo, en una necesidad para muchos recintos. Actualmente, los torniquetes se han vuelto muy interesantes para conocer la cantidad de personas que hay en cualquier edificio ante una situación de emergencia en la cual se deba dar información crítica e instrucciones a los bomberos o a las fuerzas de seguridad del estado.

3.1.3. Biometría

Hoy en día, la mayoría de los sistemas de control de acceso a los estadios están basados en "algo que se tiene" (tarjeta, entrada, abonos). De este modo se pierde la garantía en las autorizaciones de acceso. (Todos ellos son susceptibles de copia, robo, etc).

Las tecnologías biométricas proporcionan un elemento nuevo ("algo que soy") que evita este tipo de brechas, aportando además movilidad, innovación, ergonomía, seguridad y constituyendo una herramienta básica de autentificación.

La palabra biometría deriva del griego: bios que significa "vida" y metron cuyo significado es "medida". Por lo que, literalmente la palabra viene a traducirse como "medida de vida" La biometría se basa en la premisa de que cada individuo es único y posee rasgos físicos distintivos (rostro, huellas dactilares, iris de los ojos, etc.) o patrones de comportamiento (la voz, la manera de firmar o de caminar etc.), que pueden ser utilizados para su identificación inequívoca.

Por lo que, podemos definir la biometría como el conjunto de métodos automatizados de autenticación (identificación y verificación) de la identidad de una persona, basados en una característica fisiológica o de comportamiento.

Los dispositivos biométricos son capaces de capturar características de un individuo (como el rostro, huella dactilar, voz, forma de caminar o firmar), compararlas electrónicamente contra una población de una o más de estas características y actuar según el resultado de la comparación.

El campo de aplicación de la biometría es realmente extenso, aunque el escenario principal, sin duda alguna, es la identificación. Entre las posibles aplicaciones de identificación biométrica se pueden citar las siguientes: el control de acceso, el control de presencia, el acceso biométrico para aplicaciones de

software, el acceso a sistemas operativos, el pago de compras, el acceso a teléfono móviles, o cualquier otra aplicación que sustituya su identificación tradicional por la incorporación de un lector biométrico que capture una característica biométrica cualquiera.

Características Biométricas: existen numerosas características biológicas del sujeto que pueden ser medidas, pero no todas ellas pueden ser utilizadas para la biometría. Cualquier particularidad humana, física o de comportamiento, puede ser utilizada para este propósito si cumple las siguientes características:

- Universalidad: todos los individuos deben poseer la característica.
- Particularidad: dos sujetos cualesquiera deben poder ser diferenciados con dicha característica.
- Permanencia: la característica debe ser suficientemente invariable durante un periodo de tiempo.
- Coleccionabilidad: la característica debe ser medible cuantitativamente.
- Rendimiento: relativo a la precisión y a la velocidad de ejecución, así como a los recursos necesarios para conseguir dicha precisión.
- Aceptabilidad: que indica la aceptación de la población sobre el uso de esta característica durante su vida diaria.
- Evasión: que indica la posibilidad de engañar el sistema usando métodos fraudulentos.

Por tanto, una particularidad física del individuo que recoge todas estas características y puede ser utilizada en la biometría es la huella dactilar.

Para darle un tratamiento eficiente y seguro a la huella digital es necesario contar con un sensor para esta importantísima tarea. El sensor realiza una imagen en 3D, se extraen 651 minucias o puntos de reconocimiento y se establece un algoritmo identificativo a través de las minucias que almacena en formato PKI (Public Key Infrastructure). Esa estructura es la que garantiza que el usuario es quien dice ser.

Los tiempos de reconocimiento son inferiores a un segundo, lo que garantiza la eficiencia y mejora en los rendimientos de los accesos.

En los puntos de acceso se puede implementar dos modos de autenticación:

- Identificación 1:N (solo huella): la huella capturada es comparada con la Base de datos del Terminal 1:N (uno/muchos). Dependiendo del tipo de sensor instalado, este puede almacenar 3000 usuarios (2 huellas por usuario) en su memoria local o 50 000 usuarios dividido en 5 bases de datos de 10 000 usuarios cada una. (Usuarios por torno/molinete).
- Verificación 1:1 (Tarjeta más huella): la huella capturada es comparada contra una huella de referencia 1:1 (uno/uno).

Las minucias del usuario se almacenan en la BBDD local del dispositivo. En este caso el identificador del usuario es utilizado como una clave para encontrar las minucias. El identificador del usuario puede ser enviado vía tecleado o almacenado en una tarjeta de contacto.

Los beneficios del uso de dispositivos biométricos son:

- Seguridad: los sensores biométricos tienen una Tasa de Falsa Aceptación (FAR) muy baja a diferencia de los medios físicos tradicionales. La estructura de los algoritmos obtenidos en el reconocimiento dactilar PKI (Public Key Infraestrucutre) garantiza la seguridad y tratamiento en las identificaciones.

  - Niega el acceso a personas no admitidas por violencia.
  - Facilita la identificación de los individuos aún cuando carezcan de documentación.
  - Identifica a menores en caso de pérdida, etc.
  - Determina los accesos autorizados de prensa, empleados o subcontratados
- Innovación: la apuesta por el reconocimiento dactilar garantiza la innovación. El uso de una herramienta de este tipo complementará una imagen renovada y actual al asociar la imagen de un elemento tan tecnológico y vanguardista como la huella digital con la institución en cuestión.
- Movilidad: el reconocimiento dactilar aporta una gran movilidad. Ya no son necesarios elementos físicos que pueden perderse, copiarse, desprogramarse o ser robados, dado que los usuarios se identifican por "lo que son". Para los propios usuarios es un sistema más rápido y cómodo, que sin duda agradecen.
- Ergonomía: todos los sensores están adaptados para un fácil posicionamiento del dedo. Además permiten la lectura en diferentes ángulos. Los tiempos de reconocimiento inferiores a un segundo garantizan un acceso fluido, muy superior a los ratios de otras tecnologías.
- Fidelización: gracias al tratamiento del PKI se puede fidelizar y establecer una política Customer Relationship Management (CRM) con los clientes. Así, un usuario que no es socio, pero que habitualmente compra entradas, puede recibir personalizaciones de servicios (oferta de abonado, merchandasing, servicios Web…). En cuanto al socio, puede identificarse en la web para promociones o acceso a cuentas personales, identificarse en eventos, votar, etc.

Una vez desarrollado un sistema biométrico válido, obtendremos numerosas mejoras aplicables a sistemas tradicionales, como por ejemplo en los controles de acceso, controles de presencia, o de pagos.

3.1.4. Sistema centralizado

Un sistema centralizado se compone de una base de datos centralizada, donde se hallan todos los registros de los usuarios (por un lado sus datos identificativos y por otro, el algoritmo obtenido por el reconocimiento biométrico) y donde se establecen los derechos del usuario (Club, si es socio, abonado, entrada, puerta, apto, no apto…).

El sistema central está conectado al centro de registro que es la estación donde se realiza la captura del rasgo biométrico (huella dactilar, palma, etc). Una vez obtenidos los datos, el sistema central distribuye los privilegios y el rasgo biométrico a los dispositivos biométricos de las puertas de acceso a través del servidor local del inmueble.

3.2. Hipótesis

Con la implementación del sistema de detección e identificación de aficionados violentos se pretende detectar a las personas involucradas en los brotes de violencia en las tribunas del estadio, reduciendo en un alto porcentaje el número de incidentes de violencia haciendo del inmueble un lugar más seguro para todos los asistentes.

4. Antecedentes y similitudes del sistema en el mundo

4.1. Torneo Chileno

El sistema de control de acceso móvil, impulsado por Plan Estadio Seguro para los partidos de alta convocatoria, se trata de un

moderno sistema donde los fanáticos deberán mostrar su carnet en cada acceso antes de ingresar al recinto, y donde mediante el chequeo digital, la organización verificará los antecedentes de cada hincha, confirmará exactamente el aforo del estadio para esa fecha determinada y detectará alguna medida cautelar que tenga pendiente algún espectador, impidiéndole ingresar al estadio.

En el marco de la implementación tecnológica del Plan Estadio Seguro, el sistema de control móvil se ha ejecutado en varias regiones de Chile siendo el estadio La Portada uno de los primeros en poner en marcha el sistema.

4.2. Torneo Argentino

En argentina se ha comenzado a realizar las pruebas de funcionalidad del Sistema Inteligente de Admisión Biométrica (SIAB) en los estadios de Independiente Rivadavia de Mendoza y de Rosario Central.

Este sistema está basado en la utilización de la huella dactilar como credencial de identificación. Para cada persona se genera un registro único de identificación. Bajo esta modalidad el sistema puede vender entradas en estaciones remotas, vía telefónica y vía Internet de cualquier evento en cualquier parte del país sudamericano.

Cada entradas vendida pertenece a una huella dactilar única, que el cliente usará para ser admitido en el estadio correspondiente.

4.3. Real Madrid

En 2009, modernizó sus accesos al estadio Santiago Bernabéu con la tecnología biométrica, contratando a la empresa Xelios Biometrics.

4.4. Torneo Italiano

En 2010 se implementó el llamado "tessera del tifoso", una medida implementada desde el Ministerio del Interior, cuyo principal objetivo es impedir el ingreso a los estadios de los simpatizantes violentos. En ese sentido, el sistema a crear incorpora el concepto de torniquetes electrónicos accionados por análisis biométrico.

4.5. Eurocopa 2012

El estadio de fútbol Donbass Arena de Ucrania, con capacidad para más de 51.000 espectadores sentados, es el primero de Europa Oriental que cumple con los criterios fijados por la UEFA para ser un estadio de élite, lo que contribuyo a su designación como sede de la semifinal del Campeonato Europeo de Fútbol 2012.

Inaugurado en 2009 y propiedad del FC Shakhtar Donetsk, se trata de una moderna y vanguardista instalación , que no sólo están disponibles para el deporte, sino también para otros grandes acontecimientos como conciertos o eventos de diverso tipo que se celebran en el estadio.

EL sistema de video vigilancia del estadio se compone de 528 cámaras del fabricante alemán Mobotix, a las que se suman 58 cámaras PTZ de Bosch PTZ para lograr una cobertura completa del Donbass Arena.

Para contribuir y garantizar la seguridad en el estadio, la instalación de vídeo, en alta resolución, cumple con los siguientes requisitos: por una parte, debe permitir la identificación de todas las personas en el momento de entrada, permanencia y salida del estadio; por otro, sirve para vigilar y controlar la afluencia de visitantes en los puntos más estratégicos de la instalación, como las entradas y las

salidas, los accesos a la tribuna o el parque que lo rodea.

Además en los accesos al estadio se instalaron dispositivos biométricos para controlar el flujo de personas que entran al inmueble.

Aparte del estadio de Donestk, también el de Kharkiv, en Ucrania, y Wroclaw y Varsovia, en Polonia, instalaron la tecnología biométrica en sus accesos.

4.6. Mundial Brasil 2014

Se encuentra en proceso de instalación el sistema biométrico en los aeropuertos más importantes del país. Además, se prevé que el ingreso a los estadios se realice con la ayuda de un sistema de biometría, con el que a través de las huellas dactilares se podrá verificar al instante los antecedentes de la persona. En cuanto al almacenamiento de los datos se utilizará un sistema basado en la nube.

5. Conclusiones

No existe ninguna probabilidad de solucionar la violencia en el fútbol en su totalidad aplicando solo sistemas inmensos y costosos o de impacto directo en el medio.

Ninguna tecnología por más avanzada que sea tendrá éxito sin un cambio radical en la forma de recibir, alojar y atender a un espectador dentro de un estadio de fútbol.

Por lo tanto el sistema de detección e identificación de aficionados violentos en un estadio de futbol es una propuesta de aplicación que utiliza la tecnología como herramienta con la finalidad de que los clubes de futbol tengan un mayor control de la organización de los eventos efectuados en su inmueble, es decir, mediante la parte de CCTV del sistema se detecta los brotes de violencia en las tribunas; una vez detenidos los responsables, se registran con la finalidad de que en eventos posteriores, con la parte de control de acceso del sistema, se niegue el paso a dichos individuos.

Además se pone a disposición de los organismos correspondientes de gobierno la información respectiva de los responsables de los disturbios para que se tomen las acciones pertinentes de acuerdo sea el caso.

En otras palabras el sistema de detección e identificación de aficionados violentos en estadios de futbol se convierte en una herramienta adicional para garantizar mayor seguridad dentro de los estadios.

6. Referencias

[1] Mobotix AG, 2012. *Donbass Arena Modern Video System Provides Security At A UEFA-Certified Stadium In Donetsk (Ukraine).* (28 junio 2012). DOI= http://www.mobotix.com/es

[2] Accesor, 2012. *Productos de Accesos y cctv*. (27 junio 2012). DOI= http://www.accesor.com/.

[3] Umanick, 2012. *Tecnologías Biométricas.* (27 junio 2012). DOI= http://www.umanick.com/.

[4] Xelios Biometrics, 2012. *Proyecto ISIS International Soccer Identification System*. (30 junio 2012). DOI= http://www.xelios.es/