PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
Facultad de Ciencias e Ingeniería
Sección de Electricidad y Electrónica

Verificación de Identidad de Personas mediante Sistemas Biométricos para el Control de Acceso a una Universidad

Tesis para la optar el título de ingeniero electrónico

Presentado por:
Luis Eduardo Balmelli Chuquisengo

Lima - PERÚ
2006

RESUMEN

El presente documento es el resultado de la investigación realizada en la Pontificia Universidad Católica del Perú para la implementación de sistemas biométricos (lectores de huellas dactilares) como elementos de seguridad.

Dada la problemática existente en la universidad (robos, plagios, amontonamiento de personas para ingresar, etc.), al implementar sistemas biométricos se estaría mejorando sustancialmente esta situación, pues aparte de tener un lugar más seguro y confiable, se estaría involucrando a la comunidad universitaria en el uso de tecnología de vanguardia.

En el contenido del presente documento de investigación se abordará con mayor detalle los temas relacionados a los sistemas de seguridad empleados actualmente tanto en lugares públicos como privados, y la descripción y evaluación (costos y beneficios) de los sistemas biométricos más usados en el mundo.

Habiendo hecho el análisis de costos y beneficios, se llega a la conclusión de que la implementación de sistemas biométricos basados en las huellas dactilares sería la opción óptima, tanto para mejorar la seguridad como para agilizar el ingreso al campus universitario.

INDICE

INTRODUCCION

Los sistemas de seguridad para el acceso a lugares, verificación o identificación de personal, basados en utilizar rasgos biométricos se presentan como el futuro en el campo de la seguridad puesto que son los más confiables y actualmente están siendo usados en muchas partes del mundo sin mayores problemas.

En el Perú, como en la gran mayoría de países en vías de desarrollo, la falta de tecnología es algo común por lo que el uso de sistemas biométricos para la seguridad sería un gran avance. Teniendo en cuenta que la implementación de sistemas biométricos no necesariamente sería algo costoso, puesto que hay lectores biométricos con costos bajos ya que esta tecnología va avanzando y progresando rápidamente, habría que tomar en cuenta la idea de ir mejorando y creciendo junto con la tecnología.

La implementación de estos sistemas significaría un mayor control de acceso físico, evitaría largos tiempos de espera para ingresar a ciertos lugares públicos y/o privados como sería el caso a una universidad por parte de los alumnos, protegería transacciones financieras, verificaría el tiempo de llegada y salida de empleados de sus centros laborales, evitaría robos y plagios, siendo estos últimos ejemplos dos de las mayores razones para la utilización de sistemas de seguridad más confiables.

CAPITULO 1

SISTEMAS DE SEGURIDAD - CONTROL DE ACCESO

1.1 Demanda de Servicios

En la actualidad la demanda por contar con sistemas de seguridad basados en rasgos biométricos está creciendo, ya que se ha comprobado que son los sistemas de seguridad más eficientes del mercado (a pesar de no tener un 100 % de efectividad) y son el futuro de la seguridad.

La mayor parte de este crecimiento se da en países desarrollados debido a que cuentan con tecnología de punta y mayormente se encuentran estos sistemas en grandes aeropuertos, grandes compañías, etc. Pero la implementación de sistemas biométricos como seguridad no queda ahí, son usados en lugares tales como bancos, supermercados, oficinas o fábricas, como parte de la rutina diaria.

En países en vías de desarrollo no es grande la demanda por contar con estos sistemas, salvo en lugares donde la seguridad debe ser “la mejor posible” como es el caso de la torre de control de un aeropuerto o la entrada a la bóveda de un banco. Otro punto importante que debemos resaltar es que la poca difusión de estos sistemas de seguridad hace que el interés sea mínimo y las personas en su mayoría desconozcan del uso y de los beneficios de contar con esta tecnología.

1.2 Políticas de Desarrollo y Difusión de Sistemas de Seguridad

La seguridad es un tema muy importante en todo el mundo y dentro de cada país, en lugares públicos como privados; como consecuencia de ello, constantemente salen al mercado nuevas técnicas y tipos de seguridad. En el campo de la biometría también hay una continua investigación y se van probando nuevas alternativas (nuevos sistemas basados en rasgos biométricos o combinaciones entre los sistemas de rasgos biométricos ya desarrollados).

A pesar de que la falta de seguridad es un problema álgido en nuestro país, no hay una política clara de desarrollo tecnológico en este aspecto, por lo tanto no está difundido el uso de sistemas biométricos como una alternativa en lo que a seguridad se refiere. Por otra parte nos hemos acostumbrado a contar con lo más barato (en muchos casos lo menos costoso no es lo más indicado), presentándose numerosos problemas de seguridad que serían fácilmente evitados con el uso de sistemas de seguridad basados en rasgos biométricos.

1.3 Características de estos Servicios

1.3.1 Sistemas no Biométricos

Existen muchos tipos de seguridad, uno de ellos es el contar con un vigilante, esto es algo positivo ya que una máquina no tiene criterio para solucionar determinadas situaciones. El problema se presenta cuando el vigilante es “la seguridad”; esto no

es lo más conveniente debido a muchas razones, por ejemplo, en el caso de presentarse un asalto el vigilante no va a poder hacer nada para impedir que los asaltantes entren al local, o también puede darse el caso de que el vigilante deje entrar a personas no deseadas.

1.3.2 Sistemas Biométricos

El uso de estos sistemas es sencillo, éstos podrían ser operados por cualquier persona con la debida capacitación. Simplemente se debe mostrar el rasgo físico a examinar y dependiendo de los resultados se dejará acceder a la persona al lugar donde desea entrar, siempre y cuando los datos capturados concuerden con alguno de los que se encuentren en la base de datos.

Los precios de estos aparatos tienen una variabilidad dependiendo de la aplicación que se les va a dar o del tipo de rasgo biométrico que se analizará en la captura de datos. Se tienen sistemas de menos de 100 dólares y sistemas que cuestan miles de dólares.

Estos sistemas pueden ser evaluados o medidos por diferentes aspectos, como por ejemplo la necesidad de alguien que desea contar con más seguridad y tener un mejor control, el grado de aceptación del usuario con respecto al aparato biométrico usado para la captura de imágenes, en este caso se debe tener en cuenta cuánto tiempo va a tomar y qué tan cómoda se desea que sea la captura. Otra forma de

medir estos sistemas es mediante opiniones y pruebas previas realizadas por los expertos del caso.

Se debe tomar en cuenta que con el tiempo, hay que volver a actualizar la base de datos en algunos de los sistemas debido a que muchos rasgos físicos cambian con el transcurrir de los años.

1.4 Estado actual de la seguridad en una universidad

En las universidades de nuestro país la seguridad no es la más adecuada ya que constantemente ingresan personas ajenas con el propósito de perjudicar y hacer daño a estas instituciones. Se cuenta con vigilantes en las puertas para controlar el acceso de los estudiantes y de personas que no perteneciendo a la universidad, necesitan ingresar para realizar algún trámite. Los alumnos ingresan presentando su carnét universitario, pero no hay forma de probar que realmente ese documento pertenezca al portador. Se sabe, por datos y comentarios obtenidos del personal de seguridad de la universidad que existen personas extrañas que ingresan presentando carnéts universitarios falsos o ajenos, sin que los vigilantes estén en la capacidad de detectar estas irregularidades. Quienes así ingresan, frecuentemente crean problemas pues utilizan las instalaciones de esta institución sin la debida autorización, ya sea en salones de clases, laboratorios u oficinas, produciéndose graves pérdidas y perjuicios a la institución (alrededor de 20 mil dólares al año,

según la oficina de seguros de la universidad). Lamentablemente no se cuenta con sistemas de seguridad tan eficientes como para contrarrestar esta situación.

Sin embargo, la aplicación de nuevas tecnologías implica un gran avance en el país. En este caso particular de una Universidad se implementaría un Sistema Biométrico que cumpla con las necesidades de la misma. Lo que se busca es tener un sistema que sea económico, eficiente y que tenga un alto grado de aceptación por parte de las personas. Con la implementación de estos sistemas la universidad se beneficiaría ampliamente y se dejarían de lado las limitaciones que se tienen en la actualidad, ya que la base de datos del vigilante actualmente es un cuaderno que se actualiza cada año.

1.5 Principales problemas

Como ya se mencionó, para ingresar a una Universidad se debe mostrar un documento de identificación (carnét), pero muchas personas ingresan presentando carnéts de otras instituciones, burlando a los vigilantes. Si ocurre el caso en que no se tiene el carnét a la mano, se procederá a responder algunas preguntas (formuladas por el vigilante) para verificar si esta persona pertenece realmente a la universidad, lo que implica a veces pérdida de tiempo valioso para el alumno que desea ingresar (cabe la posibilidad de que el alumno tenga un examen en ese momento). Otro problema que se ocasiona es que mientras el vigilante está atendiendo al alumno, hace esperar a las demás personas.

Los vigilantes reconocen a muchas personas y de vez en cuando las dejan entrar así no tengan ningún documento, lo que puede ser un grave problema debido a que estas personas pueden ya no pertenecer a la institución.

El objetivo de este trabajo de investigación es hacer el diseño de un sistema biométrico basado en el reconocimiento de las huellas dactilares para poder contar con mayor seguridad dentro de una universidad y controlar más eficientemente el ingreso peatonal, comprobándose que una persona que dice pertenecer a la universidad, realmente pertenezca a ella. Se tomará una muestra en una universidad, en este caso, la Pontificia Universidad Católica del Perú.

Como se dijo anteriormente, la muestra se tomará en la Universidad Católica, la cual cuenta actualmente con 17700 alumnos activos aproximadamente (al decir alumnos activos nos referimos a alumnos matriculados en el ciclo actual, primer periodo del 2006). En el año 2004 hubo 15658 alumnos activos aproximadamente, por lo que ha habido un incremento sustancial. Esto se debe a que el número de alumnos nuevos que ingresan a los primeros ciclos (ya sea ciclo inicial o primer ciclo) es mayor al número de alumnos graduados por ciclo. Por lo tanto si se sigue cumpliendo esta regla cada ciclo va aumentando el número de alumnos activos en la universidad.

Se debe tomar en cuenta lo siguiente: cada nuevo ciclo (de los primeros periodos, es decir a comienzos del año) ingresan aproximadamente 3500 alumnos nuevos, y 800 alumnos para los segundos periodos (es decir a mediados del año).

En los siguientes gráficos se puede apreciar detalladamente la distribución de alumnos, profesores, trabajadores, jefes de práctica y practicantes; en la Universidad Católica, donde se hará la muestra:

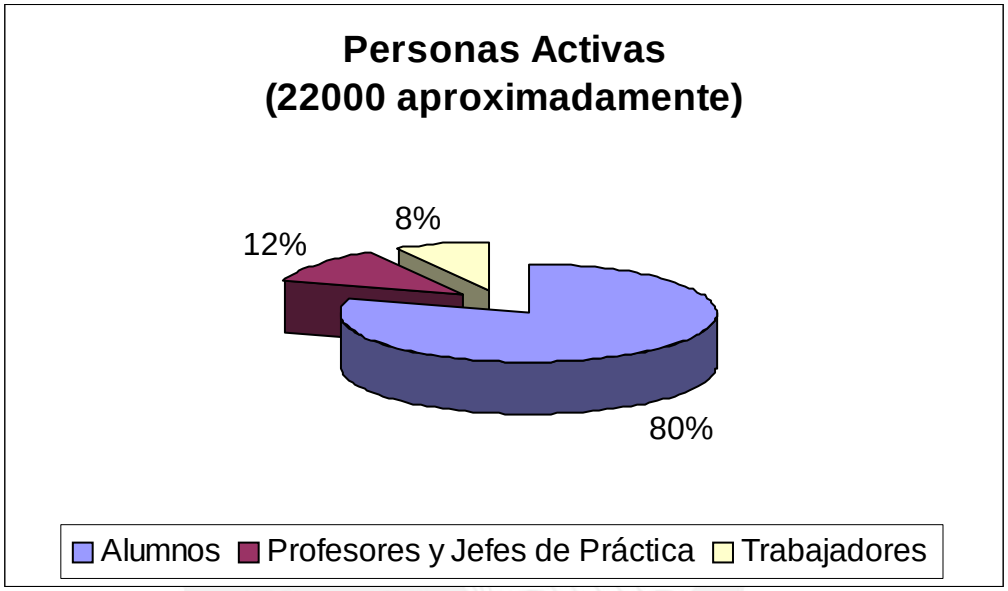


Figura 1.1: Universo de todas las personas que están autorizadas a ingresar a la universidad. [32]

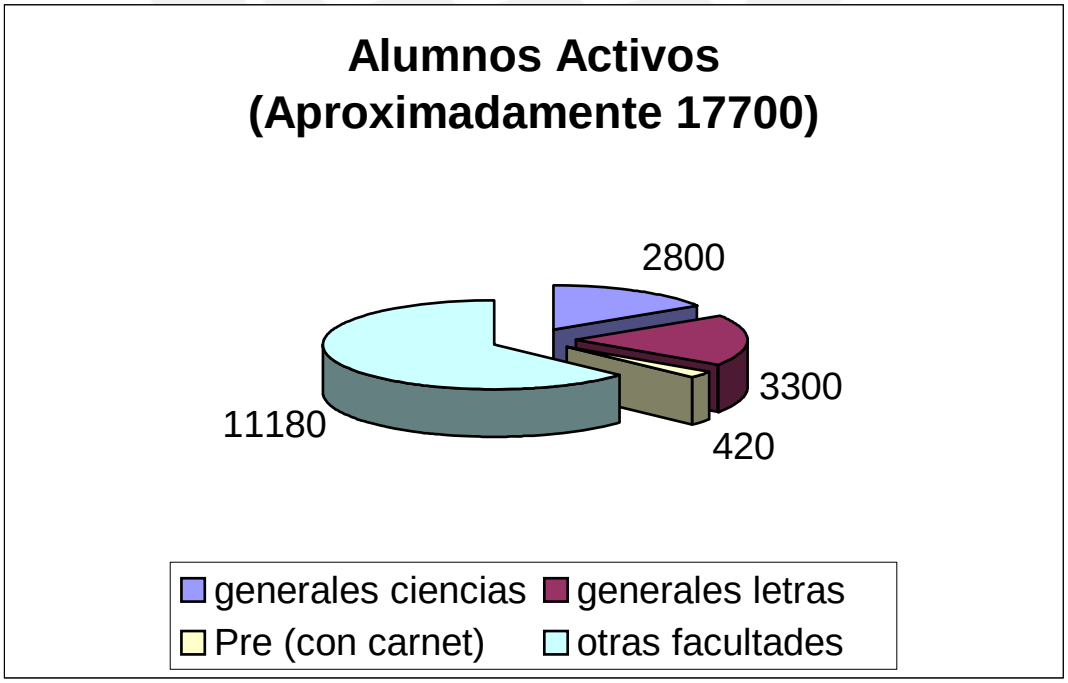


Figura 1.2: Universo de alumnos autorizados a ingresar a la universidad. [33]

***Nota**: estos números son con respecto al ciclo del 1er periodo del 2006. Durante ese semestre hubo 22175 personas aproximadamente con autorización de ingreso a la universidad.

Debido a la gran variedad de equipos (sistemas biométricos basados en las huellas dactilares) para la aplicación en estudio, es conveniente analizar varias posibilidades tanto en los productos como en el enfoque que se le va a dar (podría ser solamente alumnos del primer ciclo, sólo profesores, todos los alumnos en general, u otros casos).

Para el análisis de estos equipos se contactó a diversas empresas proveedoras nacionales como internacionales y se preguntó acerca de equipos biométricos que trabajaran en base a las huellas dactilares para realizar un reconocimiento (identificación y/o verificación) de por lo menos 20000 personas; pero la mayoría de estos equipos trabaja con pocas cantidades (ya sea 100, 500, 1000, 2000 personas, etc.) siendo muy versátiles, y si se quisiera trabajar con grandes volúmenes se deberá adquirir un software especial (SDK) para programar uno mismo en base a los requerimientos necesarios. El problema radica en que mientras más se aumenta la capacidad de estos equipos mayor será el tiempo de registro de personas y mayor será el error. Cabe resaltar que el tiempo promedio de identificación de una persona en estos sistemas es de menos de un segundo, para poblaciones de aproximadamente 5000 personas.

Para la implementación de estos sistemas en la Universidad Católica se deben tomar en cuenta muchos factores, tanto económicos como sociales. Esto implica analizar los problemas actuales y problemas que persisten desde hace mucho tiempo. Si bien estos sistemas inicialmente no calzan en el presupuesto que la universidad destina al área de seguridad, después de analizar las ventajas de sistemas biométricos frente a los que se tienen actualmente, o las desventajas de los actuales sistemas que implican gastos de reposición, pérdida permanente de objetos tangibles e intangibles, entre otras cosas, se debe tener en cuenta seriamente la aplicación de estos sistemas no sólo en esta universidad sino también en otras universidades y otros sitios públicos y privados.

Una vez que una persona ajena a la universidad ha ingresado pueden pasar muchas cosas, una de ellas es que esta persona haya ingresado con la predisposición de hacer mal, de robar, dañar las instalaciones, entre otras muchas acciones perjudiciales que podría cometer. Esta investigación busca evitar los robos. Según estadísticas obtenidas del área de seguridad de la Pontificia Universidad Católica del Perú en el año (2006) hasta la fecha (setiembre), se han detectado nueve casos de sustracciones internas en la universidad y una sustracción externa. Estos números varían constantemente pero están dentro de un promedio. Lo que se quiere es que haya un total de CERO o un número cercano de sustracciones dentro de la universidad, y para llegar a eso es necesario mejorar el sistema actual de seguridad. Hay que tener en cuenta que no solamente hay pérdida de objetos por parte de personas ajenas a la universidad sino también por parte de las personas

pertenecientes a ella por lo que sería necesario tener mayor control dentro de la universidad (salones, bibliotecas, cafeterías, entre otros).

En lo que a robos se refiere en la universidad, podemos catalogarlos en dos campos: de objetos tangibles y de objetos intangibles; como objetos tangibles nos referimos a todo lo que es computadoras, proyectores, mochilas, útiles, libros, entre muchas otras cosas que representan un gasto muy alto. No solo hay que tomar en cuenta lo listado anteriormente, también hay que sumar a la lista todos los objetos intangibles que son robados y perjudican claramente los intereses de la universidad. Nos referimos a plagios de tesis, documentos valiosos, copias de libros, conocimientos, etc. Muchas veces esto no es tomado con importancia, pero también representa un costo a la universidad.

Todo objeto tangible e intangible tiene un costo, si se va a reponer muchas veces ya no es el mismo y puede ser un poco mayor, o cabe la posibilidad de que el objeto sustraído ya esté fuera de circulación en el mercado. Si no se va a reponer el objeto, muchas veces se piensa que no se va a gastar, pero el gasto ya fue hecho cuando se adquirió el objeto. Ahora, también hay que agregar el costo de reposición de instalaciones dañadas por gente ajena a la universidad.

Según datos obtenidos gracias a la Oficina de Seguros de la universidad, desde abril del año 2005 hasta marzo del presente año el gasto por robos internos en la universidad bordea los 22 mil dólares, siendo los aparatos más robados las computadoras portátiles y los proyectores multimedia.

Actualmente la universidad gasta en seguro 6 mil dólares anuales, lo cual es relativamente poco. La prima es de mínimo 500 dólares y cuando ocurre un robo por un monto menor a 500 dólares, no hay reposición del objeto sustraído utilizando el seguro. A la hora de utilizar el seguro cuando ha habido un robo hay que tomar en cuenta factores como la antigüedad del objeto y su depreciación en el tiempo. El seguro solamente repone activos de propiedad de la universidad.

1.6 Justificación:

Una vez implementada esta propuesta, la Universidad Católica deberá mejorar la actual base de datos de las personas pertenecientes a ella, evitar burlar la vigilancia por medio de carnets falsos, caducados, o de otra institución. Se hará mas cómoda la entrada a la Universidad tanto para personas pertenecientes como personas ajenas a ella.

1.7 Objetivos:

- Investigar y profundizar el estudio de esta tecnología así como dar a conocer los beneficios que ésta puede brindar a la sociedad.
- Presentar el estudio a las autoridades de la Universidad Católica para su aplicación.

CAPÍTULO II

Sistemas Actuales de Seguridad y Control de Acceso

2.1 Sistemas biométricos

Siempre ha existido la necesidad de contar con sistemas de seguridad que sean buenos y confiables, capaces de tomar decisiones inteligentes por sí mismos. Pero es en los últimos años que se ha incrementado considerablemente esta necesidad. Uno de estos sistemas es el que trabaja a partir de un software que mediante el procesamiento de voz y/o imágenes puede lograr reconocer a una persona que desee ingresar a determinada área de algún lugar que sólo permite el acceso de personal autorizado; por lo que se desea hacer interactuar al hombre con la máquina.

El campo que se encarga de desarrollar este sistema es llamado Biometría, y ya es conocido por las ventajas que presenta, tales como una baja resolución de imágenes, bajo costo de aparatos de captura y una interacción amigable entre el dispositivo y el usuario. Los sistemas de seguridad basados en reconocer a las personas por medio de sus rasgos biométricos se han convertido en los más eficientes del mundo, llegando a tener una tasa de error de aproximadamente 0% (existen sistemas que pueden presentar un error en un millón, o un error en 100 mil). Se debe tener presente que en la Universidad Católica no se sabe a ciencia cierta cuál es el acierto de los sistemas usados, pero se sabe, según la oficina de

seguridad de la Universidad, que diariamente se detectan irregularidades (tales como robos, pérdidas, entre otros incidentes).

Por medio de estos sistemas se puede tener una mejora en: control fronterizo, seguridad ciudadana, prevención de fraude y robo de identidad, control de acceso lógico y físico.

Algunos ejemplos de técnicas utilizadas para los sistemas biométricos son los siguientes:

- reconocimiento por el iris
- detección del contorno del rostro
- reconocimiento por huellas digitales
- reconocimiento por forma de las manos
- reconocimiento de voz

Otros con mayor complejidad y más costosos son:

- reconocimiento por radiografías dentales
- reconocimiento de las venas
- reconocimiento por la cornea

Siendo el de radiografías dentales usado para casos policiales.

2.2 Aplicaciones de los sistemas biométricos

Para las diferentes aplicaciones se tiene que tomar en cuenta lo siguiente:

Registro

- La persona proporciona un documento de identificación para probar su identidad. Después la persona presenta el biométrico (por ejemplo, las yemas del dedo, mano, o diafragma) a un dispositivo de adquisición. Una o más muestras se adquieren, se codifican y se almacenan como plantilla de la referencia para las comparaciones futuras.

Verificación

- Se debe verificar que una persona es quien dice ser. Después de presentar un documento de identificación y una característica biométrica, el sistema captura los datos biométricos y genera una plantilla de ensayo, la cual es comparada con la plantilla de la referencia de la persona (almacenada en el sistema durante la inscripción) para determinar si hay similitud entre las dos plantillas.

Identificación

- Se desea identificar quién es la persona. En este caso no se presenta documento de identificación. La plantilla de ensayo se compara contra las plantillas almacenadas de referencia de todos los individuos listados en el sistema. Existen dos tipos de sistemas de identificación: positivo y negativo. En los positivos se determina si la persona que desea acceder es identificada

en la lista del sistema. Los sistemas negativos son diseñados para asegurarse de que la información biométrica de una persona no está presente en la base de datos.

Falsa captura

- Una falsa comparación ocurre cuando el sistema acepta dos plantillas de diferentes usuarios incorrectamente como si fuese una sola identidad. Las capturas falsas pueden ocurrir por semejanza entre las características de los individuos.

Falso rechazo

- Ocurre cuando un sistema rechaza una identidad válida. Ocurren porque no hay suficiente semejanza entre la plantilla de inscripción y la plantilla de ensayo; esto se da a causa de envejecimiento o alguna lesión.

2.3 Estado del Arte

2.3.1 Análisis de diferentes técnicas de reconocimiento

2.3.1.1 Reconocimiento por el Iris

Sensar, INC (Moorestown, NJ) ha desarrollado un software que primero identifica la cabeza, luego los ojos, y luego el iris. Utiliza un algoritmo que identifica tanto los bordes internos como los bordes externos del iris y excluye a los párpados si éstos

están tapando el iris. Después traduce las imágenes a un patrón de 512 bits mediante análisis de Fourier y es indiferente a cambios por la contracción de la pupila.

Zhenan Sun, Yunhong Wang, Tieniu Tan, y Jiali Cui [17] proponen un algoritmo que reconozca manchas en el iris para sobreponerse a las limitaciones de reconocimientos basados en los rasgos clasificadores del iris. La característica más distintiva de la imagen del iris proviene de los cambios espaciales en la estructura de la imagen, entonces los patrones representativos deben detectar la intensidad de las variaciones en las señales del iris.

Kang Ryoung Park, y Jaihie Kim [18] proponen un nuevo método de adquisición rápida de imágenes del iris para capturar imágenes centradas en los ojos basadas en la reflexión especular de la cornea.

John Daugman [21] usa un algoritmo que mediante una cámara que toma una fotografía del iris crea códigos digitales basados en patrones únicos de éste. El sistema no ha fallado en 6 años y hoy en día es implementado en aeropuertos importantes.

Jian Fu, H. John Caulfield, Seong-Moo Yoo y Venkata Atluri [23] sugieren que los patrones espaciales del iris son más complejos que los de las huellas dactilares por lo que con filtros artificiales de colores puede proveer un discriminante ortogonal

para el discriminante espacial de patrones. También aseveran que se pueden combinar estos discriminantes de tal modo que se mejoran los resultados.

2.3.1.2 Forma de las Manos

Ajay Kumar y David Zhang [10] proponen identificar las palmas de las manos mediante tres impresiones simultáneas para elevar la eficacia con respecto a una sola.

Wei Xiong, Kar-Ann Toh, Wei-Yun Yau y Xudong Jiang [9], se basan en las Transformaciones Euclidianas para separar y reconocer múltiples dedos rígidos, e introducen un modelo elíptico para representar los dedos y buscar la rápida alineación de éstos.

Connie Tee, Jin Andrew Teoh Beng Ong, Michael Goh Kah Ling y David Ngo Chek [19] proponen un sistema autómata que capture automáticamente y alinie las imágenes de la mano para el procesamiento. Las técnicas usadas son:

-centrarse en el análisis del componente principal (PCA)

-análisis discriminativo de lo captado (FDA)

-análisis de componentes independientes (ICA)

Las imágenes son descompuestas en diferentes subbandas de frecuencias y la mejor de estas subbandas es seleccionada para un posterior procesamiento.

2.3.1.3 Detección del Contorno del Rostro

Dario Maio y Loris Nanni [11] centran su atención en números pseudo-aleatorio que dan un ratio de error igual a cero al ser combinados con una característica biométrica (en este caso reconocedores de rostros). Cuando los números concuerdan con las características biométricas de la persona, no hay ningún error, y ésta es identificada.

Hay otros estudios en los que se plantea hacer el reconocimiento del rostro mediante el análisis y la combinación de imágenes de luz visible e imágenes de luz infrarroja.

Zuo, Fei ,De y Peter H. N. [15] plantean diseñar e implementar un sistema de reconocimiento de rostro, confiable y de bajo precio. Este sistema está basado en un procesamiento tipo “pipeline”, el cual consiste en:

-reconocimiento de rostro paso por paso

-extracción de rasgos faciales para una normalización del rostro.

-reconocimiento del rostro por un análisis discriminativo. Este sistema experimental tiene un ratio de reconocimiento del 95%.

Rong Xiao ,Ming-Jing Li John , y Hong-Jiang Zhang [16] proponen tres pasos para el reconocimiento:

-se aplica un filtro lineal para realzar la ejecución (captura de la imagen y posterior procesamiento de la misma) y remover partes del rostro que no son necesarias.

-mediante un algoritmo se combinan lo hallado con el filtro con una estructura jerárquica.

-se aplica otro filtro y se hace un procesamiento de la imagen para ver la proyección final.

2.3.1.4 Reconocimiento por Huellas Dactilares

Xiong Wei, Toh Kar-Ann, Yau Wei-Yun, y Jiang Xudong [9] realizan una localización secundaria derivada de una información mínima relativa. Por medio de una técnica se ve la correspondencia para obtener uno a uno los rasgos secundarios, después se hace un balance de los cambios hechos entre la maximización del número de correspondencias y minimización del total de los rasgos entre las huellas digitales de usuarios que deseen acceder y las huellas digitales referenciales. Este enfoque tiene la ventaja de ser compatible con bases de datos ya existentes.

Damon L. Woodard y Patrick J. Flynn [22] presentan la superficie de los dedos en 3D como un rasgo de identificación. En esta superficie se representa el dedo índice, el medio y el anular para ser comparados.

En contraposición, según la publicación hecha por David Cyranoski, Tsutomu Matsumoto [20], se afirma que la identificación de un individuo por medio de sus huellas digitales es ineficiente y se puede engañar fácilmente al sistema.

Sin embargo, se podría decir que este procedimiento es quizá el mejor en lo que a detección por huellas digitales se refiere. Todavía no está en el mercado pero estudios indican que es muy confiable y fácil de usar. La forma de trabajo es de transmitir ondas acústicas y medir la distancia basada en la impedancia del dedo, la superficie, y el aire. El ultrasonido es capaz de penetrar polvo y residuo entre la superficie y el dedo.

Las huellas digitales pueden ser de diferentes formas, en forma de arcos, espirales, círculos; siendo este último caso el 60% de las veces. En la siguiente figura se muestran los tipos más comunes de huellas:

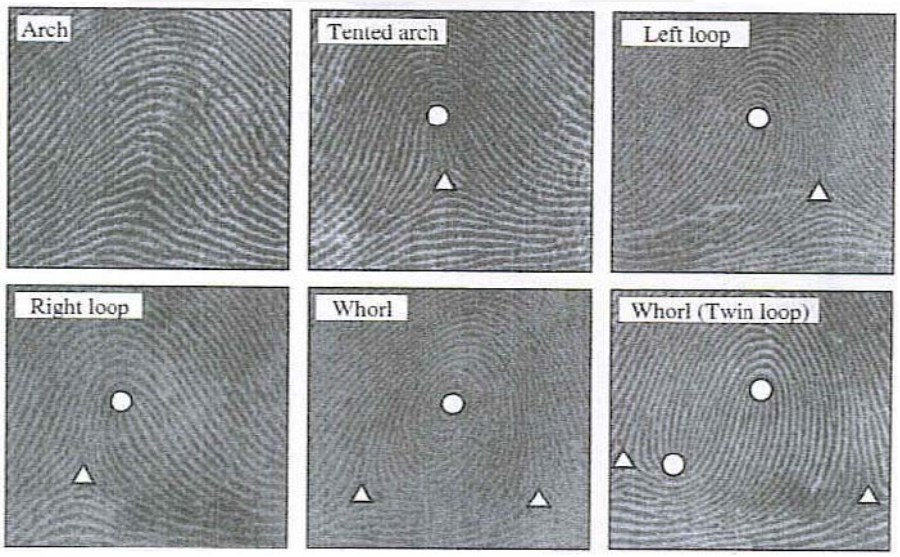


Figura 2.1: Diferentes tipos de huellas dactilares: arriba, de derecha a izquierda: arco, posible arco, espiral hacia la izquierda; abajo de derecha a izquierda: espiral hacia la derecha, círculo, dos espirales juntos. [38]

Captura: El lector en donde se pone el dedo para ser capturada la imagen contiene un chip de silicón que está provisto de una lámina con un arreglo de micro-capacitores. La superficie de la piel sirve como una segunda capa para cada micro-capacitor. Entonces se forma entre estas dos superficies (la del dedo y la de las láminas de los capacitores) una pequeña carga (dependiendo de la distancia) porque el espacio de aire actúa como un medio dieléctrico.

Después de hacerse la captura, la imagen se debe digitalizar. La huella dactilar del dedo presenta protuberancias y valles, al ser apoyada en la lámina que contiene el arreglo de capacitores se van obteniendo diferentes valores de capacitancia; los cuales son medidos y luego convertidos en píxeles de diferente intensidad para crear una imagen digital.

Una vez digitalizada la imagen se guardan detalles llamados “Minucias” y son guardadas en una plantilla para la posterior verificación del individuo. Estas “Minucias” son partes donde se juntan dos o más protuberancias, donde una protuberancia termina abruptamente, o cuando de una protuberancia salen dos o más protuberancias.

Para la captura hay diferentes sensores (lectores), pueden ser capacitores, ópticos, multiespectrales (usan diferentes longitudes de onda), por ultra sonido, entre otros.

En el siguiente diagrama de bloques se puede apreciar cómo es que se hace la

captura de la huella dactilar a través de un sensor. Esta imagen capturada es convertida o digitalizada por medio de un convertidor análogo/digital (A/D converter), luego por medio de una interfase la señal llega al computador para ser analizada y dar la respuesta al usuario.

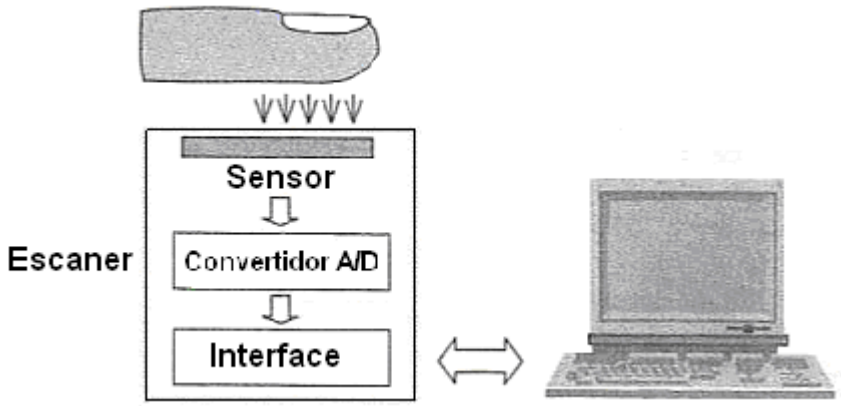


Figura 2.2: Diagrama de bloques del proceso que va desde la captura de la imagen hasta la respuesta al usuario. [38]

2.3.1.5 Reconocimiento por Voz

Hoy en día los procesadores de reconocimiento de voz son más precisos y vienen acompañados con mejores herramientas para hacer más fácil la conexión a cualquier producto [25]. El reconocimiento de voz puede ser dividido en tres clases: locutor independiente (SI), locutor dependiente (SD), y verificación de locutor (SV). Los sistemas basados en el reconocimiento de voz deben de alguna forma avisar al usuario que ha escuchado el comando correcto y está listo para más información.

En Octubre del 2005 Schultz y su colega Alex Waibel [40] demostraron el primer traductor automático que podía tomar señales eléctricas del rostro y de los músculos de la garganta y convertirlos en una técnica llamada reconocimiento de habla “sub-vocal”. Si bien esta técnica solamente capta una correcta secuencia de fonemas en el 62% de las veces, es un logro significativo.

2.4 Ventajas y desventajas de los sistemas biométricos

Después de analizar las diferentes formas de adquisición de datos para la posterior identificación de la persona, se desprende que si sólo se toma el reconocimiento de huellas digitales se puede engañar a la máquina por lo que no es muy seguro, o simplemente no se obtiene una buena imagen, ya sea por el sudor de los dedos, por polvo, y otros. La ventaja con respecto a otros métodos radica en el precio, y que este indicador ha sido utilizado por los seres humanos para identificación personal por más de cien años, representando en la actualidad una de las tecnologías biométricas más maduras, inclusive considerada como prueba legítima de evidencia criminal en cualquier corte del mundo.

Por otro lado, gracias a muchos estudios previos se ha demostrado que para cada persona el iris proporciona una única estructura (hasta en personas gemelas es distinta), para poder hacer el cálculo debido y de esta forma poder identificar a la persona. En contraposición con las huellas digitales, el iris puede ser captado hasta de 1 metro de distancia. Los patrones del iris son estables y solamente cambian de

manera notoria cuando la pupila se abre y se cierra como reacción a la luz. Este sistema ya es implementado en muchos aeropuertos de todo el mundo con gran aceptación y un alto grado de confiabilidad. Una desventaja es que el uso de este método es complicado debido al alto costo y la poca aceptabilidad por parte de las personas en algunas situaciones, puesto que puede tomar un tiempo razonable todo el proceso.

Con respecto a la detección del rostro, si bien es muy confiable, es más costoso que el de huellas dactilares y el sistema tiende a fallar cuando hay cambios en el ambiente (más luz o menos luz) o cambios en el rostro (podría ser una cicatriz).

En lo que al reconocimiento de la mano se refiere, también es un método que tiene varios años, e incluso fue usado como sistema de seguridad en los juegos olímpicos de 1996. En la revista MILTECH [29] se dice que es un buen sistema, fácil de usar, fácil de adaptar a otros sistemas, y puede ser el primer paso para otros muchos proyectos biométricos.

En cuanto a los sistemas de detección por voz se les puede engañar fácilmente con grabadoras, lo que representa un problema. Una posible solución sería que los usuarios digan frases diferentes cada vez que lo usen y que el sistema reconozca si ha habido una frase repetida, pero esto incrementaría el tiempo para la verificación. La ventaja es que es el sistema más barato en comparación con todos los demás.

A pesar de que los sistemas biométricos son los sistemas de seguridad más confiables el mayor problema que se presenta es poder llegar a tener un 100% de efectividad, ya que para cualquier método siempre está la probabilidad de que se autorice el acceso a una persona no autorizada, ó viceversa, que se prohíba el acceso a una persona autorizada.

Una forma de hacer más eficientes los sistemas biométricos es haciendo combinaciones de técnicas (por ejemplo usar huellas dactilares y reconocimiento de rostro). [5] [40]

2.5 Software para la captura de imágenes y posterior análisis

Para la captura de datos se necesita una cámara o un scanner. Posteriormente la imagen es almacenada en un computador para luego ser analizada.

El análisis consiste en procesar la imagen de tal manera que se encuentre un patrón o característica propia de cada individuo, luego se compara la imagen con las imágenes que se encuentran en la base de datos.

Para llegar a tener un modelo matemático primero se deben hacer pruebas, inicialmente se trabaja con el programa “Matlab”, con el cual se puede hacer el procesamiento de imágenes necesario después de la captura respectiva. De las pruebas realizadas con diferentes métodos se va viendo cuál de estos es el óptimo para poder tener un modelamiento matemático final con el cual se va a trabajar.

Debido a que el “Matlab” no es un programa que trabaja muy rápido, para la implementación de estos sistemas se debe buscar otro software que cumpla con las condiciones de operación (en este caso particular la velocidad de procesamiento del programa es muy importante). Un ejemplo es el Visual C.

CAPITULO 3

CONSIDERACIONES PARA EL DISEÑO

3.1 Huellas Dactilares

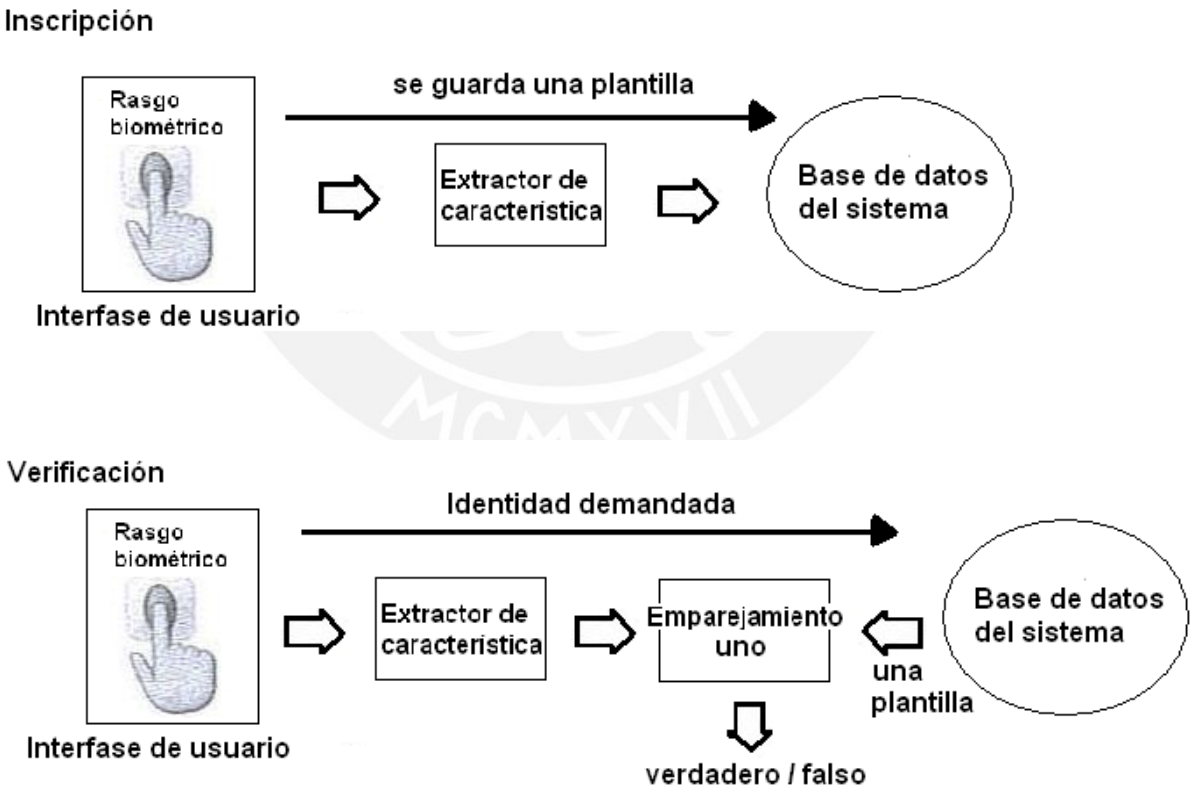
Los sistemas biométricos basados en el reconocimiento por las huellas dactilares son actualmente los más usados en el mundo; en el año 2002 [40], según el Grupo Internacional Biométrico, alcanzaron la cifra del 52.1%, dejando en segundo lugar con 12.4% a los sistemas biométricos basados en el reconocimiento del rostro.

Otro dato importante con respecto a este tipo de reconocimiento es que tiene un muy buen balance de todas las propiedades que se deben evaluar a la hora de proponer un sistema biométrico, como son:

- Universalidad: Se entiende por un sistema biométrico que es común a la mayoría de personas.
- Funcionabilidad, Ejecución: Se entiende por la eficacia con la que trabajan.
- Aceptabilidad: Se entiende por el fácil uso de estos sistemas (son rápidos y cómodos a la hora de capturar los rasgos biométricos).
- Permanencia: Se entiende por un sistema que tiene mucho tiempo en el mercado (en este caso particular, es el mas antiguo); y se sigue desarrollando.
- Características: Se entiende por aplicaciones específicas demandadas por los diferentes usuarios.

Los rasgos o detalles en una huella dactilar son permanentes, incluso si temporalmente cambian debido a cortes o variaciones en la piel debido a condiciones climatológicas. Son los sistemas biométricos más antiguos, por lo tanto tienen cierto grado de madurez tecnológica y los sensores cada vez son menos costosos.

Como se puede apreciar en la Figura 3.1, tanto para los procesos de registro por primera vez en el sistema, de verificación, y de identificación, se sigue el mismo procedimiento:



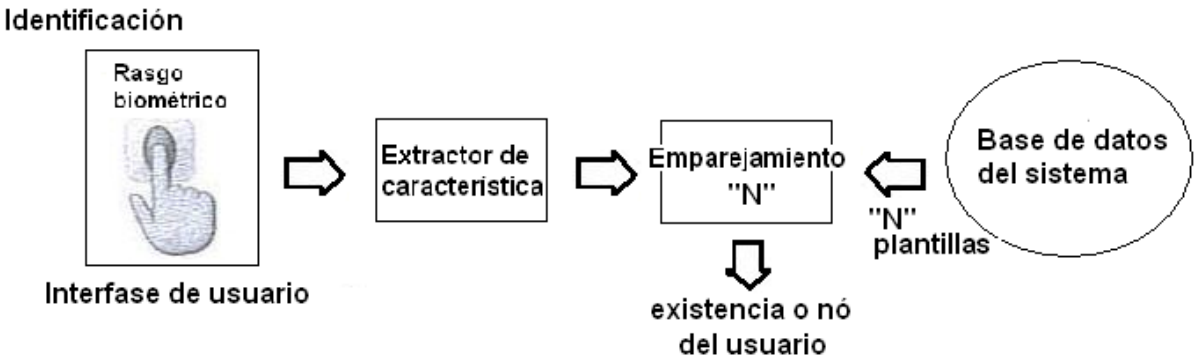


Figura 3.1: Diagramas que muestran los procesos de registro, verificación, e identificación [40]

3.2 Diseño

Teniendo en cuenta lo anterior se plantea una solución:

Solución: Ingreso al campus universitario por parte de todo el personal autorizado (alumnos, personal docente, personal administrativo, practicantes, etc.)

Para entender mejor el funcionamiento se presenta el diagrama de flujo:

Caso 1 (cuando la persona sí pertenece a la universidad)

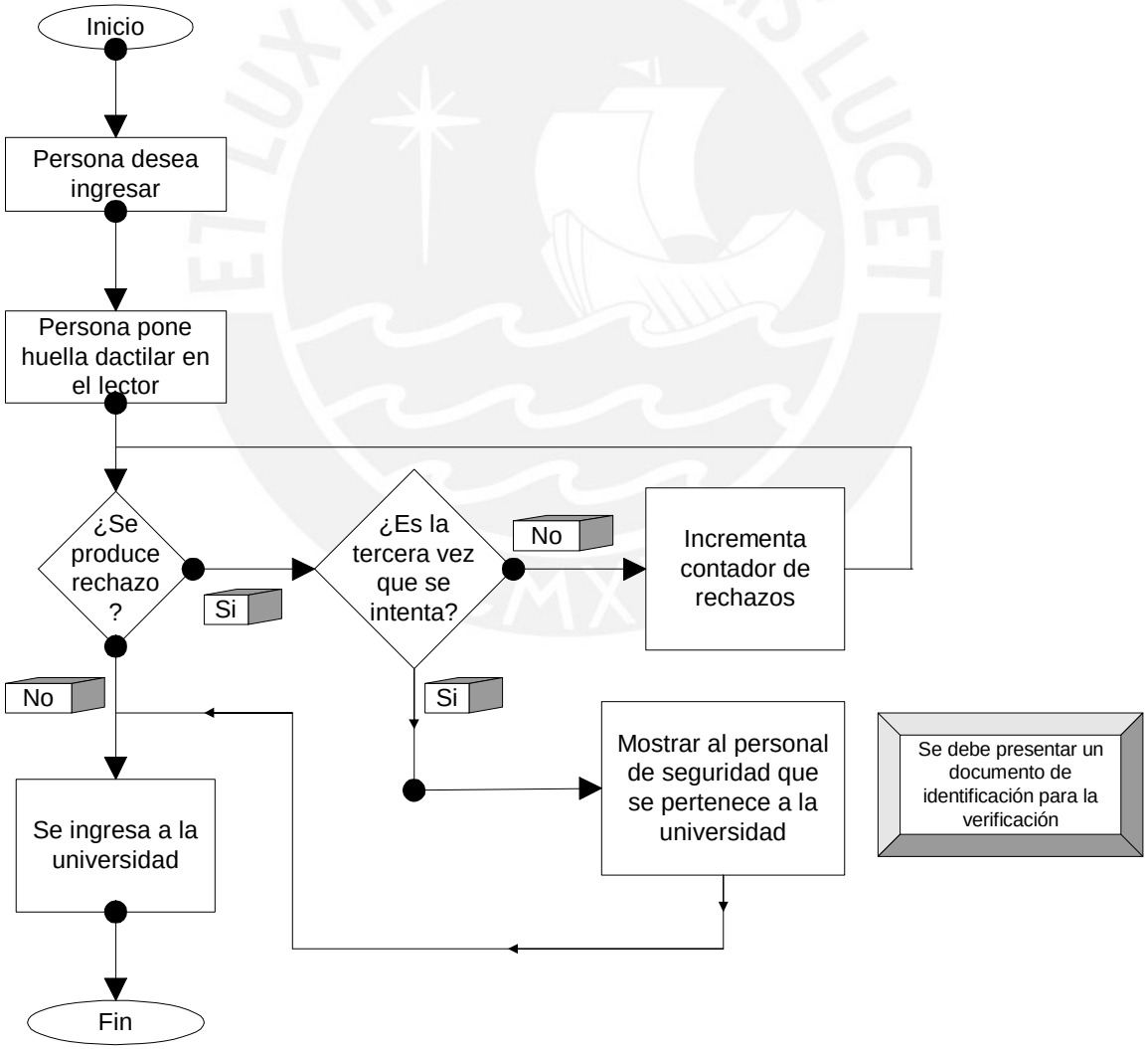


Figura 3.2: Se muestra el procedimiento a seguir para ingresar a la Universidad Católica, en el caso de que la persona sí pertenece a ésta.

Hay que tomar en cuenta lo siguiente:

Cuando se produce un rechazo se vuelve a intentar, siendo el número de intentos ya predefinido por las personas a cargo; en este caso se tomaron tres intentos.

Caso 2 (cuando la persona no pertenece a la universidad)

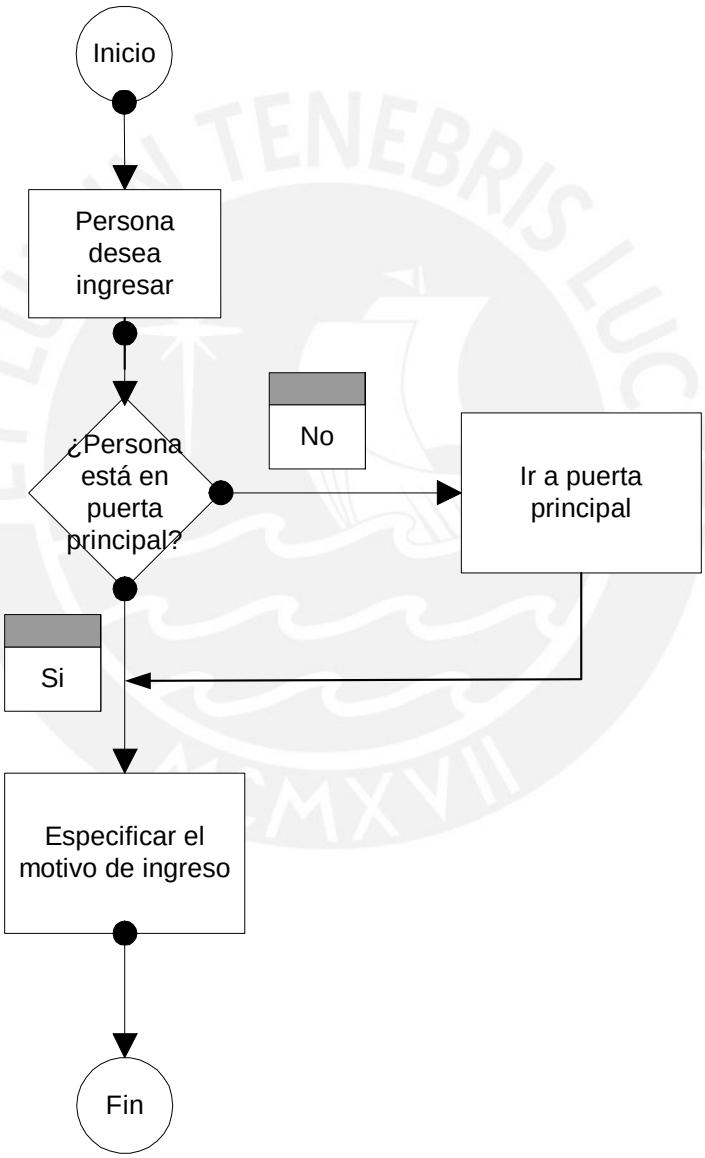


Figura 3.3: procedimiento para ingresar a una universidad sin pertenecer a esta.

Para poder llevar a cabo esta aplicación en la universidad, es necesario analizar el estado actual de la red tanto en la universidad como en sus locales externos. Es necesario entender cómo está distribuida la red:

En la Dirección de informática (DIRINFO), lugar en donde se opera toda la red de la universidad y en donde están los servidores principales, las base de datos, entre otras cosas; se encuentra el “switch principal” y es a donde van todas las conexiones de la redes LAN, WAN, PSTN, INTERNET.

En la siguiente figura se muestra la red descrita:

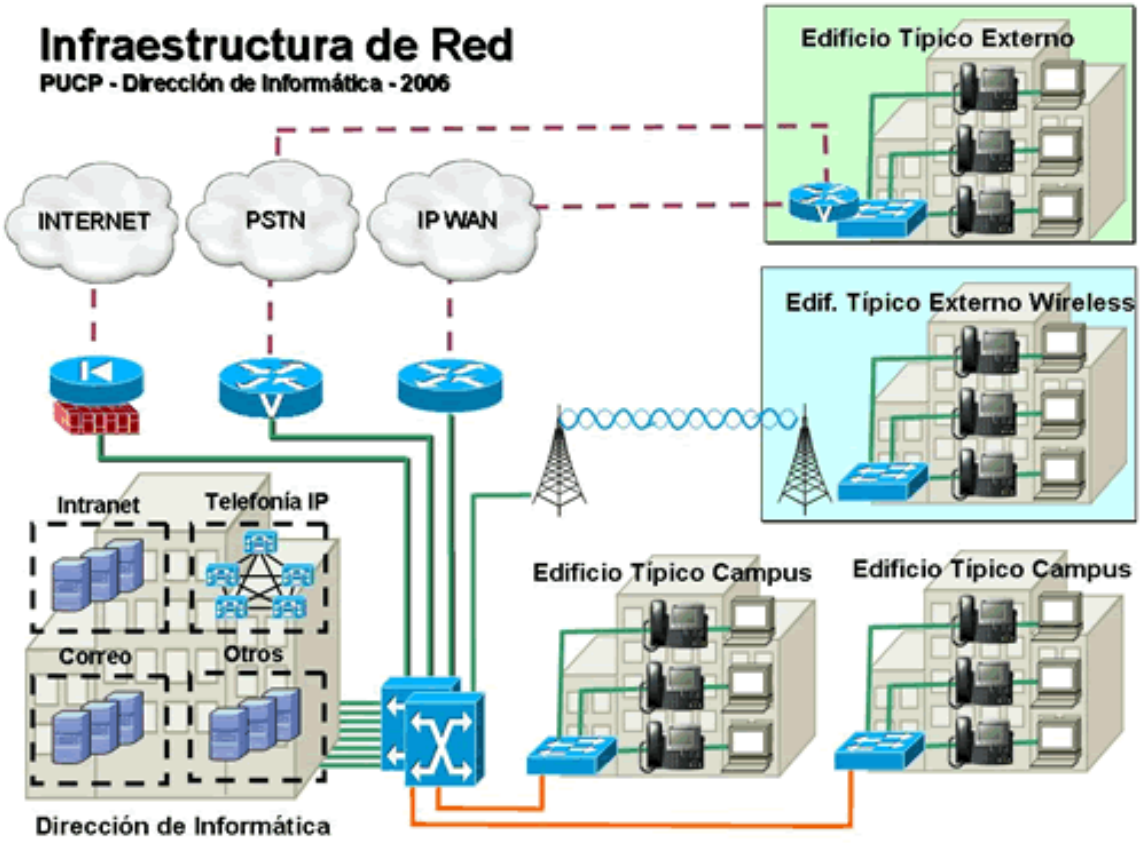


Figura 3.4: Infraestructura de Red PUCP [39]

Todas las conexiones desde cada edificio del campus hacia la central están hechas mediante fibra óptica de 6 hilos, usándose solamente 2 hilos.

La fibra llega a los edificios a un distribuidor principal en donde hay un switch y de ahí todo el cableado va hacia las máquinas (computadoras, impresoras, entre otros). Esto último se realiza mediante cableado estructurado UTP.

Por tanto teniendo en cuenta esta información, en cada entrada de la universidad hay conexiones ya hechas, listas para ser usadas. Con esto la implementación de los sistemas planteados sería algo factible de hacer debido a que existe una red de donde partir. Según la información adquirida durante este presente trabajo de investigación, la mayoría de estos productos biométricos vienen con muchas plataformas de trabajo y diversos tipos de conectividad (sea mediante USB, RS232, entre otros).

Los aparatos biométricos estarían en cada puerta, trabajando en red. La persona que desea ingresar tendrá que identificarse poniendo su huella dactilar en el lector, la información recuperada será enviada hacia la central en donde está la base de datos de todas las personas autorizadas a ingresar. Según el resultado (positivo o negativo) la persona estará o no autorizada a ingresar al campus.

La distribución de los aparatos en el campus de la Pontificia Universidad Católica del Perú será de la siguiente manera:

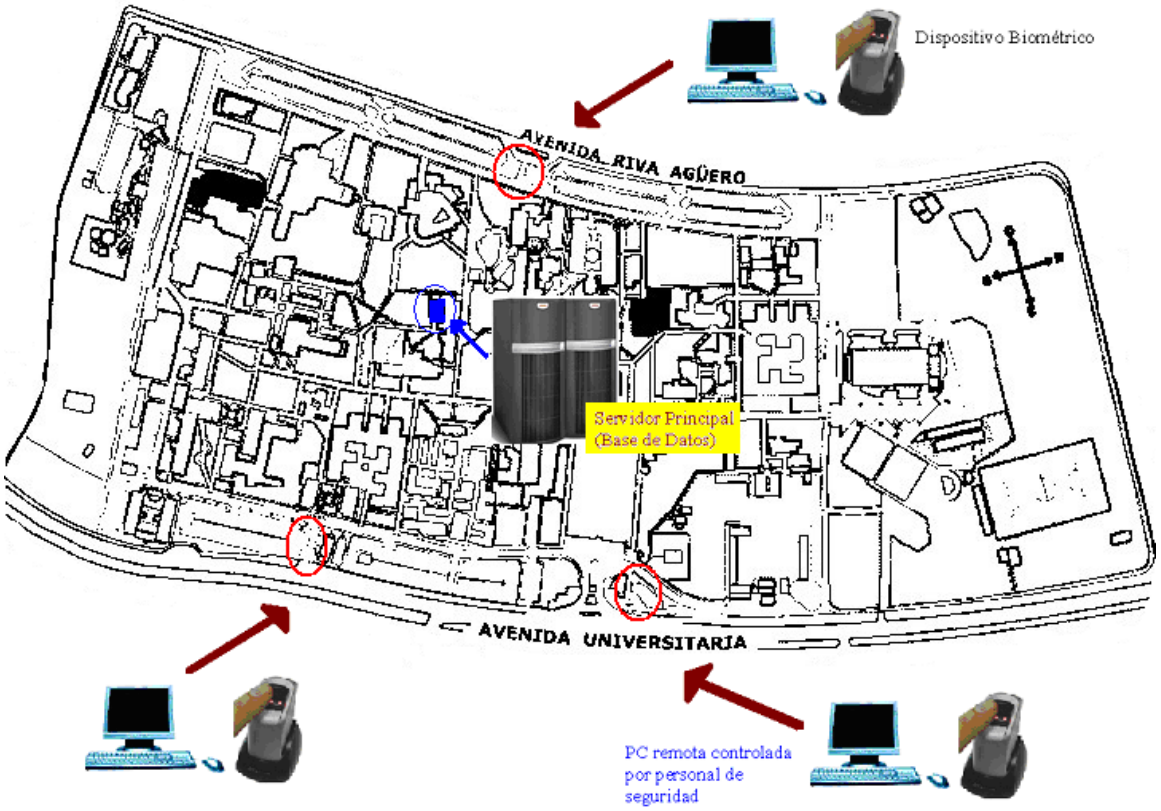


Figura 3.5: Disposición de los elementos en el campus de la Universidad católica, en cada puerta habrán capturadores biométricos, un computador y personal de seguridad.

3.3 Tabla Comparativa

Por último, es necesario conocer algunas características de los aparatos biométricos para captura de huellas dactilares que han sido objeto de estudio para la presente implementación. En la tabla 3.1 se muestran estas características y también se mencionan productos que no son idóneos para esta aplicación. Hay que considerar que la capacidad de usuarios sugerida en la tabla está tomada en cuenta en torno a un solo aparato y con un software de aplicación se puede ampliar esta capacidad. En el caso de la aplicación sugerida, ésto podrá variar de acuerdo a la cantidad de aparatos que se van a adquirir.

Fabricante o comercializador	Modelo	Costo	Resolución en dpi	Capacidad de de usuarios	Software desarrollo	Aplicación
Superma	BioEntry Pass	$780.00	500	9000 a más con software	si	Todos los alumnos
Jc Technologies Systems SAC	Fingermatch FM-200U	$980.00	500		si	personal administrativo y/o profesores
Sagem Défense Sécurité	Morphosmart: Licencias: Verif MorphoSoft IdentLite MorphoSoft IdentPlus	$795.00 $1109.00 $5048.00	500	20000 a más con software	si	Todos los alumnos
Syno Biometrix	BSS-1B		513	99		unas cuantas personas
Sagem Défense Sécurité	MorphoAccess MA200	$1883.77	500	800 sin SW 48000 con SW	si	Todos los alumnos / personal administrativo
Jc Technologies Systems SAC	Finger 007	$1550.00		4500	si	personal administrativo y/o profesores
Biometrix INT	FM-FC	EU 190	500	9000	si	Alumnos de algunas facultades
Jc Technologies Systems SAC	Magic Print 4500	$1330.00		90		Profesores o personal administrativo
Jc Technologies Systems SAC	BF 660C	$1100.00		250		personal administrativo y/o profesores
Biometric International	FIM01			1000,2000,4000	si	personal administrativo y/o profesores
Bometría Aplicada	U4000B	$89.00	512			unas cuantas personas
Synel Industries	SY-780/A					personal administrativo y/o profesores
Hit Corporation	Magic Plus 4200			500, 1000		personal administrativo y/o profesores
D2 Technology Limited	Finger Pass KF-2000	$308.00		1000, 4000		Alumnos de algunas facultades
Granding Technology Co.	X628	$308.00		1500		personal aministrativo y/o profesores
Granding Technology Co.	Biosh-F7	$374.00		500		Alumnos de algunas facultades
BioEnable Technologies	iScan V100	$350.00		100		unas cuantas personas
BioEnter International Inc.	BFS 310	$449.00		99		unas cuantas personas
D2 Technology Limited	BioSH-TA2	$493.00		1000		personal administrativo y/o profesores

Tabla 3.1: Tabla comparativa de costos de algunos aparatos biométricos

CAPITULO 4

ANALISIS DE DISEÑO Y PROPUESTA FINAL

4.1 Productos a considerar

Análisis:

Para la aplicación deseada se deben tomar en cuenta muchos factores antes de adquirir cierto dispositivo biométrico, tales como:

- Resolución
- Área del sensor
- Número de Píxeles
- Profundidad de color
- Calidad de imagen

Resolución:

Indica los dpi (número de puntos o píxeles por pulgada), siendo 500 dpi la mínima resolución para tener un buen producto, sin embargo, es probable que un algoritmo pueda identificar las minucias en los modelos de las huellas capturadas con resoluciones de hasta 300 o 250 dpi.

Área del sensor:

Es muy importante puesto que cuanto más grande es, mayor es el número de valles y protuberancias que se van a encontrar para poder hacer el posterior análisis. Una

medida óptima para poder capturar todo el dedo es de 1 x 1 pulgadas cuadradas. Pero mientras más grande es esta área el precio también se incrementa.

Número de píxeles:

Este valor es simplemente la multiplicación de la resolución (en dpi) a la que se está trabajando y el área (altura x ancho).

Profundidad de color:

En el caso de trabajar con huellas digitales, los colores no son considerados necesarios y solamente se requiere niveles de grises, entonces este valor se puede denotar como el número de bits usados para codificar el valor de cada píxel. Un valor estándar es el de 8 bits (que nos permite alcanzar hasta 256 niveles de grises).

Calidad de imagen:

Cuando los dedos están secos o mojados, o tienen cortes o las protuberancias son poco profundas, la calidad de la imagen es pobre por lo que se debe considerar lectores con ciertas habilidades.

A continuación se detallan algunos productos de interés según el tipo de solución planteada:

4.1.1 BioEntry Pass

Figura 4.1: Lector de huella dactilar, BioEntry Pass [35]

Los equipos Bioentry Pass están diseñados para la aplicación requerida inicialmente (todos los alumnos activos). Consiste en la validación de acceso por huella dactilar exclusivamente. El equipo puede acumular hasta 9000 plantillas de huellas para reconocimiento. Pero conectados a un servidor de validación, es posible llegar a cantidades mayores.

En red el tiempo promedio de reconocimiento 1:1000 es de aproximadamente 1 segundo. El costo de cada equipo, con lector FC (de barrido de huella) es de $600 incluido impuestos locales. Se aplican descuentos por cantidades mayores a 3 unidades. En el caso de que se requiera el software de desarrollo, se puede adquirir un BioEntry Pass SK que incluye un equipo, soporte y software SK con rutinas en C++ y aplicaciones desarrolladas por tan solo $ 780 incluido impuestos.

Hay que agregar que el lector FC ha demostrado una gran resistencia a vandalismo y uso intensivo.

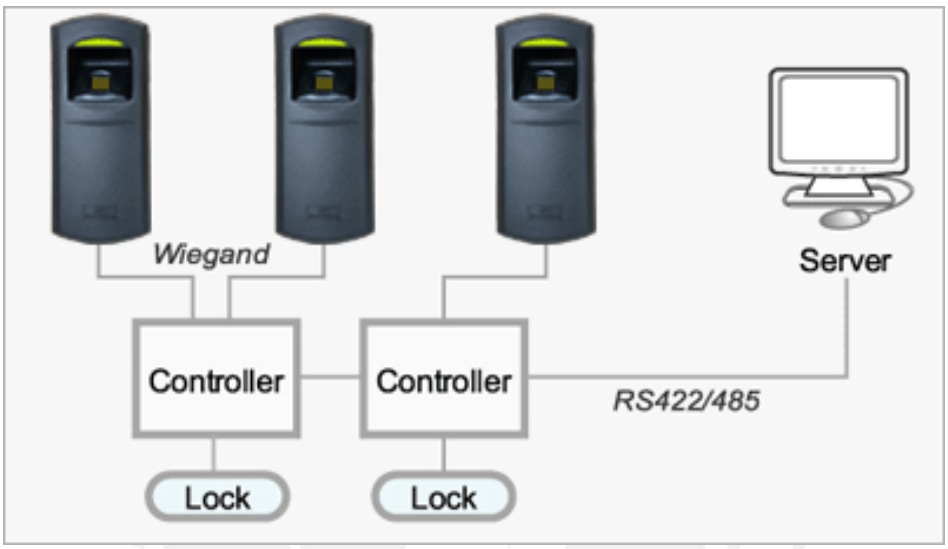


Figura 4.2: Diagrama de una red utilizando el lector BioEntry Pass [36]

4.1.2 LECTOR DE HUELLA DIGITAL FM-200U

Figura 4.3: Lector de huella digital FM-200U [37]

Modo de operación

El software de verificación dactilar permite, en una primera fase, registrar los datos y huella digital de cada empleado, los ya existentes y también personal nuevo que vaya ingresando. Cuando los empleados empiecen a llegar deben digitar un código en el teclado de la PC y luego colocar su huella en el lector, si la verificación es correcta se generará una marcación con nombre, fecha y hora. Si la verificación es incorrecta, el sistema pedirá se ingrese nuevamente el código. El precio de este aparato es de $330.00 incluido IGV y el Kit de desarrollo $650.00

Características

- Sensor óptico de huella digital CMOS/Microprocesador ASIC integrado
- Resolución óptica: 500 dpi niveles de grises
- Conexión a PC por puerto USB
- Tamaño de la minucia - 256 bytes
- Plataformas de operación WIN98/2000/XP
- No es compatible con el modelo FM100U

Algunas características operativas

- Operación en Modos de Verificación e Identificación

- Comunicación hacia la PC por Puerto USB

- Licencia de uso: Licencia única sin límite en el número de huellas.

- Interfaz de Programación: Vía DLL

- Capacidad de integrarse con redes Ethernet permite su conexión a plataformas NOVELL,WIN 95, WINDOWS NT, UNIX., ORACLE.
- Validación remota: Valida el acceso de los usuarios remotos por Internet, Intranet, Extranet o por Red Privada Virtual (VPN) como si estuvieran ubicados localmente.

Esta aplicación es disponible mediante desarrollo usando SDK.

Este producto también cuenta con un Kit de desarrollo, para poder trabajar con un mayor numero de personas, se puede programar en Visual Basic, visual C++, y DLL el precio total del producto estaría alrededor de los $650.00

4.1.3 MorphoSmart MSO300

Este producto es desarrollado y producido por Sagem Défense Sécurité [39], el líder mundial en sistemas de identificación de impresiones dactilares, el MorphoSmart MSO300 es un escáner de captura de huellas dactilares preciso, compacto, durable y fácil de integrar en aplicaciones de identificación automática de las impresiones dactilares.

El MorphoSoft es compatible con las plataformas de programación Active X de Windows, lo cual permite integrarlo fácilmente en aplicaciones de registro, autenticación e identificación automática de personas. El entorno de programación cumple con las normas técnicas BioAPI, optimizando los tiempos de puesta en marcha de los proyectos. El MorphoSoft está disponible en diversas licencias

biométricas diferenciadas, que permiten hacer procesos de verificación (1:1) e identificación (1:N) . Por ejemplo, la licencia identificación automática (1:N) MorphoSoft IdentPlus permite identificar a una persona entre 20,000 personas con sólo poner el dedo en tiempos extremadamente cortos; típicamente menores a 1 segundo en una computadora convencional.

Al hacer un análisis de estos productos nos damos con la sorpresa de que no son hechos para trabajar con grandes volúmenes, salvo uno (el MorphoSmart MSO300); en cambio si se quisiera trabajar con grandes volúmenes se deberá usar un software especial.

4.1.4 Software de desarrollo: Verifinger SDK

Verifinger SDK está basado en la tecnología de Verifinger y está previsto para sistemas biométricos de desarrollo e integración. Este permite un desarrollo rápido de la aplicación biométrica usando funciones de Verifinger DLL o de la misma librería de Verifinger , el cual asegura una alta confiabilidad en la identificación de la huella digital en los modos de emparejar: 1:1 y 1:N, una velocidad de comparación de 30,000 huellas digitales por segundo. Verifinger puede ser fácilmente integrado al sistema de seguridad del cliente. El integrador tiene un control completo sobre las entradas y salidas de la data del SDK. Es por ello que las funciones del SDK pueden ser usadas en conexión a cualquier scanner, usuarios de interfase o base de datos.

Existen varios tipos de Verifinger 4.2 SDK:

- **Verifinger 4.2 Standard SDK:** provisto para la mayoría de sistemas biométricos que desarrollan y permiten el uso de aplicaciones biométricas de Windows o Linux. Incluye una licencia para Verifinger 4.2 DLL/ instalación en biblioteca, Módulo de integración para MySQL (para Linux), uso de la biblioteca para aplicaciones de la muestra de Verifinger con códigos de fuente (para Windows y Linux), conductores de exploración de la huella digital y software de documentación.

- **Verifinger 4.2 Extended SDK:** provisto para quienes les gustaría empezar con un desarrollo rápido de su red de sistema biométrica cliente/servidor. Incluye todas las características del Verifinger 4.2 Standard SKD, además incluye 3 Verifinger DLL/licencia para la instalación de biblioteca, componentes Active X para el desarrollo de cliente/servidor (sólo para MS de Windows) y componentes para el uso de la muestra de aplicación (con códigos de fuente).

- **Verifinger 4.2 Library SDK:** provisto para proyectos de biometría grandes. Este SDK contiene bibliotecas de Verifinger para Windows y Linux sin protección para la copia.

Verifinger 4.2 Paquete del código fuente: también está disponible y contiene verifinger 4.2 código fuente de algoritmos y documentación. El código fuente de Verifinger 4.2 está escrito en ANSI C de manera bien estructurada y documentada.

Existen otros softwares de desarrollo tales como:

MegaMatcher SDK
VeriFinger SDK
FingerCell EDK
VeriLook SDK

4.1.5 Morpho Access MA20

Figura 4.4

Este producto, al igual que el Morphosmart MSO300 es desarrollado y producido por Sagem Défense Sécurité [39] el líder mundial en sistemas de identificación de impresiones dactilares; por lo que presenta las mismas prestaciones. Algunas características que pueden ser resaltadas son:

-Sistema biométrico más rápido y preciso del mundo.

- Identifica al trabajador y registra su hora de marcación con sólo poner el dedo (no requiere códigos o tarjetas).

- Registra la fecha, hora y datos del trabajador para cada marcación.
- Soporta dedos en malas condiciones (con sequedad, humedad, cicatrices, suciedad, etc.).
- Altamente tolerante a la mala posición del dedo (rotación y traslación**)**.
- Es fácilmente integrable con cualquier sistema informático de control de asistencia.
- Permite diferenciar cuatro tipos de eventos de asistencia (entrada, salida, entrada intermedia y salida intermedia).
- Cuando identifica al trabajador permite abrir una puerta automáticamente.

El MorphoAccess está dotado con comunicación Ethernet TCP/IP, lo cual permite descargar los reportes relativos a la asistencia (ingresos y salidas del personal) directamente a través de la red. Asimismo, cuenta con múltiples interfases de comunicación adicionales como RS-232 (serial), RS-422, Wiegand, etc. En forma complementaria, el MorphoAccess contiene un controlador de puerta incorporado, que permite la apertura automática de una puerta, sea esta eléctrica o magnética.

4.2 Diagrama final

Como se puede apreciar en la siguiente figura, así será la forma en que se ingresará a la universidad, el dispositivo biométrico estará conectado a la PC por medio de una interfase RS-232. La PC (que estará siendo usada por el personal de seguridad), se conecta con el servidor de la base de datos ubicado en la DIRINFO. Esta última conexión ya está implementada.

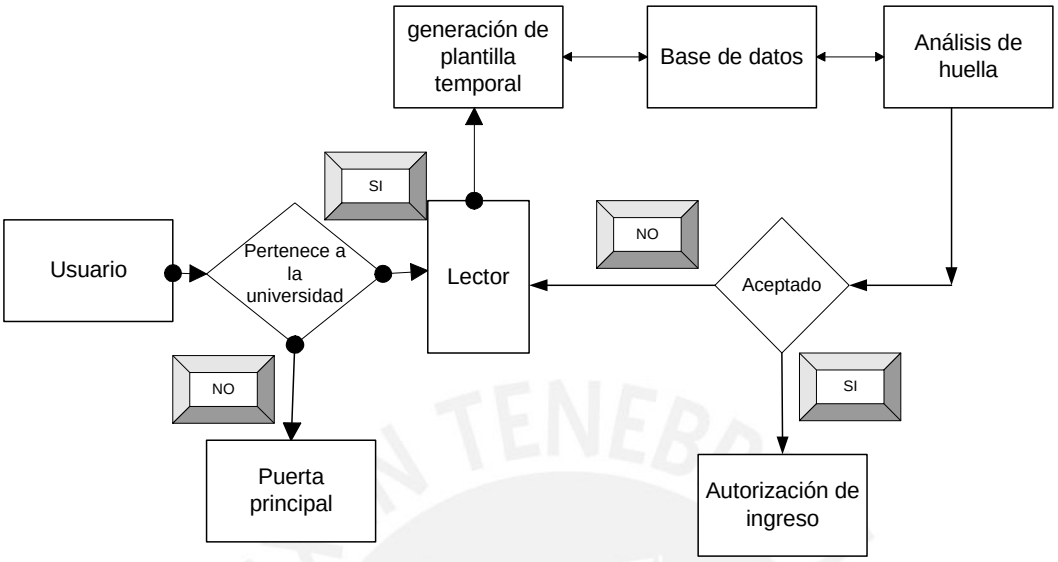


Figura 4.5: diagrama de flujo que muestra el proceso de ingreso a la Universidad Católica, incluidos los lectores biométricos

4.3 Instalación

Como se mencionó anteriormente en el capítulo 3, la red de la universidad ya está implementada por lo que simplemente los aparatos serán acomodados y conectados a esta red. El MorphoAccess MA200 cuenta con los protocolos TCP/IP o RS-232. En la siguiente figura se puede apreciar cómo será el diagrama de conexiones:

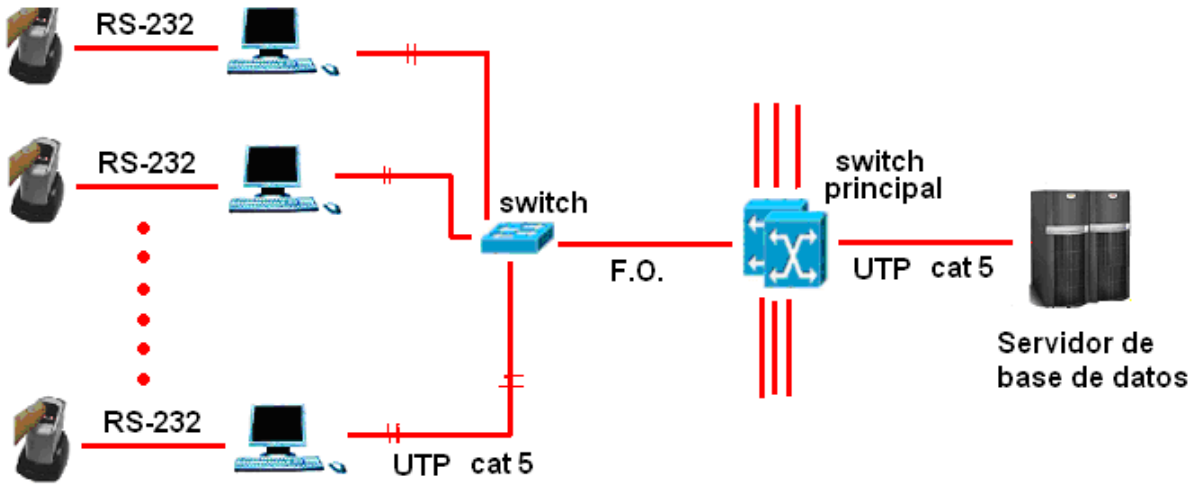


Figura 4.6: Diagrama de conexiones

4.4 Operación

Las personas que usarán este sistema serán las que pertenezcan a la universidad, monitoreadas por personal de seguridad. El MorphoAccess mantiene un registro detallado de los eventos en su memoria interna. Esta información puede ser descargada a través de la red y empleada en cualquier sistema de control de personal. En caso de falla del dispositivo, se dejará de usar por el periodo que tome repararlo y se usarán los otros dispositivos; si fuese el caso en que solamente hubiera un dispositivo en la puerta, se procederá a usar el método tradicional (pedir el carnét o presentar algún otro documento que pruebe la pertenencia a la universidad).

El personal de seguridad debe estar al tanto en caso de cualquier irregularidad, si la persona que intenta ingresar obtiene la autorización no habrá problema alguno pero si fuese el caso contrario deberá tomar medidas de corrección (hacer que la persona pruebe nuevamente o, comprobar que realmente pertenece a la universidad, o de lo contrario dirigirlo a la puerta principal).

Mantenimiento y periodo de garantía:

Al adquirir este producto se contará con soporte técnico durante un año por parte del proveedor, asimismo el periodo de garantía contra defectos de fábrica también es de un año.

4.5 Costos

La instalación del sistema no incluye obras civiles, carpintería u otras labores que correspondan ser realizadas por el cliente. La forma de pago es de la siguiente manera: 50% con orden de compra y el otro 50 % contra entrega. El plazo de entrega es inmediata o en tres semanas contra orden de compra (según disponibilidad de stock). El lugar de configuración se realiza en los locales de la institución.

En la siguiente tabla comparativa se puede apreciar el costo y algunas opciones:

	Costo ($) Unitario
Dispositivo biométrico	1883,77
Computador	400

Opción 1: un dispositivo y un computador por puerta

	Costo ($) Unitario	Cantidad	Costo Total ($)
Dispositivo biométrico	1883,77	3	5651,31
Computador	400	3	1200
		Total	6851,31

Opción 2: dos dispositivos y un computador por puerta

	Costo ($) Unitario	Cantidad	Costo Total ($)
Dispositivo biométrico	1883,77	6	11302,62
Computador	400	3	1200
		Total	12502,62

Opción 3: tres dispositivos y un computador por puerta			
	Costo ($) Unitario	Cantidad	Costo Total ($)
Dispositivo biométrico	1883,77	9	16953,93
Computador	400	3	1200
		Total	18153,93

Opción 4:cuatro dispositivos, un computador por puerta			
	Costo ($) Unitario	Cantidad	Costo Total ($)
Dispositivo biométrico	1883,77	12	22605,24
Computador	400	3	1200
		Total	23805,24

Figura 4.7:Tabla comparativa de costos del MorphoAccess, según algunas opciones

CONCLUSIONES

Los sistemas biométricos si bien no son eficientes al 100% (puede haber errores de 1 en cada 100 mil) son en este momento los sistemas de seguridad más eficientes y eficaces del mercado debido a que se trabaja identificando un rasgo físico y propio de una persona. Las aplicaciones de estos sistemas son muy variadas, las podemos dividir entre las tres categorías más tradicionales: forenses (identificación de criminales, terroristas, niños perdidos), comerciales (teléfonos celulares, acceso a Internet, tarjetas de crédito, entre otros casos), y en el ámbito gubernamental (tarjetas de identificación, pasaportes, tarjetas de seguro social, y otros casos).

Implementando sistemas biométricos no solamente a la Universidad Católica sino a otras instituciones, se estaría dando un gran paso en cuanto a contar con tecnología. Pero lo más importante es que se estaría aminorando sustancialmente algunos de los problemas que acusa la universidad como son los casos de falta de seguridad y comodidad para ingresar al campus.

Ahora, de estos sistemas hay muchos, para una aplicación de control de acceso lo ideal es combinar dos o más sistemas (por ejemplo, reconocimiento del iris y de la huella dactilar, o reconocimiento del rostro con reconocimiento de la voz, u otras posibles combinaciones); pero el más adecuado para el tipo de aplicación que se desea implementar en la Universidad Católica sería el de un sistema biométrico basado en las huellas dactilares, debido a que son los más cómodos económicamente y en los que más se ha trabajado y hecho estudios. Está claro que,

con el tiempo, las otras alternativas van a ir reduciendo su precio y fortaleciendo el grado de aceptabilidad por parte de los usuarios.

El buen funcionamiento en conjunto del sistema no depende solamente del dispositivo biométrico sino también del correcto uso del aparato por parte de los usuarios; para esto las personas deben necesariamente ser capacitadas.

Por último, cabe resaltar que los productos presentados en este trabajo no necesariamente son los únicos posibles para la aplicación que se desea llevar a cabo. Como la tecnología avanza y progresa rápidamente, antes de implementar uno de estos sistemas se debe hacer una buena búsqueda ya que hay infinitas aplicaciones, tanto requeridas por los usuarios como ofrecidas por estos productos.

RECOMENDACIONES

Como se sabe, a la Universidad Católica ingresa una gran cantidad de personas diariamente, entre alumnos, profesores, trabajadores, etc. Si tomamos en cuenta que cuando hay solamente guardias de seguridad en las puertas, el flujo de personas en hora punta es de aproximadamente de 3 a 4 personas por segundo, y que los lectores biométricos tardan menos de un segundo en reconocer a una persona (información adquirida durante este presente trabajo de investigación), una solución para este flujo de personas es tener entre 2 a 5 en lectores en una entrada, dependiendo de cual sea la puerta (Riva Agüero, Estudios Generales Ciencias, Principal). Con esta implementación no se perderá el flujo normal de entrada que actualmente tiene la universidad.

Para tener un buen sistema sería necesario contar con por lo menos 11 dispositivos repartidos de la siguiente manera:

-Puerta Riva Agüero: 2, para alumnos, profesores y personal administrativo (uno para la entrada y otro para la salida).

-Puerta de Generales Ciencias: 3 para alumnos y uno para profesores y personal administrativo (para entrada y salida)

-Puerta principal: 4 para alumnos y uno para profesores y personal administrativo (para entrada y salida)

Para el buen funcionamiento:

-No deberá estar situado en lugares donde reciba el sol o donde pueda mojarse en caso de lluvia.

-El lector deberá ser limpiado varias veces al día por el personal de seguridad.

FUENTES:

[1] "Active Video-Based Surveillance System",
IEEE SignalProccessing Mag. Vol.22 Num 2 March 2005, pp 25-37

[2] "Smart Video Surveillance"
IEEE SignalProccessing Mag. Vol.22 Num 2 March 2005, pp 38-51

[3] Hsu, Rein-Lein "Face detection and modeling for recognition"
Ph.D., Michigan State University, 2002, 178 pages; AAT 3064238

[4] Bang, Richard Doosung. "Fast techniques in object, edge, and face detection",
Ph.D., Princeton University, 1998, 156 pages; AAT 9920422

[5] Govindarajan, Rohin K. "Feature-level fusion in multimodal biometrics"
M.S.C.S., West Virginia University, 2004, 120 pages; AAT 1424304

[6] Lin, Cheng-Chung "Face detection in generic scenes: A biologically inspired approach"

[7] Balaji Ganeshan Dhananjay Theckedath, Rupert Young and Chris Chatwin
"Biometric iris recognition system using a fast and robust iris localization and alignment procedure"
[a]Department of Engineering and Design, School of Science and Technology, University of Sussex, Brighton BN1 9QT, UK
[b]Biomedical Engineering Department, D.J. Sanghvi College of Engineering, University of Mumbai, Mumbai-400 056, India

[8] Jindan Zhou and Mohamed Abdel-Mottaleb, "A content-based system for human identification based on bitewing dental X-ray images"
Department of Electrical and Computer Engineering, University of Miami, 1251 Memorial Drive, Coral Gables, FL 33146, USA

[9] Wei Xiong[a], Kar-Ann Toh[a], Wei-Yun Yau[a] and Xudong Jiang[b]
[a]Institute for Infocomm Research, 21 Heng Mui Keng Terrace, Singapore 119613, Singapore
[b]School of EEE, Nanyang Technological University, Block S1, 50 Nanyang Avenue, Singapore 639798, Singapore

[10] Ajay Kumar[a b] and David Zhang[b] "Personal authentication using multiple palmprint representation"
[a]Department of Electrical Engineering, Indian Institute of Technology Delhi, Hauz Khas, New Delhi, India
[b]Department of Computing, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong

Pattern Recognition, Volume 38, Issue 10 , October 2005, Pages 1695-1704

[11] Dario Maio and Loris Nanni "An efficient fingerprint verification system using integrated gabor filters and Parzen Window Classifier"
DEIS, IEIIT-CNR, Università di Bologna, Viale Risorgimento 2, 40136 Bologna, Italy

[12] Xin Chen, Patrick J. Flynn and Kevin W. Bowyer, "IR and visible light face recognition"
Department of Computer Science and Engineering, University of Notre Dame, Notre Dame, IN 46556, USA

[13] Xiong, Wei; Toh, Kar-Ann; Yau, Wei-Yun; Jiang, Xudong. Pattern Recognition, "Model-guided deformable hand shape recognition without positioning aids" Oct2005, Vol. 38 Issue 10, p1651, 14p-1664; DOI:10.1016/j.patcog.2004.07.008; (AN 18179622)

[14] Lerner, Eric J.. Industrial Physicist, Feb2000, Vol. 6 Issue 1, p20, 4p, 1 diagram, 1c; (AN 5517194)

[15] Zuo, Fei ,De With, Peter H. N. ," Real-time Face Recognition for Smart Home Applications"
IEEE Transactions on Consumer Electronics; Feb2005, Vol. 51 Issue 1, p183-190, 8p

[16] Rong Xiao ,Ming-Jing Li, John ,Hong-Jiang Zhang, "Robust multipose face detection in images"
IEEE Transactions on Circuits & Systems for Video Technology Jan2004, Vol. 14 Issue 1, p31-41, 11p

[17] Zhenan Sun, Yunhong Wang, Tieniu Tan, Jiali Cui, "Improving iris recognition accuracy via cascaded classifiers"
IEEE Transactions on Systems, Man & Cybernetics: Part C - Applications & Reviews Aug2005, Vol. 35 Issue 3, p435-441, 7p

[18] Kang Ryoung Park, Jaihie Kim, "A real-time focusing algorithm for iris recognition camera"
IEEE Transactions on Systems, Man & Cybernetics: Part C - Applications & Reviews; Aug2005, Vol. 35 Issue 3, p441-444, 4p

[19] Connie Tee, Jin Andrew Teoh Beng Ong, Michael Goh Kah Ling, David Ngo Chek, "An automated palmprint recognition system"
Image & Vision Computing; May 2005, Vol. 23 Issue 5, p501-515, 15p

[20] David Cyranoski, "Detectors licked by gummy fingers" Nature. London: Jun 13, 2002.Vol.417, Iss. 6890; pg. 676

[21] Sally Donnelly, “Your eyes can tell no lies” Time. New York: Nov 26, 2001.Vol.158, Iss. 23; pg. 82, 1 pgs

[22] Damon L. Woodard and Patrick J. Flynn “3D Finger Biometrics” Volume 3087/2004
Department of Computer Science and Engineering, University of Notre Dame, Notre Dame, IN 46556, USA

[23] Jian Fu, H. John Caulfield, Seong-Moo Yoo and Venkata Atluri
“Use of Artificial Color filtering to improve iris recognition and searching”
Pattern Recognition Letters, In Press, Corrected Proof, Available online 3 June 2005

[24] http://www.biometricgroup.com/reports/public/reports/finger-scan_optsilult.html

[25] Bill Teasley, Erich Adams “Jazz Up Consumer Products With Speech Recognition”
Electronic Design. Cleveland: Jun 22, 2006. pg. 56, 1 pgs

[26] Javier Ramírez, José C. Segura, Carmen Benítez, Ángel de la Torre and Antonio Rubio. “Efficient voice activity detection algorithms using long-term speech information “
Dpto. Electrónica y Tecnología de Computadores, Universidad de Granada, Campus Universitario Fuentenueva, 18071, Granada, Spain. Speech Communication Volume 42, Issues 3-4, April 2004, Pages 271-287

[27] M. Eleccion, "Automatic Fingerprint Identification",
IEEE Spectrum, vol. 10, 36- 45, 1973.

[28] Domingo Morales L, Javier Ruiz-del-Solar
http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm

[29] Ravis Das. An Introduction to Biometrics.
Military Technology – MILTECH
7/2005

[30] 2004 Homini S.A.
www.homini.com/new_page_1.htm-6k

[31] Merkatum Corporation ,2005
biometrics security & ID

[32] Pontificia Universidad Católica del Perú

[33] Pontificia Universidad Católica del Perú

[34] Pontificia Universidad Católica del Perú

[35] http://suprema.trustpass.alibaba.com

[36] JC TECHNOLOGIES SYSTEMS SAC
ndavila@biometria.com.pe

[37] PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ. Sección de informática
www.pucp.edu.pe/dirinfo

[38] Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar
Handbook of Fingerprint Recognition
Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar
2003 Springer Science+Business Media, Inc.

[39] www.sagem-ds.com

[40] "It's the next best thing to a Babel fish" Celeste Biever.
New Scientist. London: Oct 28-Nov 3, 2006.Tomo192, Nº 2575; pg. 32, 1 pgs