SISTEMA DE CONTROL Y GESTION DE PERSONAL PARA PYMES, BASADO EN SISTEMAS BIOMETRICOS

Autores: Jéssica Mariuxi Mite Tigrero [(1)], Mariuxi Annabell Rodríguez Borbor [(2)], Jéssica Viviana Franco Rodríguez [(3)]
Coautor: Gustavo H. Galio Molina Master en Sistemas de Información Gerencial ESPOL [(4)]
Facultad de Ingeniería en Electricidad y Computación
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo Km. 30.5 Vía P
Apartado 09-01-5863, Guayaquil - Ecuador
mariuxi03@hotmail.com [(1)], mannabell03@hotmail.com [(2)], jesvifra12@hotmail.com [(3)], ggalio@espol.edu.ec [(4)]

Resumen

El objetivo de los sistemas de control de acceso es permitir el ingreso autorizado del personal de una entidad a departamentos específicos. Los sistemas de acceso basados en tarjetas de proximidad pueden autorizar el ingreso a la persona quien la porte, pero no pueden distinguir que quien porte la tarjeta sea alguien autorizado. Los sistemas que usan números de identificación personal sólo requieren que un individuo se sepa un número específico para otorgarle acceso. Los dispositivos biométricos verifican la identidad de una persona mediante características físicas que son únicas e inalterables en cada individuo, como las dimensiones de la mano, peculiaridades o medidas de los ojos, huellas digitales o voz. Este documento tiene como objetivo implementar un control de acceso de personal en pequeñas y medianas empresas, a través de un dispositivo aislado o autónomo que consiste en un lector biométrico de huellas digitales. La aceptación del usuario siempre será un factor esencial en la implementación exitosa de un dispositivo biométrico. Presentamos el análisis financiero de la comercialización de un sistema biométrico junto con sus dispositivos de lectura de huella digital con lo cual las entidades interesadas puedan examinar esta propuesta económica, los beneficios ofrecidos y oportunidades nuevas de negocio.

Palabras Claves: *Sistema Biométrico Dispositivos Biométricos, Control de Accesos, Lector de Huella Digitales, Sistemas de Control Biométrico, Sistemas de Acceso Biométricos.*

Abstract

The object of Access control systems is allows the access authorized the personnel of an entity to specific departments. The Access systems based on proximity cards can authorize entry to the person who the cover, but can't tell you who someone carrying the card is authorized. The Systems that use personal identification numbers only requires an individual to know a specific number to allow access. Biometric devices verify the identity of a person by physical characteristics that are unique and unchanging in each individual, as the dimensions of the hand, characteristics or actions of the eyes, fingerprints or voice. This document has to implement a personnel access control in small and medium enterprises, through a single device or autonomous that consists of a biometric fingerprint reader. The acceptance of the user will always be an essential factor in the successful implementation of a biometric device. Introducing the financial analysis of the marketing of a biometric system along with their reading devices fingerprint which the entities concerned to examine this proposal, benefits offered and new business opportunities.

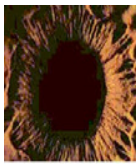
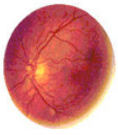
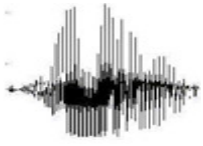
Keywords*: Biomet|rics Systems, Biometric Device, Access Control, Fingerprint Reader,, Biometric Control System, Biometric Access System.*

1.1 Antecedentes

La biometría es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos. El término se deriva de las palabras griegas "bios" de vida y "metron" de medida.
La "biometría informática" es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para "verificar" identidades o para "identificar" individuos.
En las tecnologías de la información (TI), la autentificación biométrica se refiere a las tecnologías para medir y analizar las características físicas y del comportamiento humanas con propósito de autentificación

Las huellas dactilares, las retinas, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, representan ejemplos de características físicas (estáticas), mientras que entre los ejemplos de características del comportamiento se incluye la firma, el paso y el tecleo (dinámicas). La voz se considera una mezcla de características físicas y del comportamiento, pero todos los rasgos biométricos comparten aspectos físicos y del comportamiento. En la actualidad existen sistemas biométricos que basan su acción en el reconocimiento de diversas características, como puede apreciarse en la tabla 1.

Tabla 1. Técnicas Biométricas más utilizadas

	
Rostro	Termograma del rostro
	
Huella Dactilar	Mano
	
Venas de las manos	Iris
	

Patrón de Retina	Voz
	
Firma Digital	

Cada una de las técnicas anteriores posee ventajas y desventajas comparativas, las cuales deben tenerse en consideración al momento de decidir que técnica utilizar para una aplicación específica. En particular deben considerarse las diferencias entre los métodos anatómicos y los de comportamiento. Una huella dactilar, salvo daño físico, es la misma día a día, a diferencia de una firma que puede ser influenciada tanto por factores controlables como por psicológicos no intencionales. También las máquinas que miden características físicas tienden a ser más grandes y costosas que las que detectan comportamientos. Debido a diferencias como las señaladas, no existe un único sistema biométrico que sea capaz de satisfacer todas las necesidades. Una compañía puede incluso decidir el uso de distintas técnicas en distintos ámbitos. Más aún, existen esquemas que utilizan de manera integrada más de una característica para la identificación. Se integran el reconocimiento de rostros y huellas dactilares. La razón es que el reconocimiento de rostros es rápido pero no extremadamente confiable, mientras que la identificación mediante huellas dactilares es confiable pero no eficiente en consultas a bases de datos. Lo anterior sugiere el utilizar el reconocimiento de rostros para particionar la base de datos. Luego de esto comienza la identificación de la huella. Los resultados alcanzados por el sistema conjunto son mejores que los obtenidos por sus partes por separado. En efecto, las limitaciones de las alternativas por separado son soslayadas, logrando además respuestas exactas con un tiempo de proceso adecuado.

1.1.1 Huellas Dactilares

Una huella dactilar es la representación de la morfología superficial de la epidermis de un dedo. Posee un conjunto de líneas que, en forma global, aparecen dispuestas en forma paralela (colinas o *ridge lines* y *furrows*). Sin embargo estas líneas se intersectan y a veces terminan en forma abrupta. Los puntos donde las colinas terminan o se bifurcan se conocen técnicamente como minucias. Otros puntos singulares de una huella dactilar son aquellos donde la curvatura de los ridges es máxima. Esos puntos reciben el nombre de cores y deltas.

1.1.1.3 Identificación de Huellas dactilares

Son las formas caprichosas que adopta la piel que cubre las yemas de los dedos. Están constituidas por rugosidades que forman salientes y depresiones.

Las salientes se denominan crestas papilares y las depresiones surcos interpapilares. En las crestas se encuentran las glándulas sudoríparas. El sudor que éstas producen contiene aceite, que se retiene en los surcos de la huella, de tal manera que cuando el dedo hace contacto con una superficie, queda un residuo de ésta, lo cual produce un facsímil o negativo de la huella.

1.1.1.2 Clasificación

Los patrones de huellas digitales están divididos en 4 tipos principales, todos ellos matemáticamente detectables. Esta clasificación es útil al momento de la verificación en la identificación electrónica, ya que el sistema sólo busca en la base de datos del grupo correspondiente.

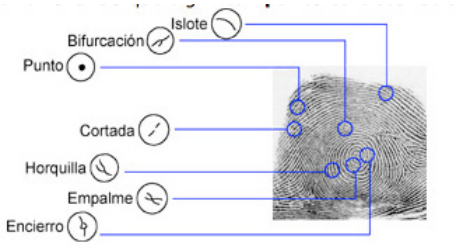


Figura 1. División Puntos característicos de un dedo

1.1.1.3 Procedimiento

Con este conjunto de puntos, el software biométrico de huella digital genera un modelo en dos dimensiones, mismo que se almacena en una base de datos, con la debida referenciación de la persona que ha sido objeto del estudio.

Tabla 2. División d puntos característicos de un dedo

	
El dedo es leído por un lector de huellas.	El dedo es codificado.
	
Una plantilla matemática es generada.	Esto guarda y reconoce un conjunto de números que solo podrán ser reconocidos como una plantilla.

1.1.2 Funcionamiento y rendimiento

En un sistema de Biometría típico, la persona se registra con el sistema cuando una o más de sus características físicas y de conducta son obtenidas, procesada por un algoritmo numérico, e introducida en una base de datos. Idealmente, cuando entra, casi todas sus características concuerdan; entonces cuando alguna otra persona intenta identificarse, no empareja completamente, por lo que el sistema no le permite el acceso. Las tecnologías actuales tienen tasas de error que varían ampliamente (desde valores bajos como el 60%, hasta altos como el 99,9%).

1.1.3 Procesos de Autentificación e Identificación biométrica.

En el proceso de autentificación (o verificación) los rasgos biométricos se comparan solamente con los de un patrón ya guardado, este proceso se conoce también como uno-para-uno (1.1).
En el proceso de identificación los rasgos biométricos se comparan con los de un conjunto de patrones ya guardados, este proceso se conoce también como uno-para-muchos (1:N).

1.1.6 Situación Actual

Los sistemas biométricos en los últimos años han llegado a convertirse en una importante herramienta de apoyo a los distintos sistemas de seguridad existentes, dado los avances científicos en el campo de la identificación de huellas dactilares, reconocimiento de rostros, lectura de iris y/o retina, reconocimiento de voz y otros. Así estas tecnologías están incursionando en las actividades laborales de diferentes instituciones como gobiernos, aeropuertos, empresas, unidades educativas, bancos, etc. El uso de la tecnología biométrica aumenta los niveles de seguridad en las entidades, ya que a las personas no autorizadas por el sistema no se les permitirán el acceso.

1.1.7 Alternativas de solución al problema

Entre las posibles soluciones al problema de control de acceso de personal tenemos las siguientes:

- Registrar las marcaciones hechas por el personal que labora en la empresa a través de tarjetas de aproximación.
- Sistema Biométrico para Análisis de iris.
- Sistema Biométrico de Huellas Dactilares

1.1.8 Solución Propuesta

Crear software de administración y base de datos, los cuales puedan agregar y eliminar huellas digitales, suspender el acceso por determinado tiempo a alguna persona con privilegio de acceso, control coordinado y

coherente del acceso, y llevar un registro histórico del ingreso a la empresa.

2. Requerimiento para la implementación

Implementar un sistema biométrico, o de cualquier otra índole, requiere además de buena programación un análisis exhaustivo de los requerimientos que se utilizarán tanto de hardware o software, ya que de esto dependela funcionalidad que vaya a tener el sistema.
A continuación se presentan los requerimientos a necesitar:

2.1. Requerimiento de Hardware

DISPOSITIVO FOH 02
Se trata de una solución que se asocia a una computadora y funciona como terminal para registrar los accesos de los empleados, su diseño es práctico y funcional, ofrece 500 DPI de resolución, su conexión es a través de un puerto USB Mnte el cual también toma la energía necesaria para funcionar, su cable de 1.5 metros, permite mayor movilidad y opciones de colocación.

Un lector de huella digital lleva a cabo dos tareas:
1) Obtener una imagen de su huella digital, y
2) Comparar el patrón de valles y crestas de dicha imagen con los patrones de las huellas que tiene almacenadas.

Figura 1. Captura de Huella

2.2 Requerimiento de Software

- Lenguaje de desarrollo: Visual 6
- Base de Datos : SQL Server 2005
- Librería del lector: SDK

2.3 Requerimiento de Infraestructura

El proceso de identificación comienza cuando el lector biométrico captura la característica del individuo a ser identificado y la convierte a formato digital, para que a continuación el extractor de características produzca una representación compacta con el mismo formato de los templates. La representación resultante se denomina query y es enviada al comparador de *características* que confronta a éste con uno o varios *templates*para establecer la identidad.

2.4. Requerimiento Funcionales de Control de Acceso

- Permitir el ingreso (Login) al sistema mediante usuario,password y huella digital
- Implementar reglas de control y de negocio a nivel de aplicación, de formularios y de datos
- Validar la información ingresada contra las reglas de control implementadas en la solución.
- Restringir el acceso a Usuarios por Fechas y Equipos.
- Restringorel acceso a las utilidades del Sistema mediante niveles de seguridad: Usuarios, Perfiles y Roles entre otros.

3. Análisis y diseño

En la actualidad las empresas manejan gran cantidad de información, debido a esto todos los datos deben estar almacenados en una base de datos para poder tener acceso a ellos mediante una aplicación profesional; sin esta funcionalidad resultaría imposible tratar y manejar en su totalidad los datos que lleva a cabo la empresa.

Uno de los pasos cruciales en la construcción de una aplicación que maneje una base de datos, es sin duda, el diseño de la base de datos. Si las tablas no son definidas apropiadamente, se tendrá dolores de cabeza al momento de ejecutar consultas a la base de datos para tratar de obtener algún tipo de información.

Sin importar si la base de datos tiene sólo 20 registros, o algunos cuantos miles, es importante asegurarse que la base de datos está correctamente diseñada para que tenga eficiencia y que se pueda seguir utilizando por largo del tiempo.

4. Análisis Financiero

El análisis financiero de los proyectos constituye la técnica matemático-financiera y analítica, a través de la cual se determinan los beneficios o pérdidas en los que se puede incurrir al pretender realizar una inversión u algún otro movimiento, en donde uno de sus objetivos es obtener resultados que apoyen la toma de decisiones referente a actividades de inversión.

4.1 Proyección de Ventas

La proyección de ventas fue basada en términos anuales en el lapso de 3 años. La información se detalla en la tabla siguiente, partiendo de nuestro mercado objetivo.

Tabla 3. Proyección de Ventas

Ventas contratos	Año			Total de ingresos		
	1	2	3	Año 1	Año 2	Año 3
Pequeña Empresa	45	50	56	51.300	57.000	63.840
Mediana Empresa	40	53	59	38.000	50.350	56.0500
Microem presa	15	20	22	11.400	15.200	16.720
TOTAL	**100**	**123**	**137**	**100.700**	**122.550**	**136.610**

4.2 Costos de Dispositivos Biométricos

A continuación se detalla el costo de los dispositivos biométricos a ser utilizados.

Tabla 4. Costo de dispositivos biométricos

Costo de Producción	Costo Unit	Año 1	Año 2	Año 3
Dispositivo BioStation	600,00	24.000,00	31.800,00	35.400,00
Dispositivo BioLite Solo y Dispositivo L2000	400,00	24.000,00	28.000,00	31.200,00
Total		**48.000,00**	**59.800,00**	**66.600,00**

4.3 Flujo de Caja del Inversionista

A continuación en la tabla siguiente presentamos los valores correspondientes al TIR y el VAN del proyecto, obtenido a partir del flujo de caja del inversionista, podemos observar que obtenemos un 52 % en la TIR,considerando una tasa de descuento del proyecto del 12 % haciendo que el proyecto sea rentable. El VAN que obtuvimos es de $13.228,18.

Tabla 5. Flujo de Caja del Inversionista

Tasa de Descuento del Proyecto	12%
VAN	13.228,18
TIR	52%

4.4 Retorno de la Inversión

La recuperación de la inversión del proyecto está basada en el flujo neto acumulado, el mismo que demuestra que la inversión estará recuperada en 1 año y nueve meses de la ejecución del proyecto.

Tabla 6. Retorno de la Inversión

Flujo de Efectivo	
Año 1	4.624,84
Año 2	13.090,81
Año 3	18.347,90
Retorno de lnversión	1,85 años

4.5 Gráfico Comparativo de los Ingresos vs. Los Egresos

A continuación presentamos los ingresos y egresos obtenidos en los 3 años, como se puede apreciar los ingresos son mucho más altos que los egresos.

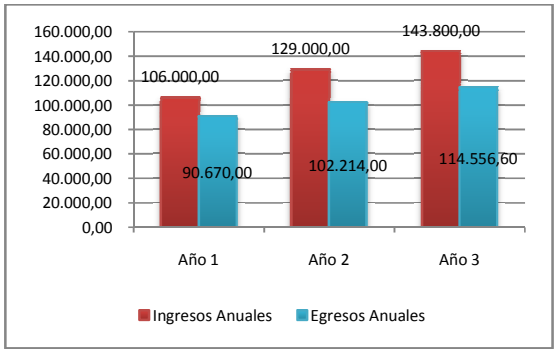


Figura 3. Gráfico Comparativo de Ingresos vs. Egresos

5. Conclusiones

Actualmente no existe el algoritmo perfecto de clasificación y de identificación para sistemas biométricos, todos se encuentran a la vanguardia haciendo innovaciones y mejorando sus algoritmos.

Pero esto no quita que los sistemas actuales sean seguros y confiables. Las empresas medianas y microempresas pueden tener acceso a un sistema confiable quien pueda controlar por ellos al personal de su entidad, en la actualidad los precios son muy accesibles, dejando de ser los sistemas biométricos un privilegio de grandes empresas.

6. Recomendaciones

Para la evaluación de la huella o impresión hay que tener en consideración que esta debe de estar lo más nítido posible ya que una imagen borrosa puede originar el hallazgo de un delta falso.

Ninguna persona a excepto del Administrador que es quien tiene todos los permisos puede tener acceso a la base de datos puesto que la manipulación inapropiada de la misma podría provocar errores y por ende la alteración de la información.

7. Agradecimientos

La presente Tesis es un esfuerzo en el cual, directa o indirectamente, participaron varias personas quienes

con sabiduría y paciencia nos supieron corregir, y dar opiniones.
Agradezco al Dr. Gustavo Galio por haber confiado en nosotras, por la paciencia y por la inducción brindada en el transcurso del desarrollo del proyecto.
Gracias a nuestros padres por su apoyo económico y anímico en todo el proceso de nuestros estudios, también a nuestros compañeros, que nos brindaron apoyo, y con quienes compartimos una grata amistad.

6. Referencias

[1] N. Ratha, S. Chen, and A. Jain, "Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images", Pattern Recognition, third edition 2006

[2]L. Hong and A. Jain, "Integrating Faces and Fingerprints for Personal Identification", IEEE Transactions on Pattern Analysis and Machine Intelligence, 2010

[3]G. Drets & H. Liljenström, "Fingerprint Sub-Classification and Singular Point Detection", International Journal of Pattern recognition and Artificial Intelligence, vol. 12, no. 4, 407-422, 1998.

[4] A. Hrechack and J. McHugh, "Automated Fingerprint Recognition Using Structural Matching", Pattern Recognition, 2004.

[5]www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm

M. Sc. Gustavo H. Galio Molina
Director del Proyecto