ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

CENTRO DE INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA

"Comercialización de Sistemas de Acceso Vehicular y Control Peatonal para las Ciudadelas Privadas, basadas en Sistemas Biométricos de Reconocimiento Facial."

Autores: Kerly Elizabeth Figueroa Peñafiel [(1)], Alan Erasmo Villacreses Pincay[(2)]
Coautor: Gustavo H. Galio Molina[(3)], Master en Sistemas de Información Gerencial, ESPOL.
Facultad de Ingeniería en Electricidad y Computación
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
kfiguero@espol.edu.ec [(1)], alervill@espol.edu.ec [(2)]
ggalio@espol.edu.ec [(3)] drggalio@hotmail.com [(3)]

Resumen

El objetivo de un sistema de acceso vehicular y control peatonal en una ciudadela privada, es asegurar que solo personal autorizado pueda tener acceso a la misma, aportando mayor seguridad a sus habitantes. La utilización de dispositivos biométricos, presentan una gran ventaja frente a otras tecnologías (códigos de acceso, tarjetas magnéticas, llaves, etc.) ya que utilizan características únicas, irrepetibles e intransferibles de cada individuo, con el fin de identificar y comprobar la identidad de cada persona que desee obtener el acceso, estos métodos de identificación están siendo utilizados a nivel mundial, por muchas entidades preocupadas por la seguridad de sus lugares de residencia y empresas. Se propone un sistema biométrico de reconocimiento facial, el cual permitirá reforzar la seguridad de estos lugares dando soporte tecnológico necesario al personal encargado de la guardianía y permitiéndoles ser más eficientes en sus labores diarias.

Utilizando el internet como medio principal de comunicación se pretende llegar a nuestro sector objetivo, como son ciudadelas privadas de la ciudad, la promoción se realizará mediante redes sociales y la comercialización a través de plataformas e-commerce, de esa forma se mantendremos informados a los usuarios de las ventajas y beneficios de la solución propuesta.

Palabras Claves: *Sistemas biométricos, reconocimiento facial, seguridad biométrica.*

Abstract

The objective of a system of vehicular and pedestrian control at a private citadel is to ensure that only authorized personnel have access to the same, providing greater security for their inhabitants. The use of biometric devices, have a great advantage over other technologies (access codes, magnetic cards, keys, etc.) As they use unique , unrepeatable and untransferable to each individual , in order to identify and verify the identity of each person seeking access these identification methods are being used worldwide by many organizations concerned for the safety of their homes and businesses . We propose a face recognition biometric system, which will strengthen the security of these places providing technological support personnel who need guardianship and allowing them to be more efficient in their daily work.

Using the internet as a primary means of communication is to reach our target sector, such as private citadels of the city, the promotion will be done through social networking and marketing through e- commerce platform, that way you keep informed users of the advantages and benefits of the proposed solution.

Keywords: *biometric systems, facial recognition, biometric security.*

1. Introducción

Los sistemas biométricos se basan en las características físicas de una persona, como pueden ser sus huellas dactilares, rostro, voz, firma, etc. Los biométricos se constituyen como mecanismos de control de acceso seguros.
En nuestra sociedad, los niveles de inseguridad son elevados, y los controles que se realizan no son suficientes, con el fin de contrarrestar estos problemas y para cubrir las deficiencias de los controles de seguridad, se ha elaborado un sistema que restrinja el acceso a personas y vehículos no autorizados, evitando el robo o préstamo de identidad, permitiendo el fortalecimiento de la seguridad en todos los sectores, obteniendo la confianza de los usuarios finales. Seguridad Biométrica propone un sistema que controle de forma efectiva el acceso de personas y vehículos basado en sistemas biométricos de reconocimiento facial.

2. ¿Por qué utilizar dispositivos biométricos?

Los dispositivos biométricos utilizan uno o más rasgos conductuales de un ser humano con el fin de crear métodos de reconocimiento únicos de personas, se basan en características intransferibles e irrepetibles de cada individuo, no requiere contraseñas o credenciales de identificación. Los sistemas biométricos más utilizados actualmente son:

- Huella dactilar.
- Reconocimiento de voz.
- Reconocimiento de retina y el iris del ojo.
- Reconocimiento facial.
- Reconocimiento de los vasos sanguíneos de la mano o la geometría de la mano.

Entre las razones para usar sensores biométricos también está su simplicidad de uso, de implementación y de manejo, además ofrece mayor comodidad a los usuarios. También son sistemas poco intrusivos y que requieren de poco entrenamiento para su uso, motivos por los cuales han alcanzado un nivel de aceptación muy alto.

2.1. Sistemas Biométricos de Reconocimiento Facial

Los sistemas de reconocimiento facial se basan en una técnica de verificación de la identidad de una persona a partir de una imagen o fotografía. Se realizan varias fotografías del rostro y se enfocan diferentes ángulos para obtener más detalles para una adecuada identificación y para permitir una búsqueda de coincidencias más precisa.

3. Análisis de Mercado

Según un informe de investigación de mercado de International Biometric Group (IBG), se espera que el mercado de las tecnologías biométricas crezca de 3.4 billones en el 2009 a 9.3 billones de dólares en el 2014.

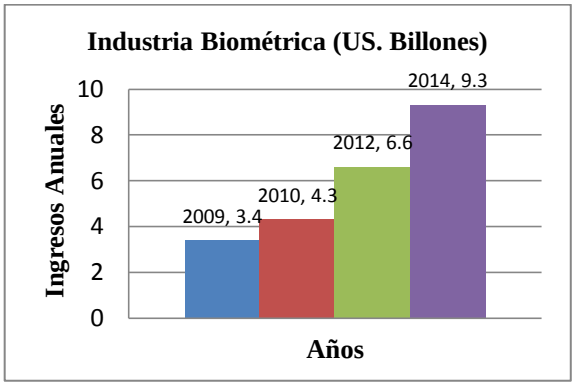

Figura 1. Cadena de Valor de un Sitio Web

Una vez obtenida la información necesaria para establecer la demanda del mercado y los objetivos de la empresa, se define al mercado primario como el grupo potencial que más acerca su perfil al de nuestros productos, siendo sus principales características, su ubicación en ciudadelas privadas, las cuales requieren fortalecer sus sistemas de seguridad actuales y mejorar el control de acceso de personas y vehículos.

Mercado Primario: Ciudadelas privadas de clase media y alta; y, empresas del país.

4. Cadena de Valor

Figura 2. Cadena de Valor de un Sitio Web

4.1. Actividades Primarias

4.1.1. Logística de Entrada. La empresa para funcionar, mantenerse y competir en el mercado, necesita de:

- Clientes potenciales, que estarían en las ciudadelas privadas y empresas con parqueo privado.
- Dispositivos Biométricos, necesarios para la implementación del sistema de control de acceso de personas y vehículos.

4.1.2. Operaciones. La empresa desarrollará el Sistema Biométrico de Reconocimiento Facial para control de acceso de peatones y de vehículos, de esta forma se logrará el aumento de las ganancias de la empresa, y se mejorará el nivel de satisfacción de los clientes, ya que se puede personalizar el sistema con las necesidades que ellos tengan, sin depender de terceros.

4.1.3. Marketing y Ventas. Para apoyar a las actividades de Marketing y Ventas, se ha implementado un Sitio Web, el cual permitirá obtener información de:

- La empresa.
- Productos que se ofertan.
- Promociones y eventos.
- Recordación de Marca.
- Pedidos en línea.

Esto con el fin de lograr captar clientes, y de crear la fidelización de los que clientes que poseemos.

4.1.4. Logística de Salida. Debido a que el producto es no perecible, pero son aparatos delicados para su transportación, estos deben ser correctamente embalados para evitar daños.

4.1.5. Servicio Post-Venta. Para mejorar la calidad del servicio se proporcionará a los clientes asistencia en:

- Soporte Técnico.
- Garantías por equipos vendidos.
- Cambios en el software por requerimientos adicionales de los usuarios.
- Mantenimiento preventivo y correctivo de los equipos.

5. Estrategias

Para conseguir que el producto se convierta en uno de los principales sistemas de seguridad biométricos en el país, nos apoyaremos las siguientes actividades:

- Implementar un sitio web en el que se levantará toda la información referente al producto.
- Realizar una estrategia comunicacional utilizando correos electrónicos masivos, con estándares IAB (Interactive Advertasing Boreu) para evitar ser considerado como correo no deseado, con el fin de que el cliente reciba el mail.
- Utilizar volantes para promocionar y fomentar el acceso al sitio web.
- Utilizar medios de comunicación gratuitos para la difusión del sistema, como son las redes sociales y YouTube, junto a estrategias de marketing viral.

6. Diseño General

El Sitio Web, www.seguridadbio.com, proporciona información sobre los productos que se comercializan, además permite crear un canal de comunicación entre la empresa y los interesados en nuestro catálogo de productos. El Sitio utiliza herramientas OScommerce y está desarrollado bajo PHP con base de datos MySQL. El servicio de alojamiento (Hosting) es proporcionado por GoDaddy.
La aplicación de reconocimiento facial está basada en .NET, dado que le dispositivo biométrico utilizado proporciona librerías que permiten el desarrollo en este lenguaje de programación, posee como base de datos MySQL, su implementación debe ser bajo el sistema operativo Windows.

7. Arquitectura

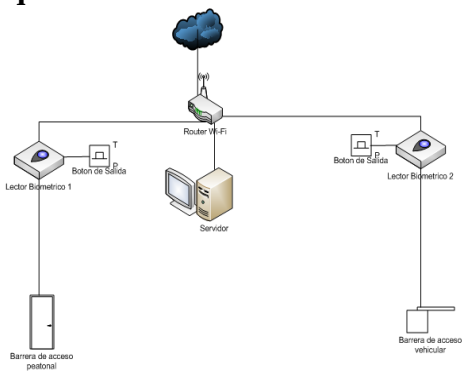

Figura 3. Arquitectura del sistema de reconocimiento facial

El sistema de control de acceso consta de dos tipos, el control vehicular y el peatonal, por lo tanto se deben controlar todas las entradas y salidas que posea el lugar, esto proveerá mayor seguridad ya que se

vigilará constantemente todos los accesos, se realiza el registro de todos las personas y vehículos que ingresan al lugar, con lo que se garantiza la eficiencia del sistema.

7.1. Características del Servidor

Tabla 1. Requerimientos Servidor

Requerimientos Generales	Microsoft Windows (32 bits o 64 bits) Procesador Intel Core i3 Windows XP o superior
Memoria RAM	4 GB
Disco Duro	500 GB (Sistema Operativo y Base de datos)
Disco Duro 2	500 GB (Respaldos)
Base de Datos	MySql
Monitor	LCD
Red	RouterWi-Fi Pachcord de 2 metros cable UTP Categoría 6A

7.2. Requerimientos para Punto de Control de Acceso

Tabla 2. Requerimientos Punto de Acceso

Biométrico	Reconocimiento Facial iFace300 o superior
Red	Cable UTP (variable dependiendo de la distancia al router)
Cerradura Eléctrica	Cualquier marca
Interruptor	Botón de Salida

El número de Puntos de Acceso puede variar dependiendo de cuantas entradas y salidas desee controlar

7.3. Otros requerimientos

- Tarjeta de Control Relay
- Barra para control de acceso Vehicular

8. Procesos utilizados

8.1. Proceso de Inscripción

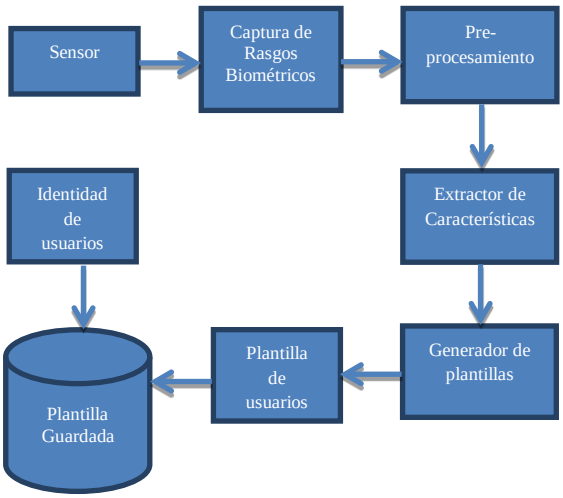

Figura 4. Diagrama del Proceso de Inscripción de los patrones biométricos

8.2. Proceso de Identificación en la Autentificación

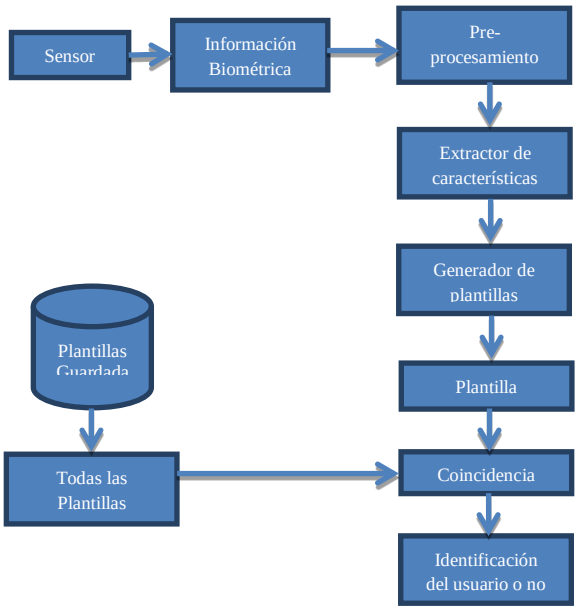

Figura 5. Diagrama del Proceso de Identificación en la autentificación

8.3. Proceso de Verificación en la Autentificación

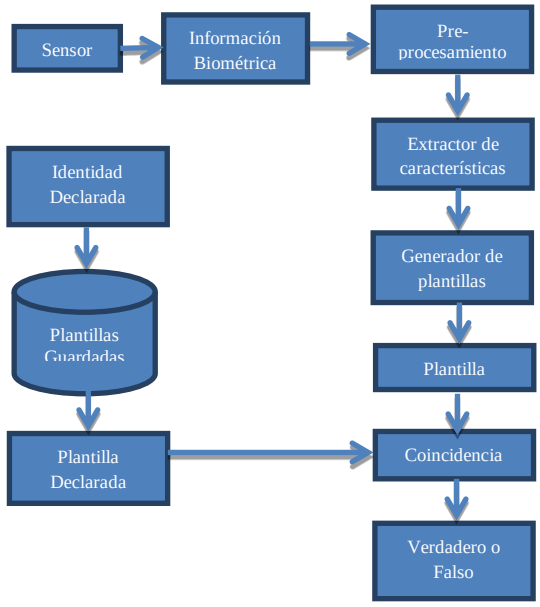

Figura 6. Diagrama del Proceso de Verificación en la autentificación

9. Escenarios

9.1. Acceso de Personal Autorizado

Para acceder al lugar la persona deberá pararse frente al biométrico de reconocimiento facial, mirar hacia ella y una vez que el realice el reconocimiento del rostro de la persona, el sistema buscará en la base de datos previamente alimentada.

Figura 7. Acceso Peatonal

9.2. Acceso de Vehículos

Si se ingresa con vehículo, el auto deberá detenerse cerca del biométrico, una vez que la se analice el rostro de la persona, buscará en la base de datos previamente alimentada y si detecta que la persona está autorizada para el ingreso al lugar, la barra de acceso se elevará de forma automática.

Figura 8. Acceso Vehicular

9.3. Acceso de Visitantes

El visitante es una persona que no consta en la base de datos, y que asiste al lugar esporádicamente, el acceso de un visitante solo podrá darse con la respectiva autorización de un residente de la ciudadela o personal de la empresa, se registran los datos del visitante, así como también los datos del vehículo en el caso de que se ingrese con uno, este proceso es responsabilidad del personal de seguridad de la ciudadela privada o empresa.

10. Conclusiones

1. En la actualidad y a nivel mundial, los dispositivos biométricos son considerados como los métodos más efectivos en el control de seguridad, ya que se basan en patrones proporcionados por las características físicas de cada persona, gracias a esta tecnología cada vez se están desarrollando nuevos avances, y con mayor frecuencia existe la necesidad de cambiar los métodos de control comunes por sistemas inteligentes que faciliten y a la vez sean más estrictos en la vigilancia de un lugar.

2. Las empresas y ciudadelas privadas carecen de un control efectivo por parte del personal de seguridad que labora en ellas, indiscutiblemente esto afecta directamente a las personas que habitan o trabajan en estos lugares. Los controles deben ser ejecutados desde el momento de la admisión al lugar, y es por eso que para ayudar a mejorar los niveles de eficiencia se necesita de la tecnología, en este caso de los dispositivos biométricos, los cuales restringirán el acceso a las personas que no estén registradas, evitando el ingreso de personas ajenas al conjunto habitacional o institución privada que se desea controlar.

3. Se debe realizar capacitación constante al personal de seguridad, y la revisión minuciosa de todos procesos que se tienen en tema de seguridad, la evaluación de estos procesos pueden contribuir con el mejoramiento de la seguridad en todos los lugares públicos y privados del país.

11. Recomendaciones

1. Se recomienda la utilización de dispositivos biométricos que posean cámara con infrarrojos para que pueda funcionar a la perfección en el día, así como en la noche, cada dispositivo debe tener una protección para soportar mayor tiempo las condiciones climáticas, las cuales son variables en nuestro país. Se sugiere que se las cubra con un protector para ayudar a protegerlas de la intemperie, la lluvia y el sol.

2. Se debe dar mantenimiento preventivo a todos los dispositivos que conforman el sistema, para evitar el desgaste y extender el tiempo de vida de cada uno de estos elementos.

12. Referencias

[1] Biometría Argentina, Ecuador: Seguridad portuaria biométrica, http://www.biometria.gov.ar/noticias, fecha de consulta agosto 2013

[2] Griaule Biometrics, SDK para Lector de Huellas de Microsoft, http://www.griaulebiometrics.com/page/en-us/downloads, fecha de consulta junio 2013

[3] Boulgouris, N. V., Konstantinos , P., & Evangelia , M., Biometrics: Theory, Methods, and Applications, Wiley,2009.

[4] Ecuavisa. Frustrado asalto en ciudadela privada deja a delincuente herido. http://www.ecuavisa.com/noticias/regionales-costa, fecha de consulta agosto 2013

[5] El Telégrafo. Ecuador identificará a delincuentes con tecnologías rusas. http://www.telegrafo.com.ec/noticias/judicial, fecha de consulta agosto 2013

[6] Gates, K. A., Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance, NYU Press, 2011

[7] Grupo IWI, Implantación de la LOPD en la empresa. Medidas de seguridad, Vértice, 2009

[8] Id Consultants, Dispositivos Biométricos, http://www.idconsultants.us, fecha de consulta junio 2013

[9] INEC, Instituto Nacional de Estadísticas y Censos, http://www.inec.gob.ec, fecha de consulta agosto 2013

[10] Instituto Nacional de Tecnologías de la Comunicación, Estudio sobre las tecnologías biométricas aplicadas a la seguridad, www.inteco.es, fecha de consulta agosto 2013

[11] Janices, P., Avances de la Biometría en América latina: una herramienta más para garantizar la identidad y la democracia, http://www.biometria.gov.ar/editoriales, fecha de consulta julio 2013

[12] López, P. A., Seguridad informática, Editex, 2010.

[13] Modi, S. K., Biometrics in Identity Management: Concepts to Applications, Artech House, 2011.

[14] Mou, D., Machine-Based Intelligent Face Recognition, Springer, 2010

[15] Muller, B. J., Security, Risk and the Biometric State: Governing Borders and Bodies, Routledge, 2010

[16] Newman, R., Biometrics: Application, Technology, and Management, Cengage Learning, 2009

[17] Ricaurte, J., Cámaras IP, http://img.redusers.com/, fecha de consulta junio 2013

[18] Sencar, H. T., Velastin, S., Nikolaidis, N., & Shiguo, L., Intelligent Multimedia Analysis for Security Applications, Springer, 2010

[19] Stan, L., & Anil, J., Handbook of Face Recognition, Springer, 2011

[20] Umanick., Autenticación Biométrica por Reconocimiento Facial, http://www.umanick.com/index.php/tecnologia/reconocimiento-facial, fecha de consulta julio 2013

[21] Vacca, J. R., Computer and Information Security Handbook, Morgan Kaufmann, 2009

[22] Wechsler, H., Reliable Face Recognition Methods: System Design, Implementation and Evaluation (Vol. 7), Springer, 2009

[23] Wikipedia, Biometría, http://es.wikipedia.org/wiki/Biometr%C3%ADa, fecha de consulta julio 2013

[24] Wikipedia, Sistema de Reconocimiento Facial. http://es.wikipedia.org/wiki/Sistema_de_reconocimiento_facial, fecha de consulta julio 2013

[25] Wikipedia, Servidor HTTP, http://es.wikipedia.org/wiki/Servidor_HTTP_Apache, fecha de consulta agosto 2013