# CONTROL DE ACCESO BASADO EN RECONOCIMIENTO DE IRIS

**OSCAR ANDRÉS SÁNCHEZ MACHADO**

**JOSE RAFAEL GONZÁLEZ GONZÁLEZ**

**CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR**

**FACULTAD DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y MECATRÓNICA**

**CARTAGENA DE INDIAS**

**2003**

# CONTROL DE ACCESO BASADO EN RECONOCIMIENTO DE IRIS

**OSCAR ANDRÉS SÁNCHEZ MACHADO**

**JOSE RAFAEL GONZÁLEZ GONZÁLEZ**

**Monografía, presentada para optar al título de ingenieros Electrónicos.**

**Director:**

**MARGARITA UPEGUI FERRER**

**Ingeniero de Sistemas**

**Magíster En Ciencias Computacionales**

**CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR**

**FACULTAD DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y MECATRÓNICA**

**CARTAGENA DE INDIAS**

**2003**

Cartagena de Indias, noviembre 24 de 2003

Señores:

**COMITÉ DE EVALUACIÓN**

Facultad de Ingeniería Eléctrica, Electrónica y Mecatrónica.

Corporación Universitaria Tecnológica de Bolívar

Ciudad

Estimados Señores:

De la manera más cordial, nos permitimos presentar a ustedes para su estudio, consideración y aprobación de la monografía **"CONTROL DE ACCESO BASADO EN RECONOCIMIENTO DE IRIS"**, la cual es presentada para obtener el título de Ingeniero Electrónico.

Esperamos que este proyecto sea de su total agrado é interés.

Cordialmente,

| | |
|---|---|
| **OSCAR A. SÁNCHEZ MACHADO** | **JOSE R. GONZÁLEZ GONZÁLEZ** |
| C.C. 91 448 163 de Barrancabermeja | C.C. 7 918 217 de Cartagena |

**Nota de aceptación**

---

---

---

---

---

---

**Firma de presidente del jurado**

---

**Firma del jurado**

---

**Firma del jurado**

**Cartagena, noviembre 24 de 2003**

*A Dios, por haberme permitido realizar mi sueño de ser un ingeniero electrónico y espero me siga guiando para ejercer con responsabilidad y honestidad, mi carrera como profesional.*

*A mis padres, quienes desde niño alimentaron mi sueño con sus consejos, dedicación y apoyo incondicional imprimiéndome fortaleza y disciplina en los momentos difíciles para continuar hasta alcanzar la meta propuesta.*

*A mi hermano, quien con su ejemplo y sus críticas constructivas siempre me motivó a ser exigente conmigo mismo para mejorar cada día.*

*A mis amigos, de quienes siempre he recibido afecto y comprensión.*

*Y a mi novia, quien pacientemente me acompañó algunas veces con sus conocimientos y otras con su presencia impulsándome siempre a seguir adelante.*

*Oscar Sánchez.*

*Doy gracias a dios por ayudarme y darme mucho animo para salir adelante, a mis padre por brindarme su apoyo incondicional, su amor, paciencia y sobre todo por darme esta oportunidad tan grande ya que gracias a ellos pude realizar mis sueños de ser un ingeniero electrónico. A mis hermanos por acompañarme siempre en mis momentos de desesperación por brindarme su mano amiga.*

*A mis demás familiares por estar siempre a mi lado brindándome su respaldo para mis metas propuestas en especial a mi tía Gregoria quien estuvo siempre a mi lado brindándome su apoyo y amor de madre. Por ultimo mi novia por haberme acompañado en la recta final de esta mi primera meta y motivarme para seguir a adelante pero especialmente por recordarme a cada momento el esfuerzo de mis padres.*

*Jose Rafael González G*

*Agradecemos a nuestros profesores, quienes no se limitaron únicamente a transmitirnos sus conocimientos para contribuir con nuestro desarrollo como futuros profesionales, sino que fueron maestros de vida inculcándonos valores para crecer como seres humanos.*

*Y de manera especial, agradecemos a nuestros directores de monografía, Margarita Upegui Ferrer y Eduardo Gómez quien con su experiencia y dedicación nos guiaron para desarrollar este trabajo que nos permite ostentar hoy a nuestro título como profesionales.*

*Oscar A. Sánchez*

*Jose R. González*

## CONTENIDO


| | | Pág. |
|---|---|---|
| | INTRODUCCIÓN | 1 |
| 1. | BIOMETRÍA | 3 |
| 1.1 | DEFINICIÓN Y ANTECEDENTES | 3 |
| 1.1.1 | Para que la biometría | 5 |
| 1.2 | GENERALIDADES DE LA BIOMETRÍA | 7 |
| 1.2.1 | Autenticación | 7 |
| 1.2.2 | Identificación | 9 |
| 1.2.3 | Verificación | 9 |
| 1.2.4 | Identificación Vs. Verificación | 10 |
| 1.2.5 | Etapas para la verificación e identificación de los diferentes Sistemas biométricos | 11 |
| 1.3 | APLICACIONES DE LA VERIFICACIÓN BIOMÉTRICA | 11 |
| 1.3.1 | Tratamiento de la señal | 11 |
| 1.3.2 | Ejemplo 1 | 14 |
| 1.3.3 | Comparación de productos | 15 |
| 1.4 | SISTEMAS BIOMÉTRICOS | 16 |

1.4.1 TIPOS DE SISTEMAS BIOMÉTRICOS 16

1.4.1.1 Identificación por huella digital 16

1.4.1.2 Reconocimiento facial 17

1.4.1.3 Geometría de la mano 18

1.4.1.4 Reconocimiento de iris 18

1.4.1.5 Reconocimiento de la retina 19

1.4.1.6 Autenticación por voz 20

1.4.1.7 Verificación dinámica de la firma 20

1.4.1.8 Multimodal 21

1.5 CALIDAD DE LOS SISTEMAS BIOMÉTRICOS 21

1.6 NIVELES DE SEGURIDAD 22

1.6.1 Código de Barra Vs. Biometría 23

1.6.2 Característica de los diferentes sistemas biométricos 26

2. EL IRIS 27

2.1 ANTECEDENTES 27

2.1.1 DEFINICIÓN 28

2.2 IRIDOLOGIA 29

2.2.1 DEFINICIÓN Y BREVE RESEÑA HISTÓRICA 29

2.2.2 VENTAJAS Y LIMITACIONES DEL IRIDOANALISIS 30

2.3 IRIDOLOGIA COMPUTARIZADA 32

2.3.1 APLICACIONES 32

2.4 IRIDIOLOGIA 36

2.4.1 DEFINICIÓN Y BREVE RESEÑA HISTÓRICA 36

2.5 TIPOS DE IRIS 38

2.5.1 Personas Joya 38

2.5.2 Personas Flor 38

2.5.3 Persona Arrollo 39

2.5.4 Personas Punta de Lanza 40

3. CONTROL DE ACCESO POR RECONOCIMIENTO DE IRIS 41

3.1 DEFINICIÓN 41

3.1.1 Autenticación 41

3.1.2 Autorización 41

3.2 IDENTIFICACIÓN POR MEDIO DEL IRIS 42

3.3 CAPTURA DE LA IMAGEN DEL IRIS 43

3.4 LOCALIZACIÓN DEL IRIS 45

3.5 NORMALIZACIÓN DEL IRIS 47

3.6 CODIFICACIÓN DEL IRIS MEDIANTE LA TRANSFORMADA WAVELET DE GABOR 48

3.6.1 LA TRANSFORMADA WAVELET 48

3.6.2 CODIFICACIÓN 56

3.7 IDENTIFICACIÓN DEL CÓDIGO 59

3.7.1 COMPARACIÓN DEL CÓDIGO PARA IDENTIFICACIÓN DEL IRIS 59

3.7.1.1 Código de Hamming 59

3.8 RECONOCIMIENTO DE IRIS UTILIZANDO REDES NEURONALES AUTO ORGANIZADORAS 62

3.8.1 LOCALIZANDO EL IRIS 63

3.8.2 RECONOCIMIENTO DE PATRONES DE IRIS 68

4. APLICACIONES BASADAS EN EL RECONOCIMIENTO DEL IRIS 71

4.1 LA HISTORIA DE SHARBAT GULA 71

4.2 AFGANISTÁN 73

4.3 UN NUEVO DETECTOR DE TERRORISTAS EN LOS AEROPUERTOS 75

4.3.1 ESTADOS UNIDOS 75

4.3.2 EUROPA 77

4.3.3 EMBARQUE EN AVIÓN POR RECONOCIMIENTO DE IRIS 79

4.4 RECONOCIMIENTO DEL IRIS APLICADO EN LOS CAJEROS AUTOMÁTICOS 81

5. DISPOSITIVOS 85

5.1 CÁMARAS PANASONIC BM-ET300 Y BM-ET500 85

5.1.1 ESPECIFICACIONES DEL PRODUCTO 86

5.1.2 CONFIGURACIÓN DE RED BÁSICA 88

5.2 CÁMARA IRISPASS – h 89

5.2.1 ESPECIFICACIONES DEL PRODUCTO 90

5.2.2 CONFIGURACIÓN DE LA RED BÁSICA 91

5.3 CÁMARA LG 3000 92

5.4 CAMARA PANASONIC BM-ET100US 94

6. SISTEMAS DE CONTROL DE ENTRADA A RECINTOS EN COLOMBIA 97

7. CONCLUSIONES Y RECOMENDACIONES 108

BIBLIOGRAFÍA 110

ANEXOS 113

## LISTA DE GRAFICAS

Pág.


Figura 1. Diferentes sistemas biométricos 5

Figura 2. Etapas para la verificación é identificación de los diferentes sistemas biométricos 11

Figura 3. Ejemplo de tasa de aceptación y rechazo en función del umbral de verificación 14

Figura 4. Sistema de reconocimiento por huella digital 17

Figura 5. reconocimiento facial 17

Figura 6. Sistema de reconocimiento Geométrico de la mano 18

Figura 7. extracción del iris con su respectivo código 19

Figura 8. Sistema de reconocimiento de la retina 19

Figura 9. Sistema reconocedor de voz 20

Figura 10. sistema de verificación dinámica de la firma 21

Figura 11. Ubicación del iris en el ojo humano 28

Figura 12. Iridoscopio computarizado 34

Figura 13. Extracción del iris por medio del iridoscopio 35

Figura 14. Características físicas del Iridoscopio 36

**Figura 15. Ojo característico de una Persona-Joya** **39**

**Figura 16. Ojo característico de una Persona-Flor** **40**

**Figura 17. Ojo característico de una Persona-Arroyo** **40**

**Figura 18. Ojo característico de una Persona-Punta de Lanza** **41**

**Figura 19. Cámara CCD** **44**

**Figura 20. Sensor CCD** **45**

**Figura 21. Imagen del contorno del iris** **48**

**Figura 22. Wavelets de Haar** **50**

**Figura 23. Gráficos de varios tipos distintos de wavelets**

**(a) Wavelet de Haar, (b) Wavelet de Daubechies, (c) Wavelet de Morlet** **52**

**Figura 24. Degradación de la imagen al aplicar Wavelets** **55**

**Figura 25. Codificación del signo de la parte real y la parte imaginaria** **57**

**Figura 26. Mapa del Iris** **59**

**Figura 27. Código generado del patrón del iris (iriscode)** **59**

**Figura 28. a. Imagen original b. Imagen binaria en escala de 255 colores** **65**

**Figura 29. Pasos tomadas para la extracción dela coordenada central**

**y radio del iris** **66**

**Figura 30. Reconstrucción de iris y pupila** **67**

**Figura 31. Información de iris extraída** **68**

**Figura 32. Iris reconstruido en forma rectangular** **69**

**Figura 33. Arquitectura del mapa auto organizador** **70**

**Figura 34. Sharbat Gula 18 años después** **72**

**Figura 35. Sistema reconocedor del iris en los principales aeropuertos de los EE.UU 77**

**Figura 36. Dispositivo utilizado para el reconocimiento del iris en el aeropuerto de ÁMSTERDAM 78**

**Figura 37. Tarjeta personal de identificación por medio del iris con su respectivo código 79**

**Figura 38. Dispositivo utilizado para el reconocimiento del iris en el aeropuerto británico de Heathrow 81**

**Figura 39. Cajero automático Argentaría utilizando el sistema de reconocimiento del iris diseñado por la NCR 83**

**Figura 40. Cajero automático STELLA del Royal Bank de Canadá 84**

**Figura 41. cámaras panasonic BM-ET300 Y BM-ET500 86**

**Figura 42. Configuración de la red básica para un control de acceso 89**

**Figura 43. Dispositivo del registro de la identificación 89**

**Figura 44. Cámara OKI IRISPASS-h 90**

**Figura 45. Configuración de una red básica para el control de acceso 92**

**Figura 46. Cámara reconocedora del iris LG 3000 93**

**Figura 47. Cámara panasonic BM-ET100US reconocedora del iris 95**

**Figura 48. Panasonic AuthenticamTM sistema de control de acceso para computadoras portátile 97**

**Figura 49. Oficina de Dactiloscopia y reseña del INPEC sede Cartagena 101**

**Figura 50. Mesa para la toma de la huella digital 102**

**Figura 51. Obtención de los datos personales del individuo 103**

**Figura 52. Toma de la huella dactilar del sindicado 104**

**Figura 53. Archivos donde se encuentran la base de datos de los reos 105**

**Figura 54. Conexión de la red LAN del sistema OKI IRISPASS-h en la institución nacional penitenciaria y carcelaria de Cartagena 107**

## LISTA DE TABLAS

Pág.


Tabla 1. Identificación Vs. Verificación 10

Tabla 2. Código de Barra Vs. Biometría 23

Tabla 3. Característica de los diferentes sistemas biométricos 26

Tabla 4. Ventajas y limitaciones del iridoanalisis 30

Tabla 5. comparación de las cámaras BM-ET300 Y BM-ET500 87

Tabla 6. Especificaciones de la cámara OKI IRISPASS-h 91

## LISTA DE ANEXOS

**Pág.**

**Anexo A. Plano de interconexión del sistema OKI IRISPASS-h en la institución nacional penitenciaria y carcelaria de Cartagena 114**

# GLOSARIO

**Hacker:** Persona que disfruta con la exploración de los detalles de los sistemas programables y cómo aprovechar sus posibilidades; al contrario que la mayoría de los usuarios, que prefieren aprender sólo lo imprescindible.

**Holistica:** trata al individuo como un todo. Holístico deriva del término griego holos, que significa todo; el holismo es una filosofía que motiva el tratamiento del organismo como un todo (una unidad) más que como partes individuales.

**Iriscode:** Es el código que se obtiene al realizar el procesamiento del iris, se deben obtener una cantidad de datos mínima de 256 *KByte*) suficiente para los propósitos de autenticación.

**Minucias:** Recibe el nombre de minucia cualquier punto de la imagen que indica que una determinada cresta presenta un final, un comienzo o una bifurcación. Una minucia estará determinada, por tanto, por sus coordenadas espaciales dentro de la imagen. Generalmente, los patrones biométricos de huella dactilar están constituidos por las coordenadas espaciales de cada minucia.

**Redes Neuronales:** es el intento de poder realizar una simulación computacional del comportamiento de partes del cerebro humano mediante la réplica en pequeña escala de los patrones que éste desempeña para la formación de resultados a partir de los sucesos percibidos.

**XOR:** función lógica que invierte los bits entre dos datos cuando están en diferente estado (0 ó 1).

## RESUMEN

El control de acceso basado en reconocimiento de iris es quizás uno de los métodos más ajenos para las personas, ya que entre nosotros no nos reconocemos por la apariencia del iris y tampoco es un método utilizado por la ley u otra entidad. Es este misterio lo que seguramente haya hecho de este método uno muy utilizado en las películas de espionaje y hasta en juegos de video.

Sabiendo la necesidad de implementar en el mercado un aparato confiable para el control de acceso; y conociendo los métodos actuales de seguridad, se optó por trabajar con la biometría, siendo éste el método mas eficaz para el control de acceso en nuestro caso por reconocimiento de iris.

La imagen del iris (el área de color) se captura con una cámara de alta resolución en blanco y negro, en un entorno correctamente iluminado; esta imagen se somete a deformaciones pupilares (el tamaño de la pupila varía enormemente en función de factores externos, como la luz) y de ella se extraen patrones que a su vez son sometidos a transformaciones matemáticas hasta obtener una cantidad de datos (típicamente 256 *KBytes*) por medio de señales analógicas, pasando por una etapa de interfase, la cual, entre otras cosas; hace la conversión de las señales analógicas en digitales que son mandadas después a la PC. En la PC se analiza,

procesa y captura la imagen (denominada imagen patrón), la cual es almacenada en un archivo. Esta imagen después es comparada con imágenes posteriores de iris de personas

que requieren ser identificadas. De acuerdo a estos parámetros podemos tomar una decisión de aceptación ó rechazo de identidad. El iris es tan único que no hay dos iris iguales, aun en mellizos como en toda la humanidad. En la actualidad, identificar el iris es convertirlo en un código matemático, la probabilidad de que dos irises produzcan el mismo código es de 10 elevado a la 78; siendo que la población de la tierra se estima en 10 elevado a la 10.

# INTRODUCCIÓN

En una sociedad industrializada como la nuestra, la identificación de personas es muy necesaria, ya sea en negocios, empresas, lugares sociales y en las cárceles de nuestro país. Algunas técnicas de identificación son fáciles de violar, por lo que se optó en buscar una forma confiable y segura de reconocer la identidad de una persona. Un área en la cual la tecnología está abordando y simplificando nuestra capacidad para identificar personas, es la biometría. Los sistemas biométricos son métodos automatizados para identificar personas vivas a base de sus características fisiológicas, como es la huella digital ó a base de algunos aspectos del comportamiento como es la voz y la firma. En este caso se optó por las características fisiológicas del iris para realizar la identificación, ya que es uno de los métodos mas seguros en la rama de la biometría.

La biometría es la ciencia que se dedica a la identificación de individuos a partir de una característica anatómica ó un rasgo de su comportamiento. Una característica anatómica tiene la cualidad de ser relativamente estable en el tiempo, tal como una huella dactilar, la silueta de la mano, patrones de la retina ó el iris. Un rasgo del comportamiento es menos estable, pues depende de la disposición psicológica de la persona, por ejemplo la firma. No cualquier característica anatómica puede ser utilizada con éxito por un sistema biométrico. Para que esto así sea debe

cumplir con las siguientes características: Universalidad, Unicidad, Permanencia y Cuantificación.

El proceso general de autenticación sigue unos pasos comunes a todos los modelos de autenticación biométrica: captura ó lectura de los datos que el usuario a validar presenta, extracción de ciertas características de la muestra, comparación de tales características con las guardadas en una base de datos, y decisión de si el usuario es válido ó no. Es en esta decisión donde principalmente entran en juego las dos características básicas de la fiabilidad de todo sistema biométrico (en general, de todo sistema de autenticación): las tasas de falso rechazo y de falsa aceptación. Por tasa de falso rechazo ( False Rejection Rate, FRR) se entiende la probabilidad de que el sistema de autenticación rechace a un usuario legítimo porque no es capaz de identificarlo correctamente, y por tasa de falsa aceptación ( False Acceptance Rate, FAR) la probabilidad de que el sistema autentique correctamente a un usuario ilegítimo; evidentemente, una FRR alta provoca descontento entre los usuarios del sistema, pero una FAR elevada genera un grave problema de seguridad; el cual se esta proporcionando acceso a un recurso a personal no autorizado a acceder a él.

Un indicador biométrico que satisface estos requisitos es el patrón de iris. En la actualidad el patrón de iris representan una de las tecnologías biométricas más seguras y son consideradas pruebas legítimas para la identidad de una persona.

# 1. BIOMETRÍA

## 1.1 DEFINICIÓN Y ANTECEDENTES

El concepto biometría proviene de las palabras bio (vida) y metría (medida), por lo tanto con ello se infiere que todo equipo biométrico mide e identifica alguna característica propia de la persona.

La biometría es una tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de las personas, como por ejemplo, el reconocimiento del iris. Los sistemas biométricos incluyen un dispositivo de captación y un software biométrico que interpreta la muestra física y la transforma en una secuencia numérica. En el caso del reconocimiento del iris, se ha de tener en cuenta que en ningún caso se extrae la imagen del iris, sino una secuencia de números(basados en códigos) que la representan. Sus aplicaciones abarcan un gran número de sectores: Desde el acceso seguro a computadores, redes, protección de ficheros electrónicos, hasta el control horario y control de acceso físico a una sala de acceso restringido.

*Por esta razón la definen como una rama de las matemáticas estadísticas que se ocupa del análisis de datos biológicos y que comprende temas como población, medidas físicas, tratamientos de enfermedades y otros por el estilo.*

*Todos los seres humanos tenemos características morfológicas únicas que nos diferencian. La forma de la cara, la geometría de partes de nuestro cuerpo como las manos, nuestros ojos y tal vez la más conocida, la huella digital, son algunos rasgos que nos diferencian del resto de seres humanos.*

*La medición biométrica se ha venido estudiando desde tiempo atrás y es considerada en la actualidad como el método ideal de identificación humana.*

*Las identificación por medio del iris humano constituye una de las formas más seguras de la utilización de la biometría. No obstante, la tecnología biométrica ha sido prohibitiva en costos para implementaciones en gran escala y muchas versiones no son aún 100% confiables.*

*El Consorcio sobre Biométrica, http://www.biometrics.org/, es el sitio de una organización sin fines de lucro del gobierno de los Estados Unidos para la Investigación, desarrollo, pruebas y aplicaciones de la biométrica a la identificación y verificación de personas.*

**Figura 1. Diferentes sistemas biométricos**


**1.1.1 Para que la biometría:** En lugar de utilizar una contraseña como forma de identificarse, ¿por qué no utilizar una característica física como la voz, la cara, el iris ó la huella digital? Estas medidas corporales, conocidas como biometría, tienen la ventaja de que no pueden ser extraviadas, olvidadas o traspasadas de una persona a otra, aparte de que resulta sumamente difícil falsificarlas. Sin embargo, la tecnología biométrica debe todavía enfrentar algunos desafíos técnicos considerables. El hardware es costoso, los diferentes sistemas son incompatibles entre sí y la tecnología se encuentra en pleno proceso de maduración. Conforme las computadoras se vuelven parte del tejido de la vida cotidiana y más transacciones desde firmas de contratos a compras se realizan digitalmente, las firmas especializadas en biometría piensan que sus productos

pronto serán indispensables. Los sistemas modernos de biometría por computadora se emplean para dos funciones básicas:
la primera es la identificación ('¿quién es esta persona?'), en la que la identidad de un sujeto es determinada comparando su medida biométrica con una base de datos de registros almacenados.

La segunda es la} verificación (¿es esta persona quien afirma ser?), que efectúa una comparación de una medida biométrica con otra que sabe que proviene de una persona en particular.

En un reciente articulo sobre el ***FBI Law Enforcement Bulletin,*** se dice que las huellas digitales son lo mejor para aplicaciones en las que hay una gran cantidad de usuarios. Las del iris pueden igualar o exceder la precisión de las huellas digitales, pero "el número limitado de vendedores y la carencia de precedentes de reconocimiento a través del iris no los hacen tan atractivos" [*]. La geometría de la mano ha dado buenos resultados en las prisiones. El reconocimiento facial puede identificar a las personas "discretamente y sin su cooperación". El reconocimiento por la voz es menos preciso, pero podría ser lo mejor para identificar a alguien en el teléfono. Los lectores biométricos utilizados por el Software Puntual son el HandKey y el HandPunch, para el Software de control de Acceso Handnet for Windows son los Handkey, Ambos equipos son fabricados desde 1986 por la empresa norteamericana *Recognition Systems*, y fueron introducidos en el

[*] Articulo Law Enforcement Bulletin

mercado mexicano en 1990 por DICSA, A la fecha existen más de 1,700 unidades instaladas a lo largo y ancho del país en empresas e Instituciones de todos los tamaños cubriendo aplicaciones de Control de Puntualidad y Asistencia, Acceso, Firma Digital, Acceso a Comedores, Etc....

Estos equipos están basados en el reconocimiento tridimensional de la mano, largo, ancho y espesor, son algunas de las más de 90 medidas que toman en cuenta para conformar la identidad biométrica de la persona. Esta tecnología es la más utilizada mundialmente, siendo líder del mercado con una participación del 36% según la publicación inglesa Biometric Technology Today (1998).

## 1.2 GENERALIDADES DE LA BIOMETRÍA

**1.2.1 Autenticación:** Autenticación es el proceso que permite el reconocimiento de un usuario en un entorno electrónico. En el mundo real, esto sería equivalente a dos partes diciéndole cada una a la otra su nombre, en forma personal o por teléfono. En el mundo electrónico, es el nombre de usuario que se le ha asignado.
El próximo paso de autenticación es el acto de verificar que un individuo es realmente quien dice ser. Esto sería lo mismo que reconocer la voz de alguien en una llamada telefónica. La autenticación es crítica, no solo para identificar y, en consecuencia, denegar el acceso a un hacker, sino también es muy importante

para autenticar con precisión a los usuarios legítimos. Crear una abundancia de falsos positivos (advertencias que resultan ser falsas) llevará eventualmente a los usuarios a sentirse frustrados y encontrar formas de eludir completamente al sistema.

La autenticación puede ser llevada a cabo utilizando distintos tipos de información:

- Lo que una persona conoce - Ej. utilizar una contraseña, frase, ó PIN.
- Lo que una persona tiene - Ej. una ficha, tarjeta inteligente ó certificado.
- Lo que una persona hace – Ej. La forma en que una persona habla o la velocidad a la que una persona escribe.
- Lo que una persona es - Ej. La forma en que una persona luce u otros atributos biométricos.

Una tarjeta ATM y un PIN son las formas más comunes de autenticación de dos factores.

Estas metodologías son comúnmente combinadas para crear niveles variables de seguridad. Cuantas más categorías de información se utilizan para autenticar a un usuario, más seguro es el proceso. La mayoría de los usuarios están familiarizados con la utilización de una ID de ingreso (login) y una contraseña (password). Esta forma de autenticación de factor único es insegura, dado que la

mayoría de los usuarios utilizan contraseñas extremadamente comunes o las dejan a la vista (a veces hasta en el mismo dispositivo).

Un método más seguro para autenticar a un usuario es mediante el uso de autenticación de dos factores, lo cual incorpora dos categorías de información del

usuario. Por ejemplo, puede utilizar información "de lo que usted conoce" (Ej. Una contraseña o PIN), con algo que la persona tiene (Ej. Una tarjeta inteligente o ficha). Esto hace mucho más difícil que una persona no autorizada pueda ingresar a un sistema porque necesitaría ambos ítem para lograr el acceso.

**1.2.2 Identificación:** la identificación suele estar relacionadas con aplicaciones policiales (por ejemplo saber a quien pertenece una determinada huella dactilar, de entre todos los individuos fichados con antecedentes policiales).

**1.2.3 Verificación:** la verificación suele aplicarse en ámbito domestico y empresarial, como mecanismo para proporcionar seguridad adicional ó alternativa a las claves de acceso.

### 1.2.4 Identificación Vs. Verificación

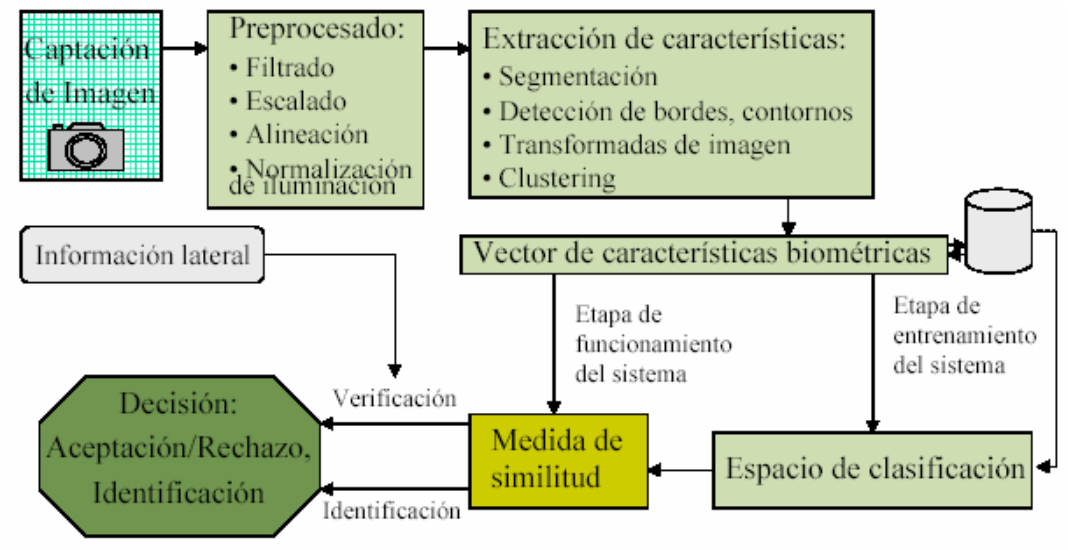
- Base de datos de referencias ó modelos para N individuos
- Técnicas de análisis y decisión similares
- Errores: falso rechazo y falsa aceptación (contrapuestos)

**Tabla 1. Identificación Vs. Verificación**

| **VERIFICACIÓN** | **IDENTIFICACIÓN** |
|---|---|
| Comparación con solo una referencia ó modelo | Selección de una entre N referencias ó modelos |
| Error poco dependiente de N | Mas errores al aumentar N |
| Aplicaciones de control de acceso y búsquedas en Bases de Datos (no forenses) | Aplicaciones de control de acceso y búsquedas en Bases de Datos (forenses) |

### 1.2.5 Etapas para la verificación e identificación de los diferentes Sistemas biométricos

**Figura 2. Etapas para la verificación é identificación de los diferentes sistemas biométricos**




## 1.3 APLICACIONES DE LA VERIFICACIÓN BIOMÉTRICA

**1.3.1 Tratamiento de la señal:** En las aplicaciones de verificación el resultado es una decisión binaria “si” o “no” que permite o niega el acceso al sistema. El funcionamiento puede resumirse en los siguientes pasos:

1. El usuario suministra su identidad (mediante un teclado, tarjeta magnética, etc.), así como la característica biométrica que desea medirse (voz, cara, huella dactilar, etc.). Obsérvese que en las aplicaciones de identificación el usuario no suministra su identidad.

2.-El sistema realiza la parametrización de la característica biométrica de entrada, consistente en calcular un conjunto de números (usualmente unos centenares de bytes).

3.-Se compara la información parametrizada con el modelo correspondiente a la persona cuya identidad se ha suministrado en el punto 1. Este modelo se obtuvo durante el proceso de entrenamiento y modelado de dicha persona.

4.-El resultado de la comparación es una distancia (ó dependiendo del tipo de modelo, probabilidad de semejanza) entre ambas informaciones. Se compara dicha distancia con un umbral prefijado para dicho usuario, si la distancia es menor que el umbral se acepta al usuario. Si es menor se niega el acceso.

El sistema de verificación puede valorarse en función de las tasas de falsa aceptación (TFA) y falso rechazo (TFR), calculadas en un proceso de test del sistema mediante expresiones:

$$TIR = \frac{N° \ usuarios \ autorizados \ rechazados \ por \ el \ sistema}{N° \ usuarios \ autorizados \ usados \ en \ la \ prueba}$$

$$TFA = \frac{N° \ de \ impostores \ aceptados \ por \ el \ sistema}{N° \ de \ impostores \ usados \ en \ la \ prueba}$$

Uno de los aspectos claves es la determinación del umbral de distancia, puesto que condiciona dichos valores. En algunas aplicaciones interesa que una de las dos tasas sea baja a costa de elevar la otra. Por ejemplo, el caso de acceso a recintos militares interesa que la TFA sea muy baja, aún a costa de elevar la TFR.

En otras ocasiones interesa que el umbral sea variable en función de cada situación en particular. Por ejemplo, para autorizar transferencias bancarias puede fijarse un umbral mas ó menos restrictivo en función del importe solicitado.

En general la elección del umbral se realiza a partir de un procedimiento de prueba y error. Un posible ejemplo es el siguiente:

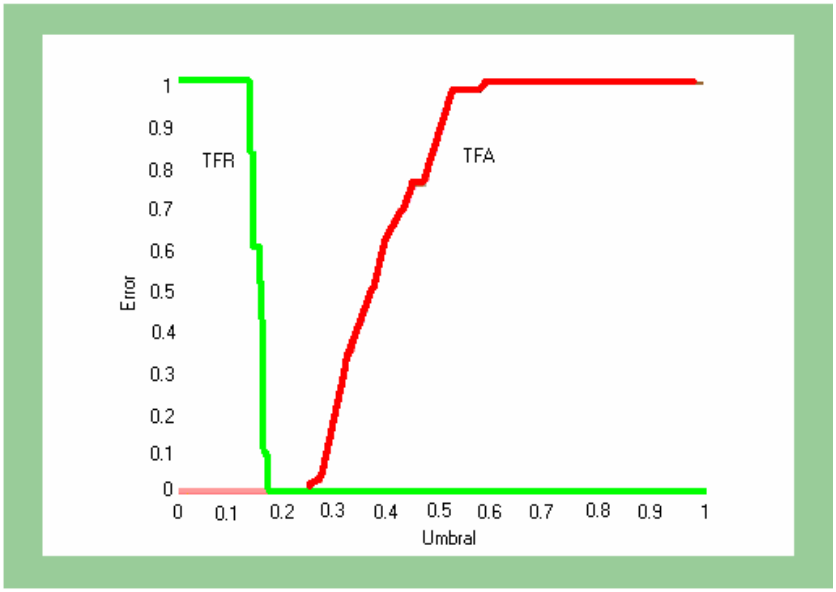
1.-Para cada uno de los usuarios se prueban varios umbrales posibles, entre el valor mínimo de distancia y el máximo (por ejemplo, cien valores en el intervalo [0, 1], habiendo normalizado las distancias a valor máximo la unidad).

2.-Para cada uno de los umbrales de test se calculan las correspondientes tasas TFA y TFR.

3.-Usualmente se escoge como umbral aquél que consigue TFA = TFR.

**Figura 3. Ejemplo de tasa de aceptación y rechazo en función del umbral de**

**Verificación**




**1.3.2 Ejemplo 1.** En la figura 2. presenta la TFA y TFR en tanto por uno en una aplicación de verificación de locutores (a partir de la voz), en las siguientes condiciones:

1. Se ha usado una base de datos micro fónica de 49 locutores muestreada a $f_m$ = 16 KHz y diezmada a 8 KHz.

2. La señal utilizada para entrenar los modelos de cada locutor consistió en un minuto de texto leído.

3. La señal utilizada para calcular los umbrales consistió en cinco frases por locutor, de una duración de unos tres segundos cada frase.

Por lo tanto el numero de usuarios autorizados utilizando el calculo del umbral de un usuario es 5, y el numero de impostores es (49-1).

En la figura anterior se presenta las TFA y TFR para un locutor determinado, en función de los umbrales evaluados. Estos resultados provienen de aplicar el método de reconocimiento de locutor mediante matrices de covarianza descrito anteriormente. Obsérvese que la selección del umbral optimo supone un compromiso entre la TFA y la TFR y que en este ejemplo su valor óptimo está en torno a 0,2.

**1.3.3 Comparación de productos:** Cuando la tasa de falsa aceptación es igual a la tasa de falso rechazo, se habla de *Equal Error, Rate (EER)* ó tasa de errores idénticos. Esta tasa suele usarse para comparar diversos sistemas ó implementaciones de distintos fabricantes (generalmente se ajustan los umbrales para conseguir que ambas tasas sean idénticas). Sin embargo, no modela totalmente al sistema y hay que ser cuidadoso a la hora de hacer valoraciones.

## 1.4 SISTEMAS BIOMÉTRICOS

### 1.4.1 TIPOS DE SISTEMAS BIOMÉTRICOS

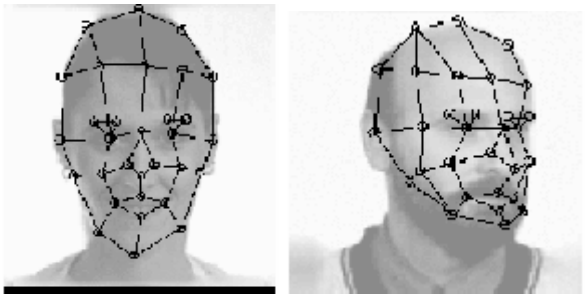
Hoy en día, el mercado ofrece una gran variedad de sistemas biométricos que pueden ser clasificados de acuerdo a la característica del individuo que capturan para efectuar la autenticación. De acuerdo a esta categorización, se pueden describir ocho tipos diferentes de sistemas biométricos:

**1.4.1.1 Identificación por huella digital:** Se obtienen imágenes ópticas o electrónicas del dedo por un proceso de enrolamiento. Estas se registran en una base de datos o en una tarjeta inteligente en forma de algoritmo. La transacción positiva se produce cuando el dedo de quien pretende ser aceptado por el sistema coincide con el registro existente.

**Figura 4. Sistema de reconocimiento por huella digital**


**1.4.1.2 Reconocimiento facial:** Analiza las características faciales por medio de una imagen óptica que explora algunas aspectos sobresalientes del rostro. Eso es registrado por medio de un algoritmo en una base de datos. La verificación para la aceptación se produce también por coincidencia del registro con el rostro actual.

**Figura 5. reconocimiento facial**



**1.4.1.3 Geometría de la mano:** Similar a los anteriores en cuanto al procedimiento. Un scanner captura la mano y sus características principales de modo tridimensional.

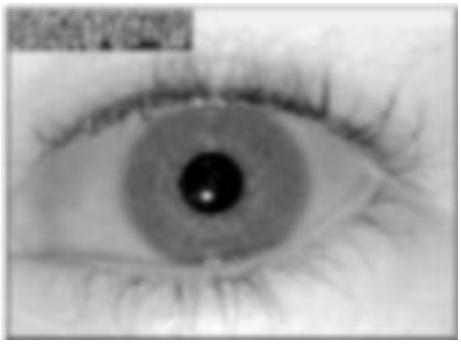
**Figura 6. Sistema de reconocimiento Geométrico de la mano**

Se trata de la medición de las características físicas de manos y dedos desde una perspectiva tridimensional. Estos sistemas son adecuados a bases de muchos usuarios con acceso infrecuente y pueden estar menos predispuestos y disciplinados a ser detectados. La precisión puede ajustarse hasta ser elevada y son técnicas muy flexibles a los escenarios.

**1.4.1.4 Reconocimiento de iris:** Un haz infrarrojo ilumina el iris para obtener una imagen de alta resolución. El procedimiento es similar al de los anteriores.

**Figura 7. extracción del iris con su respectivo código**

El barrido de iris es sin lugar a dudas la tecnología menos intrusa, pues, se utiliza una cámara convencional y no requiere contacto íntimo entre el sistema de registro y la persona. Su precisión es buena y no hay problemas en los registros de personas con anteojos o lentes de contacto. Ha sido probada con variados grupos étnicos.



**1.4.1.5 Reconocimiento de la retina:** Requiere que el usuario mire en el scanner hacia un punto especifico. El registro y su aplicación es similar a los anteriores.

**Figura 8. Sistema de reconocimiento de la retina**

**1.4.1.6 Autenticación por voz:** Usa como modelo de reconocimiento los timbres de voz únicos y personales de cada usuario. La identificación se realiza como en los sistemas anteriormente descriptos

**Figura 9. Sistema reconocedor de voz**

**1.4.1.7 Verificación dinámica de la firma:** Registra la firma escrita a mano por análisis de forma, velocidad y presión en el acto de firmas, factores que indican "como" fue realizado el acto de firmar. La comparación de autenticación es similar a las anteriores.

**Figura 10. sistema de verificación dinámica de la firma**


**1.4.1.8 Multimodal:** Combina diferentes métodos biométricos para aumentar los recaudos de seguridad.

## 1.5 CALIDAD DE LOS SISTEMAS BIOMÉTRICOS

Los parámetros que miden la calidad de los sistemas biométricos son:

- **Coeficiente de fallas de enrolamiento:** es el porcentaje de población que no puede ofrecer una muestra compatible con el sistema instalado. Por ejemplo, un 2% de la población no pude presentar una impresión digital utilizable.

- **Coeficiente de rechazos falsos:** que es el porcentaje de usuarios autorizados que el sistema rechaza por error.

- **Coeficiente de aceptaciones falsas:** que es el porcentaje de personas no autorizadas que el sistema deja entrar.

## 1.6 NIVELES DE SEGURIDAD

los coeficientes de seguridad *"in the field"* tienen alguna dependencia con los factores presentes en este momento, siendo los principales:

- Características demográficas de la población de usuarios.
- Extensión de la muestra de la población
- Volumen de transacciones por hora
- Condiciones ambientales
- Tiempo transcurrido desde que se aplicó el sistema (Tasa de error tomada sobre la base uno a uno)
- Identificación por huella digital: 1% a 10%
- Reconocimiento facial: mas del 10%
- Geometría de la mano: 0,4% a 10%

- Reconocimiento por el iris: 1/1.000.000
- Autenticación por voz: aprox. 1%
- Verificación dinámica de la firma: aprox. 1%
- Multimodal: mejor que cualquier componente

### 1.6.1 Código de Barra Vs. Biometría

**Tabla 2. Código de Barra Vs. Biometría**

| CONCEPTO | CÓDIGO DE BARRAS, BANDA MAGNÉTICA | BIOMETRÍA | CONCLUSIONES |
|---|---|---|---|
| **TECNOLOGÍA** | Sistema de tecnología de punta, que incluye comunicación por puerto ethernet, tiene capacidad de crecimiento en memoria. | Sistema de Tecnología de punta, con opción de comunicación por puerto ethernet. Tiene capacidad de crecimiento en memoria. | Ambos sistemas cuentan con opción electrónica actualizada, sólo que el biométrico es un equipo distinto d reconocimiento, ya que identifica personas, lo cual lo hace más confiable que código de barras, banda magnética o proximidad. |
| **IDENTIFICACIÓN** | Estos sistemas reconocen OBJETOS, mediante el uso de credenciales con código de barras, banda magnética o tarjetas de proximidad. | Este sistema reconoce PERSONAS, mediante el uso de la forma tridimensional de la mano. | No es lo mismo reconocer OBJETOS, que reconocer PERSONAS |

| | | | |
|---|---|---|---|
| **VELOCIDAD** | Estos sistemas pueden ofrecer un tiempo de respuesta en el registro de puntualidad y asistencia de hasta dos segundos por empleado. | Estos sistemas pueden ofrecer un tiempo de respuesta en el registro de puntualidad y asistencia entre tres y seis segundos, dependiendo del equipo que se utilice. | En ocasiones es importante el tiempo de respuesta y la velocidad que los equipos ofrecen, pero se tiene que considerar la veracidad del registro final, el cual se puede obtener en dos segundos (identificación de objetos, no se sabe quién lo hace) o en seis segundos (identificación de personas, único por empleado). |
| **MANTENIMIENTO** | **Las fallas más comunes en estos equipos ocurren** en el teclado, en caso de que venga incluido, y en la base de deslizamiento de la credencial, la cual se desgasta con el tiempo. Solo requiere de limpieza general y en especial el área de lectura del código de barras o de la cabeza lectora en banda magnética. Proximidad requiere muy poco mantenimiento. | Las fallas más comunes en estos equipos ocurren en el teclado, el cual tiene movimiento mecánico y también, la base de posición de la mano, la cual puede desgastarse con el uso. Sólo requiere de limpieza general y en especial en la base donde se coloca la mano y los espejos | En ambos casos, las fallas más comunes se pueden corregir con un mantenimiento preventivo o en caso de ser correctivo, estas piezas son consumibles normales. También, en ambos casos, este material es una refacción poco costosa y fácil de reemplazar. |
| **VANDALISMO** | Los sistemas de código de barras o de banda magnética pueden ser dañados, metiendo objetos en la ranura del lector, rociándoles algún líquido o simplemente agrediéndolos físicamente, mientras que en los lectores de proximidad, el vandalismo es muy reducido. | Estos sistemas pueden ser dañados, si se les rocía algún líquido o si se rompen sus espejos y/o postes, también si se agreden físicamente | Entre más restrictivo sea un equipo, más susceptible será al vandalismo, ya que representará mayor obstáculo a las personas que lo utilizan. |

| | | | |
|---|---|---|---|
| **COSTOS** | Según la calidad del equipo y de las funciones que incluyan, se pueden conseguir desde los $1,000.00 US hasta los $8,000.00 US | Un equipo Biométrico para 512 usuarios, tiene un costo desde $1,800.00 US. Dependiendo de la aplicación en que se vaya a instalar. | Los costos son siempre importantes en la toma de decisiones para la adquisición de un equipo. Siempre se deberá tomar en cuenta aspectos como: ¿Qué se desea controlar? ¿Cuál es la seguridad que se desea tener en la veracidad de la información?, etc. De tal forma que en una tabla de comparativo costo-beneficio, se obtenga la mejor decisión para una compañía. |
| **COSTO CONSUMIBLE** | En un sistema de código de barras, banda magnética o proximidad, se pueden elaborar credenciales con precios desde $1.00 U.S., hasta los $15.00 U.S., dependiendo de la tecnología a utilizar. | En un sistema biométrico el costo del consumible es de $0.00, ya que la mano no le cuesta a la empresa. | En cada proyecto de puntualidad y asistencia, si éste es de código de barras o cualquier otra tecnología que identifique objetos, se debe considerar un 30% adicional a la credenciales que se necesiten, ya que la rotación y las pérdidas necesitarán de reposición inmediata. En un biométrico no se da este caso. |

### 1.6.2 Característica de

### 1.6.3 los diferentes sistemas biométricos

## Tabla 3. Característica de los diferentes sistemas biométricos

| Sistemas biométricos | Identificación y autenticación | Interferencias | Fiabilidad | Facilidad de uso | Prevención de ataques | Aceptación | Estabilidad | Utilización |
|---|---|---|---|---|---|---|---|---|
| **Ojo– Iris** | Ambas | Gafas | Muy alta | Media | Muy Alta | Media | Alta | Instalaciones nucleares, servicios médicos, centros penitenciarios Instalaciones nucleares, servicios médicos, centros penitenciarios Policía, industrial General Industrial Accesos remotos en bancos o bases de datos |
| **Ojo– retina** | Ambas | Irritaciones | Muy alta | Baja | Muy alta | Media | Alta | |
| **Huellas dactilares** | Ambas | Suciedad, heridas, asperezas | Alta | Alta | Alta | Media | Alta | |
| **Geometría de la mano** | Autenticación | Artritis, reumatismo | Alta | Alta | Alta | Alta | Media | |
| **Escritura Firma** | Ambas | Firmas fáciles o cambiantes | Alta | Alta | Media | Muy alta | Media | |
| **1Voz** | Autenticación | Ruido, resfriado | Alta | Alta | Media | Alta | Media | |

# 2. EL IRIS

## 2.1 ANTECEDENTES

La investigación en la tecnología de la identificación ocular comenzó en el año 1935. Durante ese año apareció un articulo de el *'New York State Journal of Medicine'* sugirió que “el patrón de las arterias y venas de la retina podría ser usado para la identificación univoca de un individuo” [*].

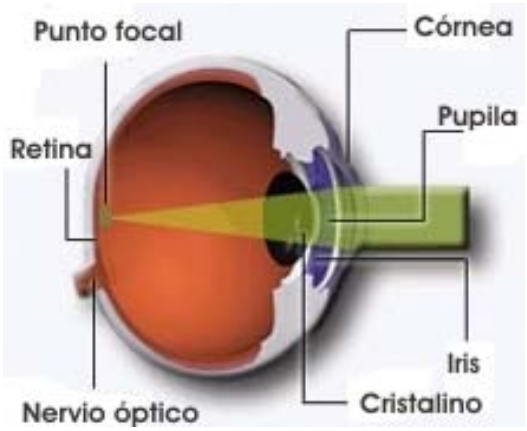
Ha sido bien documentada la unicidad de la identificación ocular. El iris es tan único que no hay dos iris iguales, aún en mellizos, como en toda la humanidad. La probabilidad de que dos iris produzcan el mismo código es de 10 elevado a la 78, dándose a conocer que la población de la tierra se estima aproximadamente en 10 elevado a la 10 millones de habitantes.

[*] Articulo de el 'New York State Journal of Medicine'

### 2.2.1 DEFINICIÓN

El iris humano (el anillo que rodea la pupila, que a simple vista diferencia el color de ojos de cada persona) es igual que la vasculatura retinal, una estructura única por individuo que forma un sistema muy complejo, inalterable durante toda la vida de la persona. El alto nivel de aleatoriedad en su estructura que permite 266 grados de libertad que pueden ser codificados y una densidad de información de 3.4 bits por mm² de tejido. Su función es controlar el tamaño de la pupila (esta controla la cantidad de luz que entra al ojo, en presencia de mucha luz la pupila se cierra, mientras qué con poca luz, se dilata, aumentando su tamaño. Esto lo logra contrayendo o expandiendo los músculos con que cuenta).

**Figura 11. Ubicación del iris en el ojo humano**



## 2.2 IRIDOLOGIA

### 2.2.1 DEFINICIÓN Y BREVE RESEÑA HISTÓRICA

La iridologia es el estudio de las alteraciones del iris en correspondencia con los órganos del cuerpo, cuya historia se remonta desde los tiempos de Hipócrates de Cos, médico y filósofo griego que vivió entre los años 460 a 377 AC. Así, la Ciencia egipcia era descendiente de la mesopotámica, la que a su vez se hallaba emparentada con la hindú. Los sacerdotes mesopotámicos, los cuales eran grandes astrólogos y astrónomos, veían en el iris una proyección de la cúpula estelar, bajo la cual estudiaban las influencias constitucionales que enmarcaban al hombre en su entorno natal; según la fecha, lugar y hora de nacimiento cada individuo recibía un órgano débil y otro fuerte. De ahí que la iridología, durante siglos era una ciencia y enseñanza secreta. De esta manera existen documentos que certifican la importancia que le daban los antiguos médicos-sacerdotes al estudio del iris como forma de análisis del estado de los órganos de un organismo humano. Sin embargo la Iridología moderna nació junto con un médico húngaro llamado Ignaz Von Peczely, oriundo de Budapest (1826-1911), quien en 1873 publicó su primer libro sistemático sobre la Iridología. Peczely describe la observación casual que le llevó a intuir la relación existente entre el iris y los demás órganos del cuerpo, de esta manera: "... Cuando era niño, mientras

intentaba cazar una lechuza, le rompí sin querer una pata; al día siguiente pude constatar la aparición de una ancha fisura negra en su iris... " [*]. A partir de ese momento comenzó a difundirse esta ciencia, pese a la burla de la medicina convencional. Así encontraremos en las filas de la Iridología, profesionales, tales como Nils Liljequist, Henry Lindahr, León Vannier, Theodor Kriege, Joseph Deck, Gilbert Jausas, Bernard Jensen, etc. quienes aportaron conocimientos con el objeto de enriquecer y ampliar la ciencia y técnica de la Iridología.

### 2.2.2 VENTAJAS Y LIMITACIONES DEL IRIDOANALISIS

**Tabla 5. Ventajas y limitaciones del iridoanalisis**

| Lo que se ve por el iris | Lo que no se ve por el iris |
|---|---|
| - Debilidades y fortalezas inherentes de órganos, glándulas y tejidos. | - Si el sujeto es masculino o femenino. |
| - Fortaleza o debilidad constitucional del individuo ya sea adquirida o heredada. | - Enfermedades por nombres. |
| - Estado de la inflamación de órganos, tejidos, su localización y el grado de necesidad de cuidados. | - Las operaciones quirúrgicas que un individuo ha tenido |
| - La cantidad relativa de toxicidad en órganos, glándulas y tejidos. | - Embarazo |
| - Condición del sistema gastrointestinal, grado de acidez, espasticidad, abombamiento, prolapso, inflamación y | - Si hay un tumor y que tamaño tiene. |

[*] "Descubrimientos en el reino de la naturaleza y el arte de curar" Von Peczely 1880.

| | |
|---|---|
| condición nerviosa. | |
| - Deficiencia de asimilación nutricional y deficiencias de minerales en órganos, tejidos y glándulas. | - La presencia de piedras en riñones o vesícula biliar. |
| - Congestión linfática | - La presencia del SIDA. |
| - Capacidad de recuperación del cuerpo y calidad de la fuerza / energía nerviosa en el cuerpo. | - Si hay bloqueo en una arteria |
| - Fuente de infecciones de bajo nivel. | - Si existe hemorragia. |
| - Resultados del la fatiga por estrés físico y mental. | - Nivel de la presión sanguínea, azúcar en sangre u otros resultados de laboratorio. |
| - Condición preclínica de muchas enfermedades tales como diabetes, cardiovascular, apendicitis, prostatitis, etc. | - Niveles de ácido úrico en el cuerpo. |
| - Nivel de circulación sanguínea en órganos y tejidos así como la influencia de un órgano sobre otro. | - El tiempo y causa de una herida. |
| - Potencial senil. | - La presencia de infecciones por microorganismos. |
| - Signos de curación en órganos, tejidos y glándulas y el grado de respuesta al tratamiento que indica si la terapia está funcionando. | - Si una operación es necesaria.<br>- Qué alimentos un individuo come o no come específicamente. |

## 2.3 IRIDOLOGIA COMPUTARIZADA

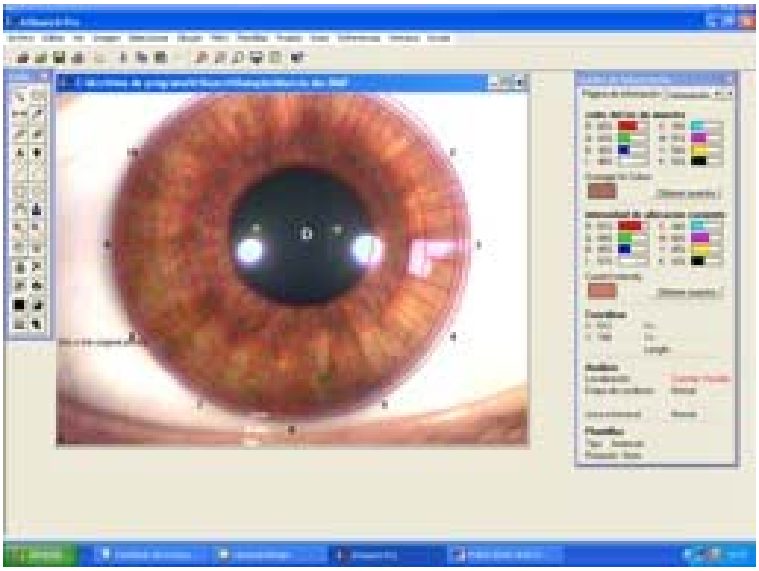
### 2.3.1 APLICACIONES

La iridologia computarizada es una eficaz herramienta de la tecnología moderna, para el análisis del iris. NO DESCARTA AL IRIDOLOGO, pero le permite analizar detenidamente el iris de su paciente, EN EL MONITOR, sin las molestias que conlleva analizar directamente: (lloriqueo, cansancio, poner el aliento bucal en la nariz del paciente) y permite la participación del paciente, ya que visualiza directamente las señales de su propio iris y la posibilidad de llevarse una copia a colores para su futura comparación. Estas señas le motivan a llevar más control en su terapia y en su dieta. Le da mas status al consultorio o Clínica y más credibilidad al médico.

**Figura 12. Iridoscopio computarizado**

Con un simple clic, se captura la imagen del iris, donde el paciente solo tiene que poner su barbilla y frente a la cámara. Un programa analiza el iris. Con solo colocar el puntero del mouse, le señala el área anatómica que representa y el estado en que se encuentra, (normal, agudo, sub agudo, crónico o degenerativo) partiendo de un parámetro comparativo de colores.

**Figura 13. Extracción del iris por medio del iridoscopio**



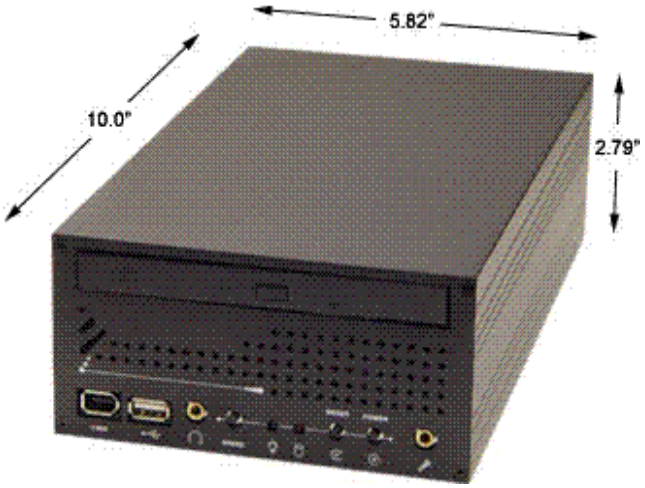
Este novedoso equipo cuenta con:

- Fuente de poder con regulación de intensidad de la luz
- Una tarjeta con salida USB-2 la cual tiene una velocidad 40 veces mayor que su antecesora USB-1 logrando una mayor resolución.
- Procesador Pentium IV a 1.7 Ghz (Puede ser substituido por uno de mayor velocidad)
- 128 Mb de memoria RAM (expandidle hasta 1 Gb)
- Disco duro de 20 Gb
- puertos USB 2.0
- Monitor LCD extraplano

- Teclado flexible
- Mouse óptico

Además de ser un equipo muy avanzado en cuanto a su software y hardware es muy compacto y fácil de transportar lo que lo hace mas eficiente.

**Figura 14. Características físicas del Iridoscopio**



## 2.4 IRIDIOLOGIA

### 2.4.1 DEFINICIÓN Y BREVE RESEÑA HISTÓRICA

La iridiología es la ciencia que estudia al hombre a través del iris, una forma holística de entender al ser humano que nos habla tanto de su camino espiritual como de sus patrones genéticos. Nada en el iris está dispuesto al azar; por el contrario, los ojos revelan una gran información sobre sus propietarios a través de los colores, formas y patrones que contienen.

Para los iridiólogos, a través del iris es posible observar de qué manera la persona se relaciona con el mundo, cómo se expresa, cómo aprende y qué tipo de compañías le atraen. Así mismo, el iris muestra la pauta de la transferencia genética de rasgos físicos y comportamientos de generación en generación, con lo que es posible comprender los rasgos y habilidades específicas que un niño ha recibido de su padre y su madre.

Uno de los sistemas de estudio del iris con mayor desarrollo en la actualidad es el llamado método Rayid, creado en los años ochenta por el médico naturópata

Denny Ray Jonson, quien consideraba que los ojos poseen una habilidad innata para crear patrones de respuesta en otras personas y se convierten, por tanto, en utilísimas herramientas de autoconocimiento. Para Harry Wolf, presidente de la asociación Internacional de Iriodiología y alumno destacado de Rayid, “a través del iris humano se entiende la naturaleza de las enfermedades y el proyecto genético, físico y psicológico de una persona, su conexión con el Universo” [*]. De ahí que, según Wolf, observando el iris podamos ayudar al ser humano a ser artífice de su propia curación y saber, además, cuál es el hemisferio cerebral que predomina en cada uno de nosotros y cuáles son los rasgos más destacados de nuestra personalidad.

Pues bien, según esta formulación es posible reconocer cuatro tipo de personalidades básicas dependientes de tres patrones básicos en el iris, y que se describen metafóricamente como personas flor, personas joya, personas arroyo y personas punta de lanza.

[*] Harry Wolf FRAMPTON/NORDESTON Editorial G.G.

## 2.5 TIPOS DE IRIS

**2.5.1 Personas Joya: (Analíticas y Verbales)** las personas joya se identifican por las concentraciones de color en forma de manchitas o puntos que aparecen en las fibras del iris y que varían del color dorado claro al negro.

**Figura 15. Ojo característico de una Persona Joya**

**2.5.2 Personas Flor: (Visuales y Emocionales)** Las personas flor se caracterizan por tener aberturas curvadas o redondeadas en las fibras del iris, destacando por ser gente emocional y espontánea que responde a la vida con sentimientos y comunicación visual.

**Figura 16. Ojo característico de una Persona Flor**


**2.5.3 Persona Arrollo: (Intuitivas y Controladas)** Las personas arroyo se caracterizan por poseer sutiles fibras en el iris que parecen rayas o zonas de color. Suelen ser sensitivas y, energéticamente, responden a los demás con gestos delicadamente controlados.

**Figura 17. Ojo característico de una Persona Arroyo**

**2.5.4 Personas Punta de Lanza: (Intensas y Paradójicas)** Se tratan de las personas que constituyen una mezcla de personalidades joya y personalidades flor, siendo su patrón bastante fácil de identificar en el iris por ser el resultado de una síntesis entre ambas características. El comportamiento resultante de esta combinación difiere notablemente de los demás patrones. A veces, su naturaleza extremista les hace ser difíciles de enseñar o controlar; sin embargo, una vez que su energía está equilibrada, pueden llegar a producir cambios nuevos y duraderos en la sociedad.

**Figura 18. Ojo característico de una Persona Punta de Lanza**

# 3. CONTROL DE ACCESO POR RECONOCIMIENTO DE IRIS

## 3.1 DEFINICIÓN

El control de acceso constituye una poderosa herramienta para proteger la entrada a un recinto completo o sólo a ciertos puntos del recinto concretos, e incluso, a objetos o sistemas individuales. Este control consta generalmente de dos pasos: Autenticación y Autorización.

**3.1.1 Autenticación:** Identifica al usuario o a la máquina que trata de acceder a los recursos, protegidos o no.

**3.1.2 Autorización:** Procede la cesión de derechos, es decir, que dota al usuario de privilegios para poder efectuar ciertas operaciones con los datos protegidos, tales como leerlos, modificarlos, crearlos, etc.

## 3.2 IDENTIFICACIÓN POR MEDIO DEL IRIS

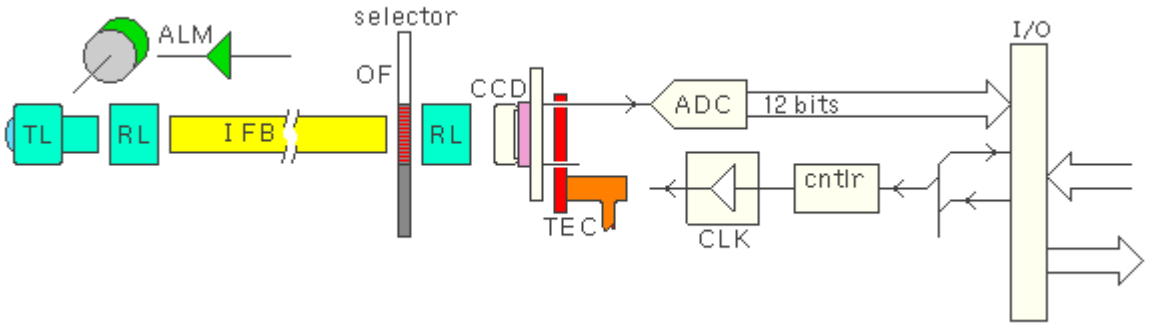
La identificación basada en el reconocimiento de iris es más moderna que la basada en patrones retínales; desde hace unos años el iris humano se viene utilizando para la autenticación de usuarios. Para ello, se captura una imagen del iris en blanco y negro, en un entorno correctamente iluminado; esta imagen se somete a deformaciones pupilares (el tamaño de la pupila varía enormemente en función de factores externos, como la luz) y de ella se extraen patrones, que a su vez son sometidos a transformaciones matemáticas hasta obtener una cantidad de datos (típicamente 256 Bytes) suficiente para los propósitos de autenticación.

Este pequeño patrón proporciona una ventaja cuando de búsquedas en base de datos se trata. Como resultado hasta 100.000 registros pueden ser comparados por segundo en una PC estándar.

## 3.3 CAPTURA DE LA IMAGEN DEL IRIS.

En sistemas para el reconocimiento del iris se utilizan cámaras de vídeo de tipo CCD. En la figura 19 se puede apreciar un diagrama de bloques de esta cámara.

**Figura 19. Cámara CCD**




El corazón de la cámara es un circuito integrado tipo CCD (Dispositivo de Carga Acoplada)[*]. Este dispositivo contiene varios cientos de miles de elementos individuales (píxeles) localizados en la superficie de un diminuto CI.

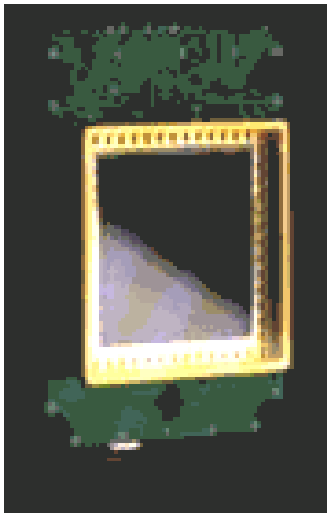
Cada píxel se ve estimulado con la luz que incide sobre él (la misma que pasa a través de los lentes y filtros de la camera), almacenando una pequeña carga de

[*] The CCD Camera Cookbook. de Richard Berry, Veikko Kanto y John Munger

electricidad. Los píxeles se encuentran dispuestos en forma de malla con registros de transferencia horizontales y verticales que transportan las señales a los circuitos de procesamiento de la cámara (convertidor analógico-digital y circuitos adicionales). Esta transferencia de señales ocurre 6 veces por segundo.

En la figura 20, podemos apreciar un arreglo comercial de este tipo de CI. En el campo de procesamiento de imágenes, este integrado ha revolucionado todo lo establecido, siendo el componente principal de las llamadas Cámaras Fotográficas Digitales.

**Figura 20. Sensor CCD.**



## 3.4 LOCALIZACIÓN DEL IRIS

La localización del iris es posible gracias a la ecuación descrita por John Daugman, de la Universidad de Cambridge [*]. En la cual Primero es necesario localizar los bordes interno y externo del iris, detectar y excluir los párpados si ellos se interponen como se muestra en la figura 21. Estas operaciones de detección son llevadas a cabo empleando las siguientes operaciones integro diferenciales.

$$\max_{(r,x_0,y_0)} \left| G(r) * \frac{\partial}{\partial r} \oint_{(r,x_0,y_0)} \frac{I(x,y)}{2\pi r} ds \right|$$

$$G_\sigma(r) = \frac{1}{2\pi\sigma^2} \ell^{\left(-\frac{r^2}{2\sigma^2}\right)}$$

En donde I(x,y) representa los nivel de gris de la imagen en la coordenada (x,y).
La función G(r) será la muestra de la distribución gaussiana.

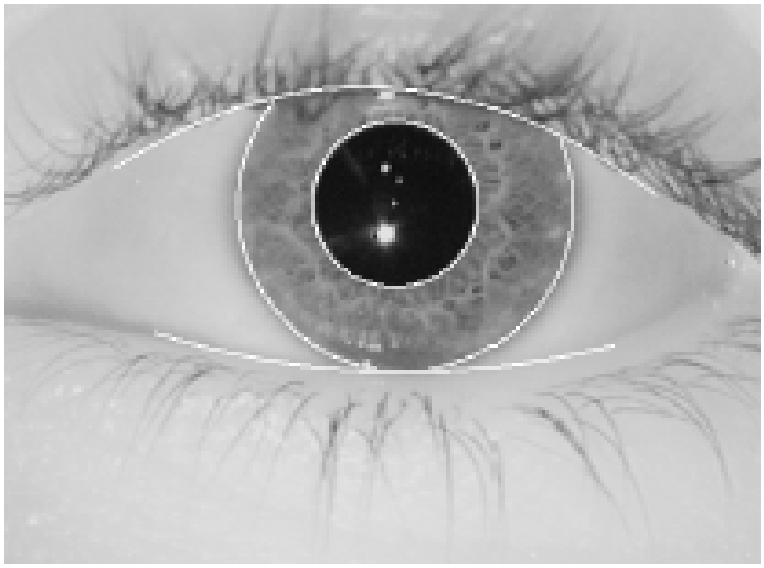
En la localización del iris lo primero que se realiza es la marcación de las fronteras del iris. Estas fronteras se caracterizan por que hay una transición notable de color entre las partes del ojo. por ejemplo: Entre el globo ocular y el iris existe un cambio

[*] John Daugman Recognizing persons by their iris patterns. In *Biometrics: Personal Identification in Networked Society*, pages 103-121. Kluwer, 1998.

en el brillo bastante notable ya que el globo ocular es blanco y el iris es de otro color (café, azul, verde, etc). De esta forma se localiza la primera frontera entre el globo ocular y el iris[*]. Otra frontera importante es la que se encuentra entre el iris y la pupila. la pupila es mucho mas oscura que el iris debido a que esta parte del ojo deja ver solo la oscuridad de una caja negra (interior del globo ocular) y a pesar de que el color del iris sea oscuro nunca va a llegar a ser tan negro como la pupila. De esta forma se marca la otra frontera entre el iris y la pupila, de igual forma podemos encontrar otras fronteras como por ejemplo entre el párpado y el iris. En la figura 21 podemos ver claramente las fronteras del iris. Después de tener marcadas la fronteras principales se observa que se forma una circunferencia casi perfecta. De esta forma podemos hallar el centro de la misma conociendo el radio de dicha circunferencia. Teniendo localizado el centro del iris podemos comenzar a hacer un rastreo de la conformación del iris en forma polar, desde la frontera entre el iris y la pupila hasta la frontera del iris y el globo ocular.

[*] Tratamiento Digital de Imágenes. Alberto Domingo Ajenjo. Anaya Multimedia 1994

**Figura 21. Imagen del contorno del iris**



## 3.5 NORMALIZACIÓN DEL IRIS

Después de la localización del iris es necesario definir un sistema de coordenadas bidimensional en el cual se ubica el tejido del iris de tal forma que los cambios de la pupila, las variaciones de la cámara por el acercamiento y la distancia del ojo, no generen efectos. La normalización se hace necesaria, para tener una cierta independencia de las propiedades de la imagen, como lo son el brillo y el contraste, y así poder comparar el iriscode.

Las ecuaciones que nos permiten realizar esto son las siguientes:

$$\left.\begin{aligned} x(r,\theta) &= (1-r)x_i(\theta) + rx_e(\theta) \\ y(r,\theta) &= (1-r)y_i(\theta) + ry_e(\theta) \end{aligned}\right\} 0 \le r \le 1,\ 0 \le \theta \le 2\pi$$

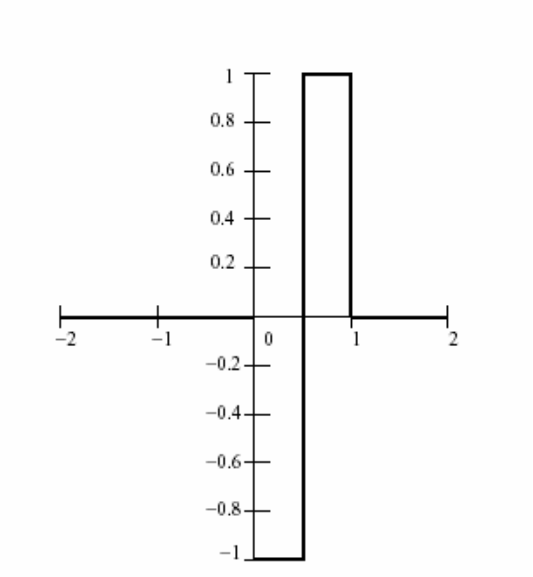
Las cuales permiten la transformación de coordenadas cartesianas a coordenada polar para la posterior codificación.

## 3.6 CODIFICACIÓN DEL IRIS MEDIANTE LA TRANSFORMADA WAVELET DE GABOR

### 3.6.1 LA TRANSFORMADA WAVELET

El primer participante en la carrera de las wavelet fue un matemático húngaro llamado Alfred Haar, que introdujo en 1909 las funciones que actualmente se denominan "wavelets de Haar". Estas funciones consisten simplemente en un breve impulso positivo seguido de un breve impulso negativo

**Figura 22. Wavelets de Haar**



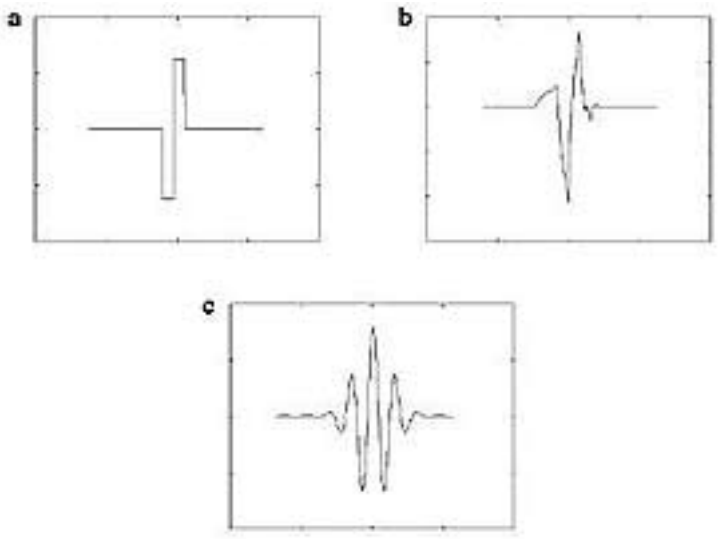

Aunque los impulsos breves de las wavelets de Haar son excelentes para la enseñanza de la teoría de las wavelets, no resultan de tanta utilidad en la mayoría de aplicaciones, ya que producen líneas irregulares con picos en lugar de curvas suaves. Por ejemplo, una imagen reconstruida con las wavelets de Haar tiene el aspecto de una pantalla de calculadora barata, y una reconstrucción realizada con wavelets de Haar del sonido de una flauta es demasiado áspera.

Durante varias décadas posteriores, surgieron otros precursores de la teoría de las wavelets. En la década de 1930, los matemáticos ingleses John Littlewood y R.E.A.C. Paley desarrollaron un método de agrupación de frecuencias por octavas, creando de esta forma una señal con una frecuencia bien localizada (su

espectro se encuentra dentro de una octava) y también relativamente bien localizada en el tiempo. En 1946, Dennis Gabor, un físico británico-húngaro, presentó la transformación de Gabor, análoga a la transformación de Fourier, que separa una onda en "paquetes de tiempo-frecuencia" o "estados coherentes" que tienen la mayor localización simultánea posible tanto en tiempo como en frecuencia. Y en las décadas de 1970 y 1980, las comunidades de procesamiento de señales y procesamiento de imágenes presentaron sus propias versiones del análisis de wavelets con nombres tales como "codificación de subbandas", "filtros de duplicación de cuadratura" y "algoritmo piramidal".

Aunque no eran exactamente idénticas, todas estas técnicas tenían características similares. Descomponían o transformaban señales en partes que se podían localizar en cualquier intervalo de tiempo y que también se podían dilatar o contraer para analizar la señal a distintas escalas de resolución. Estos precursores de las wavelets tenían algo más en común, nadie que se encontrara al margen de comunidades especializadas individuales sabía de ellos. Pero en 1984, la teoría de las wavelets adoptó finalmente su carácter propio.

**Figura 23. Gráficos de varios tipos distintos de wavelets. (a) Wavelet de Haar, (b) Wavelet de Daubechies, (c) Wavelet de Morlet**




Hasta ahora, la principal aplicación excepcional de las wavelets ha sido la compresión de imágenes digitales. Son el eje central del nuevo estándar de imágenes digitales JPEG-2000 y del método WSQ (del inglés *Wavelet Scalar Quantization*, Cuantización escalar de wavelets) que utiliza el FBI para comprimir su base de datos de huellas dactilares. En este contexto, se puede pensar en las wavelets como los componentes básicos de las imágenes. Una imagen de un bosque puede estar formada por las wavelets más amplias: una gran franja de verde para el bosque y una mancha de azul para el cielo. Las wavelets de mayor detalle y nitidez se pueden utilizar para distinguir un árbol de otro. Es posible añadir ramas y agujas a la imagen con wavelets aún más finas. Al igual que una pincelada de un cuadro, cada wavelet no es una imagen en sí, pero muchas

wavelets juntas pueden recrear cualquier cosa. A diferencia de una pincelada de un cuadro, una wavelet puede hacerse arbitrariamente pequeña: una wavelet no tiene limitaciones físicas de tamaño porque sólo se trata de una serie de ceros y unos almacenados en la memoria de una computadora.

En contra de la creencia popular, las wavelets en sí no comprimen una imagen: su finalidad es permitir la compresión. Para comprender por qué, supongamos que una imagen se codifica como una serie de números distribuidos en el espacio, tales como 1, 3, 7, 9, 8, 8, 6, 2. Si cada número representa la oscuridad de un píxel, siendo 0 el blanco y 15 el negro, esta cadena representa una especie de objeto gris (los 7, 8 y 9) sobre un fondo claro (los 1, 2 y 3).

El tipo más sencillo de análisis multiresolución filtra la imagen calculando el promedio de cada par de píxeles adyacentes. En el ejemplo anterior, el resultado es la cadena 2, 8, 8, 4: una imagen de menor resolución que todavía muestra un objeto gris sobre un fondo claro. Si quisiéramos reconstruir una versión degradada de la imagen original a partir de esto, podríamos hacerlo repitiendo cada uno de los números de la cadena: 2, 2, 8, 8, 8, 8, 4, 4.

Sin embargo, supongamos que queremos recuperar la imagen original perfectamente. Para hacerlo, tendríamos que guardar en primer lugar cierta información adicional, es decir, un conjunto de números que se puedan añadir o restar a la señal de baja resolución para obtener la señal de alta resolución. En el ejemplo, esos números son -1, -1, 0 y 2. (Por ejemplo: al añadir -1 al primer píxel

de la imagen degradada, el 2, se obtiene 1, el primer píxel de la imagen original; al restarle -1 se obtiene 3, el segundo píxel de la imagen original).

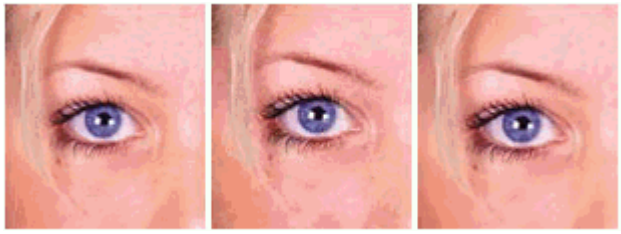
Por tanto, el primer nivel del análisis multiresolución divide la señal original en una parte de baja resolución (2, 8, 8, 4) y una parte de alta frecuencia o "detalle" (-1, -1, 0, 2). Los detalles de alta frecuencia se denominan también coeficientes de wavelets de Haar. De hecho, todo este procedimiento es la versión multiresolución de la transformación de wavelets que Haar descubrió en 1909.

Puede parecer que no se ha ganado nada en el primer paso de la transformación de wavelets. Había ocho números en la señal original y siguen habiendo ocho números en la transformación. Pero, en una imagen digital típica, la mayoría de los píxeles se parecen mucho a sus vecinos: los píxeles del cielo se encuentran junto a los píxeles del cielo, y los píxeles del bosque junto a píxeles del bosque. Esto significa que los promedios de los píxeles próximos serán casi iguales que los píxeles originales y, por tanto, la mayoría de los coeficientes de detalle serán cero o estarán muy próximos a cero. Si simplemente redondeamos estos coeficientes a cero, entonces la única información que necesitamos conservar es la imagen de baja resolución junto con algunos coeficientes de detalle que no se hayan redondeado a cero. Por consiguiente, la cantidad de datos necesarios para almacenar la imagen se ha comprimido con un factor próximo a 2. El proceso de redondeo de números de gran precisión a números de baja precisión con menos

dígitos se denomina cuantización (la "Q", del inglés "*quantization*", en "WSQ"). Un ejemplo es el proceso de redondeo de un número en dos cifras significativas.

El proceso de transformación y cuantización se puede repetir tantas veces como se desee, y cada vez disminuirán los bits de información según un factor de casi 2 y se degradará ligeramente la calidad de la imagen. En función de las necesidades del usuario, el proceso se puede detener antes de que la resolución baja comience a apreciarse o continuar hasta obtener una imagen "en miniatura" de muy baja resolución con capas de detalles cada vez más precisos. Con el estándar JPEG 2000, se pueden conseguir índices de compresión de 200:1 sin diferencias perceptibles en la calidad de la imagen. Tales descomposiciones en wavelets se obtienen al calcular el promedio de más de dos píxeles próximos cada vez. La transformación de wavelets de Daubechies más simple, por ejemplo, combina grupos de cuatro píxeles, mientras que otras más suaves combinan seis, ocho o más.

**Figura 24. Degradación de la imagen al aplicar Wavelets**



Las wavelets permiten comprimir imágenes con muy poca degradación de la calidad[*]. De izquierda a derecha, imagen original, la misma imagen comprimida en una proporción de 200:1 mediante tecnología JPEG estándar y la misma imagen comprimida en la misma proporción mediante JPEG 2000, un método que utiliza wavelets.

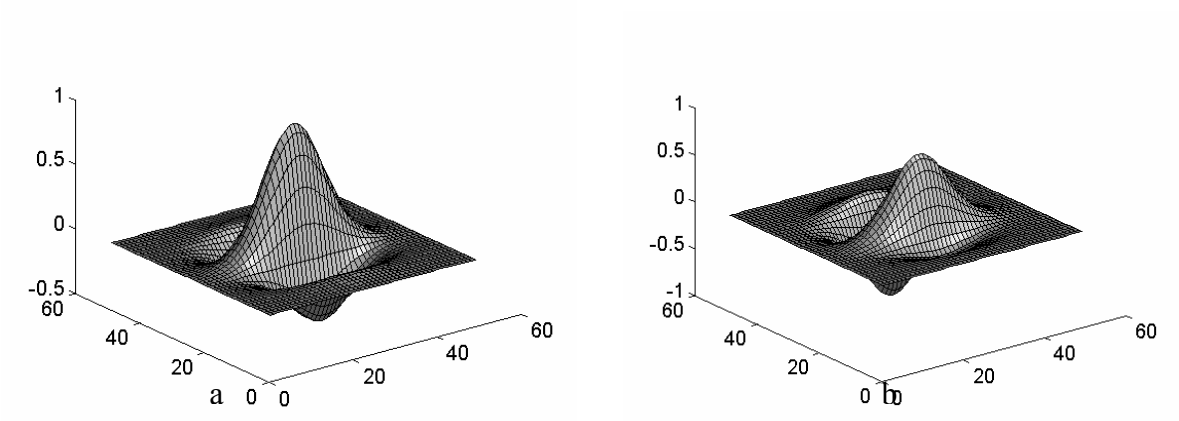
Una propiedad fascinante de las wavelets es que eligen automáticamente las mismas características que nuestros ojos. Los coeficientes de las wavelets que quedan aún tras la cuantización corresponden a píxeles que son muy distintos a sus vecinos, en el borde de los objetos de una imagen. Por tanto, las wavelets recrean una imagen principalmente trazando bordes, que es exactamente lo que hacen los humanos cuando esbozan un dibujo. De hecho, algunos investigadores han sugerido que la analogía entre las transformaciones de wavelets y la visión humana no es accidental, y que nuestras neuronas filtran las señales visuales de forma parecida a las wavelets.

[*] Trasformada Wavelet, Teoría y Aplicación - Jorge Osmar Lugo -Trabajo de Laboratorio IIFaCENA. 1999

### 3.6.2 CODIFICACIÓN

La mayor parte de los sistemas de análisis del iris se basan en el software creado por John Daugman, El cual a partir de una imagen del iris con todas sus pequeñas depresiones, elevaciones y finas cadenas que lo hacen único se elabora una serie de mapas de contorno tridimensionales que se comprime en un código binario de 2048 dígitos de longitud.

**Figura 25. Codificación de la señal: a. parte real - b. parte imaginaria**



Para lograr todo esto es necesario emplear operaciones de desmodulación matemática empleando las transformada wavelet de Gabor.

El patrón detallado del iris es codificado en un código de 256 bytes, el cual representa todos los detalles de la textura empleando fasores en el plano complejo.

Los filtros de gabor son los encargados de la codificación de la imagen. El procedimiento que se realiza para la codificación es una convolución entre las coordenadas polares de la imagen I(r,$\theta$) y un conjunto de filtros en cuadratura selectivos en frecuencia y centrados en la posición ($r_0$ , $\theta_0$) que son generados por medio de las variables $\alpha$ y $\beta$ que varían en proporción inversa a w (frecuencia).

La ecuación para la codificación de iriscode es:

$$I(r,\theta) * h(r,\theta)$$

$$\int_{\rho}\int_{\phi} I(\rho,\phi)\ell^{(-iw(\theta_0-\phi))}\ell^{\left(-\frac{(r_0-\rho)}{\alpha^2}\right)}\ell^{\left(-\frac{(\theta_0-\phi)^2}{\beta^2}\right)}\rho.d\rho.d\phi$$

Al aplicar esta operación sobre la imagen obtenemos una serie de códigos que representen las superficies circulares que vemos en el iris pero como si las estiráramos. La siguiente figura muestra las líneas de contorno sobre el iris y su respectiva codificación.

**Figura 26. Mapa del Iris.**

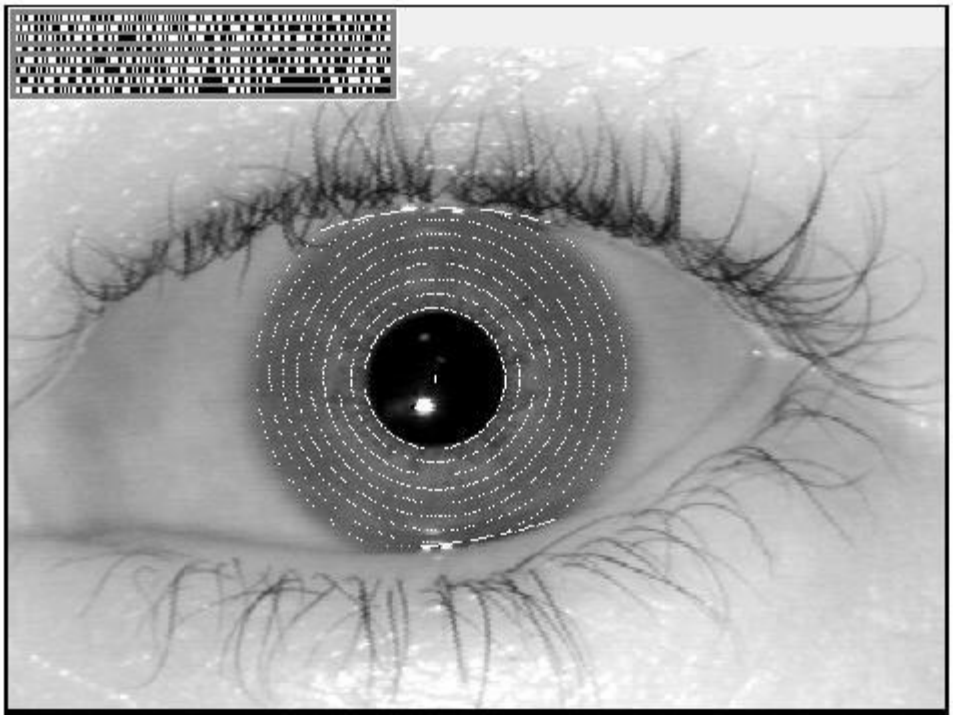
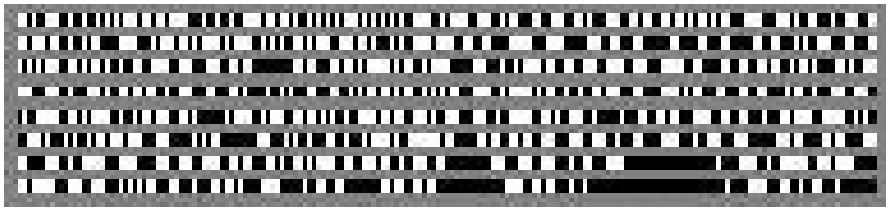


**Figura 27. Código generado del patrón del iris (iriscode)**



## 3.7 IDENTIFICACIÓN DEL CÓDIGO

### 3.7.1 COMPARACIÓN DEL CÓDIGO PARA IDENTIFICACIÓN DEL IRIS

#### 3.7.1.1 Código de Hamming

El método mas común para la identificación del iris por comparación es utilizando la distancia de hamming. En el que se miden las diferencias que existe entre dos códigos binarios. Este código también se conoce como Código corrector de errores de n bits, la idea es mantener el error lo menor posible con relación a un error deseado.

La distancia de Hamming entre dos cadenas de bit (números enteros binarios) es el número de las posiciones de bit correspondientes que los diferencian[*]. Esta puede ser encontrada usando la función XOR.

Por ejemplo, en las dos secuencias de bit que siguen:

A = 0100101000

B = 1101010100

A XOR B = 1 0 0 1 1 1 1 1 0 0

[*] Richard W. Hamming. Coding and Information Theory. Segunda edición, Prentice Hall, 1986

La distancia de Hamming HD entre estas secuencias 10-bit es 6, el número de 1 en la secuencia de XOR.

La distancia de Hamming se mide en porcentaje por ejemplo:

$$\%HD = \frac{A \otimes B}{n} = \frac{\left\| 0100101000 \otimes 1101010100 \right\|}{10} = \frac{6}{10} = 0.6$$

Donde n es el numero bit que conforman el dato en esta caso es de 10 bit.

La distancia de Hamming será del 60%.

El proceso de comparación del iris con una base de dato, se realiza por medio de la operación antes descrita, entre los valores de cada píxel que componen las imágenes, los cuales son datos de 4 bit que van desde 0 para el negro hasta 255 para el blanco. Para lograr una aceptación en la comparación hay que fijar un valor máximo a la distancia de Hamming que en el caso de Daugman, fue menor de 0.3. Para lograr este valor se vio en la necesidad de eliminar los factores que hacen que haya discrepancia en los códigos. En base a esto halló la siguiente expresión:

$$HD = \frac{\left| (Codigo\ A \otimes\ Codigo\ B) \cap MaxkA \cap MaxkB \right|}{\left| MaxkA \cap MaxkB \right|}$$

***HD = Distancia de Hamming***

***Código A = Código a comparar***

***Código B = Código con el que se compara***

***Maxk A = Información de códigos no deseados del código a comparar.***

***Maxk B = Información de códigos no deseados del código con el que se compara.***

Maxk A y Maxk B son los factores que nos sirven para eliminar información no propia del iris como pestaña, párpado y reflejo, que ocasionan que la distancia de Hamming sea mayor que la deseada, que debe ser menor al 30% esto es HD = 0.3.

## 3.8 RECONOCIMIENTO DE IRIS UTILIZANDO REDES NEURONALES AUTO ORGANIZADORAS

El sistema esta constituido por dos partes principales: localización del iris y el reconocimiento de patrones del iris. Utilizando una cámara digital la imagen es capturada, luego se extrae el iris de la cara, se aumenta, se mejora y por ultimo se elimina el ruido de la imagen. Debido al ruido y al alto grado de libertad en el patrón del iris, solo partes de la estructura son seleccionadas para el reconocimiento. La estructura seleccionada del iris es entonces reconstruida en un formato rectangular. Utilizando un mapa neuronal auto organizador[*] entrenado, los patrones del iris son reconocidos.

La estructura del iris es imposible de cambiar sin riesgos inaceptables en la visión. Hoy en día, con las ventajas del desarrollo de la tecnología computacional y algoritmos artificiales inteligentes, el sistema de reconocimiento de iris puede ganar rapidez, simplicidad de hardware, precisión y aplicabilidad.

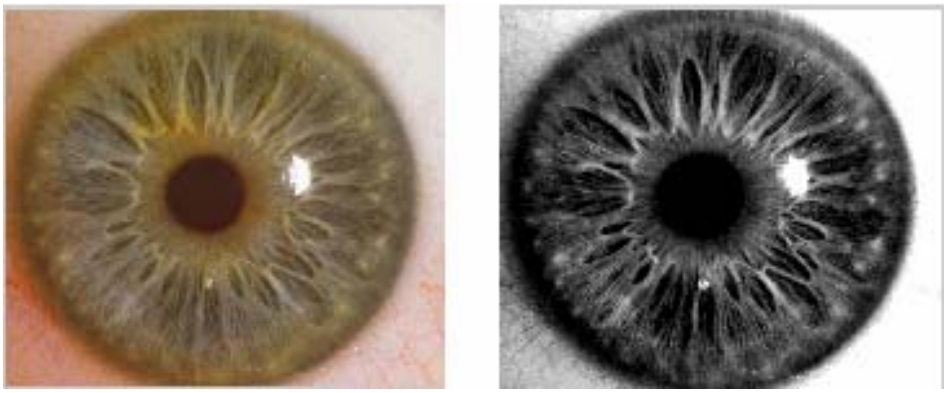
[*] Hinton, G.E. (1992) Redes neuronales que aprenden de la experiencia. Investigación y ciencia Noviembre 1992.

### 3.8.1 LOCALIZANDO EL IRIS

Es imposible capturar la imagen del iris manualmente. Normalmente, una imagen más grande que contiene el iris es capturada. La porción de la imagen adquirida que corresponde a un iris será localizada para realizar una comparación de patrones de iris. La pupila normalmente es más oscura que el iris. El iris es más oscuro que los alrededores al lado del párpado. El contraste del párpado es bastante variable; depende de la piel relativa del individuo. Los párpados o pestañas normalmente cubren las porciones superior e inferior del iris. El iris y pupila normalmente tendrán un menor contraste que en los alrededores.

La imagen del ojo es primero capturada utilizando una imagen digital. Las imágenes son sometidas a procesos de mejoramiento del contraste sin cambiar el patrón del iris. La imagen es entonces convertida a una imagen binaria. La técnica de umbral une la pupila y el iris. En algunos casos, un bajo contraste del párpado relativo al iris se juntará con el iris después del umbral. Generalmente el iris tiene una forma de disco y nosotros obtendremos una forma redonda de la técnica de umbral.

**Figura 28. a. Imagen original b. Imagen binaria**



a b

El iris y la pupila pueden ser extraídos del fondo buscando el disco en la imagen. Primero, creamos una máscara en forma de anillo con grosor de un píxel. El radio **r** cambiará de acuerdo a un valor. En el estado inicial, ponemos el radio en un valor inicial que es más pequeño que el radio verdadero del iris. La máscara correrá a través de toda la imagen. Esto se expresa matemáticamente mediante la siguiente ecuación:

$$S = \sum_{\theta=0}^{\theta=2\pi} I\left(x + r\cos\theta, y + r\sin\theta\right)$$

La cual resume el cálculo del umbral para mejorar el radio **r**.

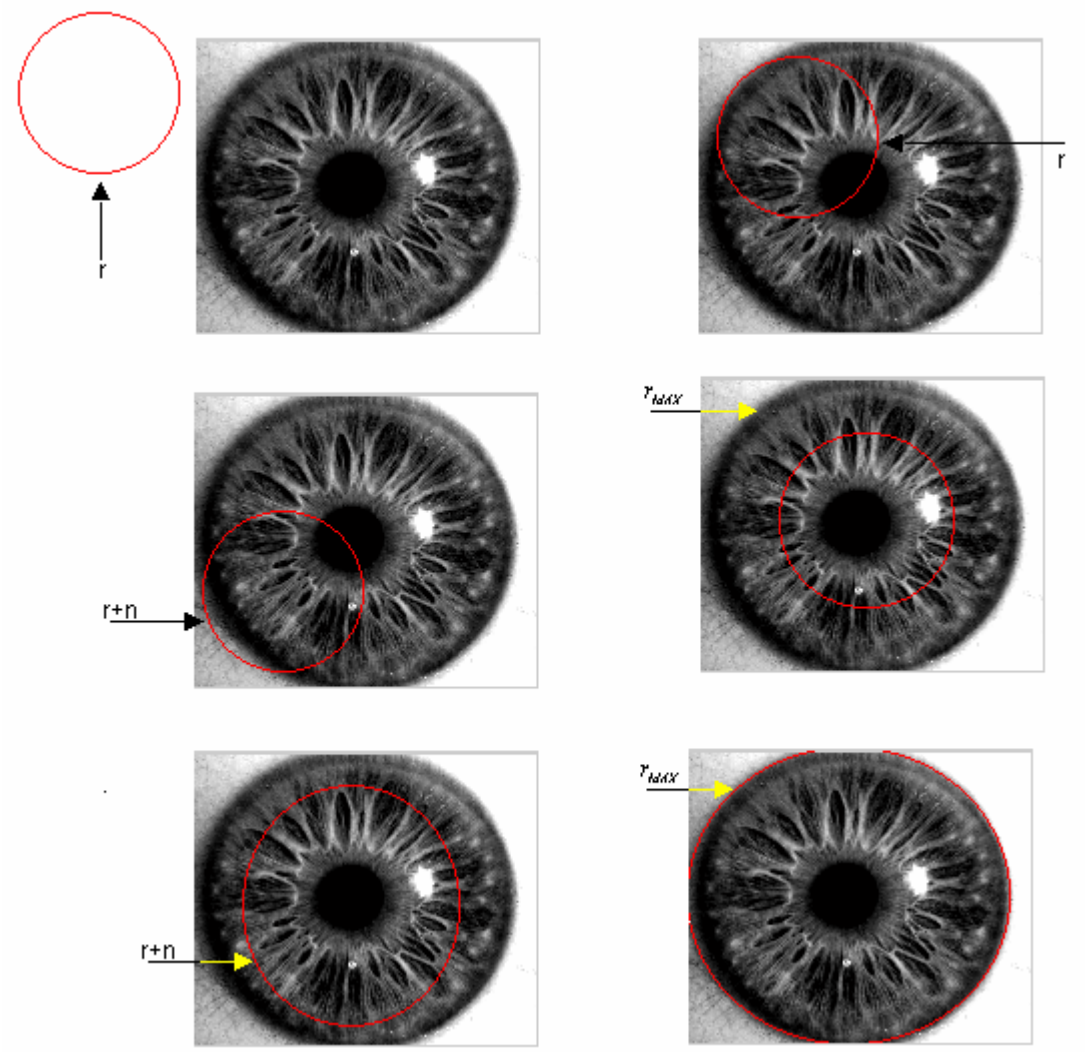
Donde:

x,y = coordenadas centrales del anillo

r = radio del anillo

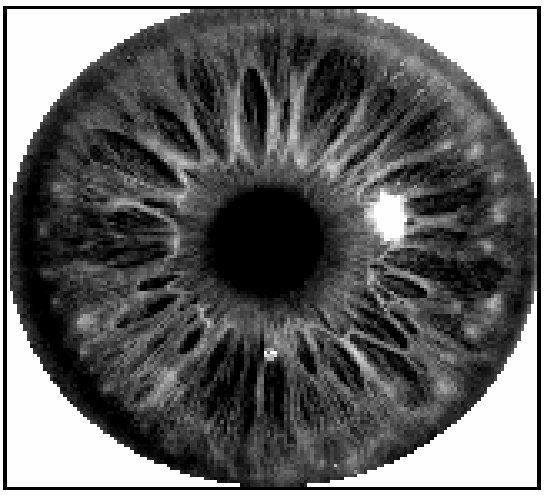
Cuando el valor de ***S*** es más pequeño que el umbral, en las mismas coordenadas centrales, el radio será aumentado. La coordenada central del iris es igual a la coordenada central de la máscara donde tiene el radio **r** más grande.

**Figura 29. Pasos tomadas para la extracción dela coordenada central y radio del iris**



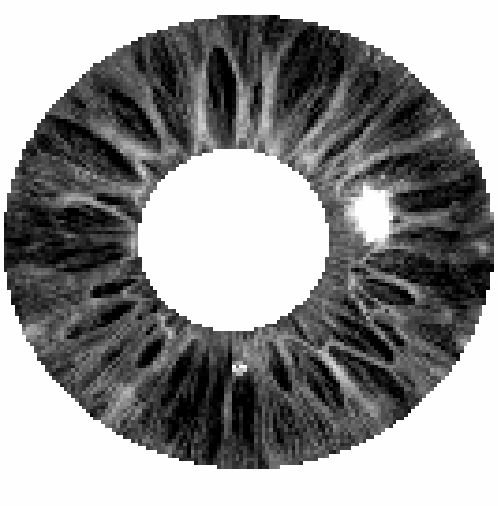
Utilizando la coordenada central y el radio del iris, este fue recortado de la imagen y posteriormente reconstruida utilizando el método de ventana cuadrada.

**Figura 30. Reconstrucción de iris y pupila**



De la imagen extraída, la información del iris puede ser transformada en un formato deseable. Aquí solo necesitamos tomar una parte de la estructura del iris para reconocimiento. Los bordes del iris estarán probablemente cubiertos por los párpados o pestañas y distorsionados por la reflexión, por lo tanto tomamos solo la parte central del iris para reconocimiento. Tomando una parte de los datos del iris solucionamos también el problema de eliminación de la pupila del iris.

**Figura 31. Información de iris extraída**



Las transformaciones de un iris en forma de dona a un iris en forma de rectángulo están expresadas por la siguiente ecuación:

$$I(n, r - p) = I(r, \theta_n)$$

donde:

n = entero 1, 2, 3.....m

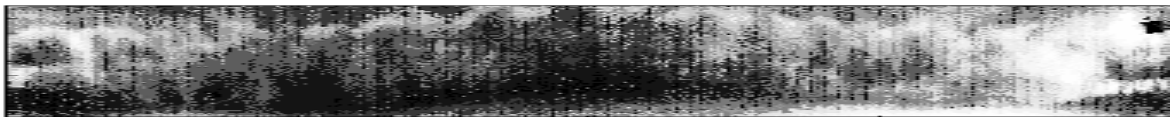
p = es un parámetro

r = radio

$$\theta_n = 0, \frac{2\pi}{n}, \frac{4\pi}{n}, \frac{6\pi}{n}, .....2\pi$$

Utilizando el método de estiramiento de histograma, la imagen transformada es mejorada para una estructura de iris más clara como se muestra a continuación.

**Figura 32. Iris reconstruido en forma rectangular**



El iris en una forma rectangular está ahora listo para ser alimentado en el sistema para reconocimiento.

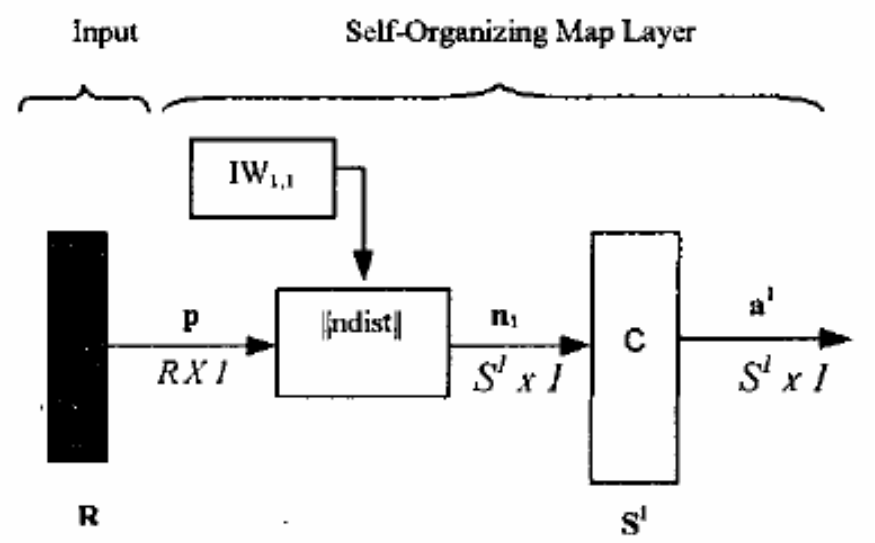
### 3.8.2 RECONOCIMIENTO DE PATRONES DE IRIS

Para el reconocimiento del patrón del iris se ha escogido el sistema de mapa auto organizador o de aprendizaje no supervisado. En este tipo de aprendizaje se presenta a la red una serie de ejemplos pero no se presenta la respuesta deseada. Lo que hace la red es reconocer regularidades en el conjunto de entradas, es decir, estimar una función densidad de probabilidad p(x) que describa la distribución de patrones x en el espacio de entrada Rn .

El sistema contiene una única capa de la función Euclineana de un solo peso. Donde **R** es la información de entrada, $IW_{1,1}$ es el peso del sistema y $a^{I}$ es la salida

del sistema. Las distancias Manhattan son usadas para calcular la distancia de una neurona x en particular a la neurona y en las inmediaciones.

**Figura 33. Arquitectura del mapa auto organizador**




Donde:

$n_1 = -|| IW_{1,1} – p ||$

$a^1 = f(n_1)$

Distancia Manhattan $= \sum \left\| \bar{x} - \bar{y} \right\|$

Donde:

$\bar{x}, \bar{y} =$ vector de localización de neurona

El sistema inicial con 25 neuronas, fue arreglado en una topología de cuadrícula con un valor de carga de 0.5. Todos los códigos de iris son alimentados en el sistema para reconocimiento.

# 4. APLICACIONES BASADAS EN EL RECONOCIMIENTO DEL IRIS

## 4.1 LA HISTORIA DE SHARBAT GULA (los ojos que ya no brillan)

***Luego de una búsqueda que incluyó el estudio de su iris, la National Geographic consiguió, 18 años después, a la ahora mujer que adornó una de sus portadas: Sharbat Gula. Tanto ayer como hoy, es el reflejo del drama afgano.***

**Figura 34. Sharbat Gula 18 años después**

El científico que inventó la fórmula matemática para "leer" la información que se desprende del iris John Daugman, profesor de la Universidad de Cambridge prefiere no entrar en disputas y explica uno de sus más famosos logros: la identificación de la chica afgana de 12 años y ojos esmeralda que fue tapa de la revista National Geographic en 1984 y que fue descubierta hace pocos meses por el mismo fotógrafo que la retrató 18 años atrás. El algoritmo inventado por Daugman permitió establecer que los ojos de esa mujer envejecida eran iguales a los de la de chica de la tapa de 1984.

Sharbat Gula nunca supo que su rostro, fotografiado por Steve McCurry para National Geographic, cautivaría por sus impresionantes ojos verdes. Y que no sólo fue la portada de junio de 1984 de la revista sino que también ilustra el libro de las mejores imágenes que ha reunido esa sociedad científica en su centenaria historia. Una cara, unos ojos que, 18 años después, ha sido encontrada y que enseña que su vida ha estado lejos de ser un jardín de rosas: No sabe exactamente qué edad tiene, 28, posiblemente 29, hasta 30. Ni ella ni los que la rodean están seguros, sólo están seguros del presente porque así como no hay registro del pasado, el futuro no es precisamente un camino de certidumbres. Y es que su rostro es la muestra de lo que una afgana o un afgano vive: la dureza del clima y de la vida en ese país está claramente marcado en sus rostro: de los ojos vivos que tenía de vida, ya casi no hay brillo. Siguen siendo hermosos, pero ya no son profundos. Del cutis ni se diga: la suavidad de la piel no existe y la piel más bien parece un cuero seco. En todo este tiempo, nunca supo ni se imaginó

que su rostro ha sido reproducido innumerables veces alrededor del mundo. Su nombre, según se lee en la página web de la National Geographic, tiene un significado especial dentro de la lengua de los pastún, tribu a la que pertenece Sharbat Gula: Niña Flor, y que refleja la admiración que tienen los afganos a las flores. Hallarla no resultó sencillo, pero fue reconocida con la ayuda de la alta tecnología de reconocimiento del iris.

## 4.2 AFGANISTÁN (Uso de tecnología avanzada aporta grandes beneficios)

***La siguiente información es un resumen de las declaraciones del vocero del ACNUR Kris Janowski durante la rueda de prensa del día 8 de agosto de 2003, en el Palacio de las Naciones en Ginebra, Suiza.***

De los 250.000 refugiados afganos que retornaron desde Pakistán este año, más de la mitad se ha sometido al examen de reconocimiento del iris en alguno de los tres centros de verificación ubicados en las regiones fronterizas de Pakistán.

Optamos por utilizar este sistema de reconocimiento biométrico a fin de evitar fraudes en la identificación. Este sistema se probó con éxito el año pasado en la

provincia fronteriza de Peshawar, al noroeste de Pakistán. Hasta el momento, más de 130.000 refugiados se han sometido al examen de reconocimiento del iris sin ningún tipo de inconveniente o protesta. Este proceso de verificación utiliza tecnología de avanzada y no es invasivo. Se pide a los posibles retornados que miren por un pequeño orificio mientras que una cámara captura un plano del iris. Cada iris fotografiado se guarda como una imagen, sin nombre, para simplificar el proceso y proteger la privacidad de los retornados. Luego se agrega la imagen a una base de datos computarizada que es compartida por los tres centros de validación del iris. El personal del ACNUR es notificado si alguien intenta someterse al proceso por segunda vez. En vistas de las sensibilidades culturales que no permiten que las mujeres afganas se quiten el velo en presencia de hombres, el ACNUR ha contratado a operadoras femeninas para procesar las imágenes de las mujeres y los niños refugiados. Recientemente, ampliamos el uso del examen de reconocimiento del iris en Pakistán para todos los refugiados a partir de 6 años (antes se realizaba a partir de los 12 años), ya que nuestro personal había notado que algunos niños que pasaban por el centro les resultaban familiares. Se cree que algunos afganos podrían haber estado haciendo pasar niños repetidamente por los centros de verificación a fin de recibir su paquete de asistencia más de una vez. Gracias a la tecnología de reconocimiento del iris, en lo que va del año, se identificó a alrededor de 600 personas que intentaban retornar por segunda vez para acceder a los beneficios correspondientes a su condición.

## 4.3 UN NUEVO DETECTOR DE TERRORISTAS EN LOS AEROPUERTOS

### 4.3.1 ESTADOS UNIDOS

Tras los atentados del 11 de septiembre comenzó a utilizarse el reconocimiento del iris para identificar a los pasajeros. Aseguran que este método es mucho mas seguro y preciso que el las huellas digitales. “Mire fijamente a la cámara, sin pestañear. ¡Click!”. En apenas un segundo, una computadora comparará sus ojos con millones de otros ojos y anunciará su veredicto: usted es un terrorista, un delincuente internacional, un inmigrante ilegal o un simple pasajero que acaba de descender de un avión.

No es un juego. Los atentados del 11 de septiembre pusieron en alerta total a los expertos en seguridad en aeropuertos y desde entonces viven desvelados por exprimir al máximo las nuevas tecnologías para combatir el terror o los visitantes indeseados. La respuesta la encontraron muy cerca de sus narices: rápido y sencillo, el sistema de reconocimiento del iris (la parte coloreada del ojo) comienza hoy a expandirse por importantes aeropuertos de Europa, Estados Unidos y

Canadá como uno de los métodos mas innovadores y seguros de chequeo de identidad de pasajeros.

**Figura 35. Sistema reconocedor del iris en los principales aeropuertos de los EE.UU**

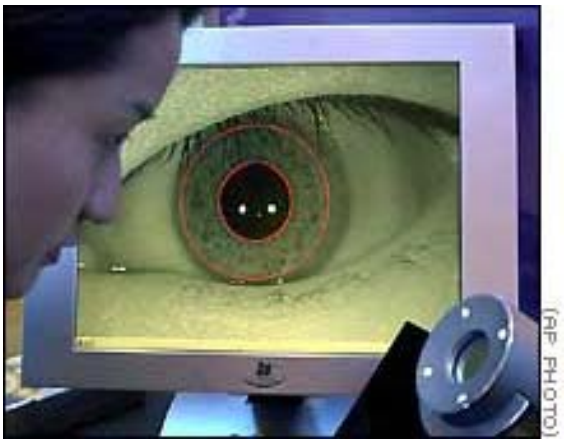
Los pasajeros deben ingresar a una cabina donde está el equipo especial. Una cámara digital controlada por computadora retrata el ojo y, casi instantáneamente determina la identidad del individuo comparando las características únicas de su iris con un banco de datos, donde la persona previamente había dejado información. El problema que se plantea para que este sistema sea realmente efectivo en la lucha contra el terrorismo es que se necesitará bastante tiempo para que exista un banco de datos universal. Además, muchos plantean dudas sobre el destino de la información recolectada. En un país como Gran Bretaña, por

ejemplo, donde los habitantes no poseen ni siquiera un Documento Nacional de Identidad, el método levanta algunos interrogantes.

### 4.3.2 EUROPA

***AEROPUERTO HOLANDÉS UTILIZA CON ÉXITO UN SISTEMA BIOMÉTRICO DE SEGURIDAD***

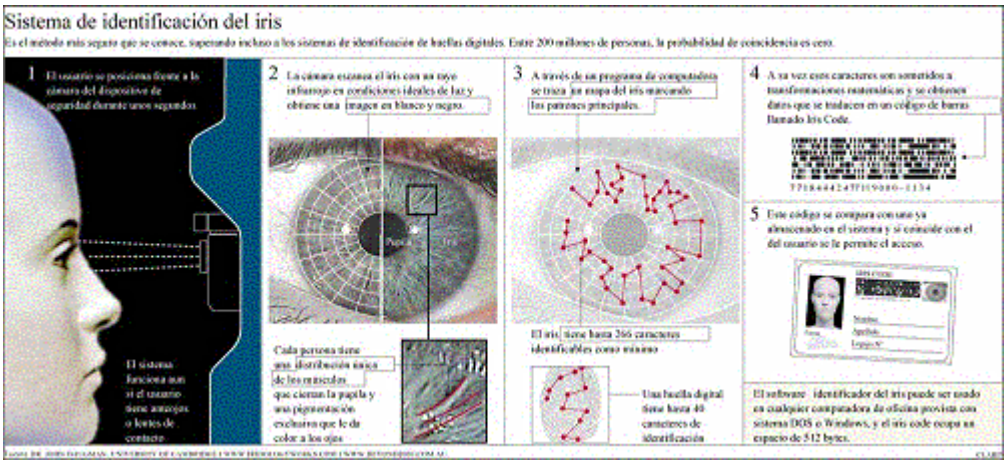
**Figura 36. Dispositivo utilizado para el reconocimiento del iris en el aeropuerto de ÁMSTERDAM**



ÁMSTERDAM, Holanda -- El aeropuerto Schiphol de Ámsterdam está utilizando con éxito un sistema de seguridad biométrico basado en el escaneo del iris que evita a los pasajeros los tediosos controles de pasaporte.

Schiphol es uno de los grandes aeropuertos europeos que utiliza avanzadas tecnologías para recuperar la confianza de los viajeros tras las suspicacias levantadas por los atentados del 11 de septiembre. El proyecto del aeropuerto Schiphol llamado Privium, Los pasajeros introducen primero sus datos personales. A continuación se toma una fotografía de su iris el diafragma de color que controla el tamaño de la pupila y se registra en una tarjeta parecida a una de crédito.

**Figura 37. Tarjeta personal de identificación por medio del iris con su respectivo código**



Una vez realizado el registro, los pasajeros acceden a las terminales aéreas insertando la tarjeta y mirando en el escáner, que compara los ojos con la información contenida en la tarjeta. Privium está pensado para los hombres de negocios que viajan con el tiempo justo. "Los controles de pasaporte y visados más rápidos pueden demorar hasta 30 minutos", indicó Kuypers. "El control biométrico, en el que invertimos tres años para desarrollarlo, sólo tarda diez segundos... es ideal para los viajeros de negocios".

### 4.3.3 EMBARQUE EN AVIÓN POR RECONOCIMIENTO DE IRIS

Más de 2000 ciudadanos americanos, que viajaban muy frecuentemente al Reino Unido entran a formar parte de un programa piloto de reconocimiento del iris para cuestiones de embarque y desembarque en los aeropuertos.

**Figura 38. Dispositivo utilizado para el reconocimiento del iris en el aeropuerto británico de Heathrow**

El aeropuerto británico de Heathrow, ha sido el escogido para implantar un sistema de reconocimiento del iris y permite la identificación de los usuarios en tiempo real a través de un banco de datos previamente recogido. El sistema de biometría aplicado a la identificación se basa en ciertos elementos morfológicos únicos y propios de cada persona como el iris, de manera que sólo la presencia física del usuario permite acceder al sistema. Tras realizar el correspondiente examen, el dispositivo biométrico se comunica con los ordenadores del aeropuerto y de la línea aérea para simplificar el control de pasaportes y el resto de registros rutinarios.

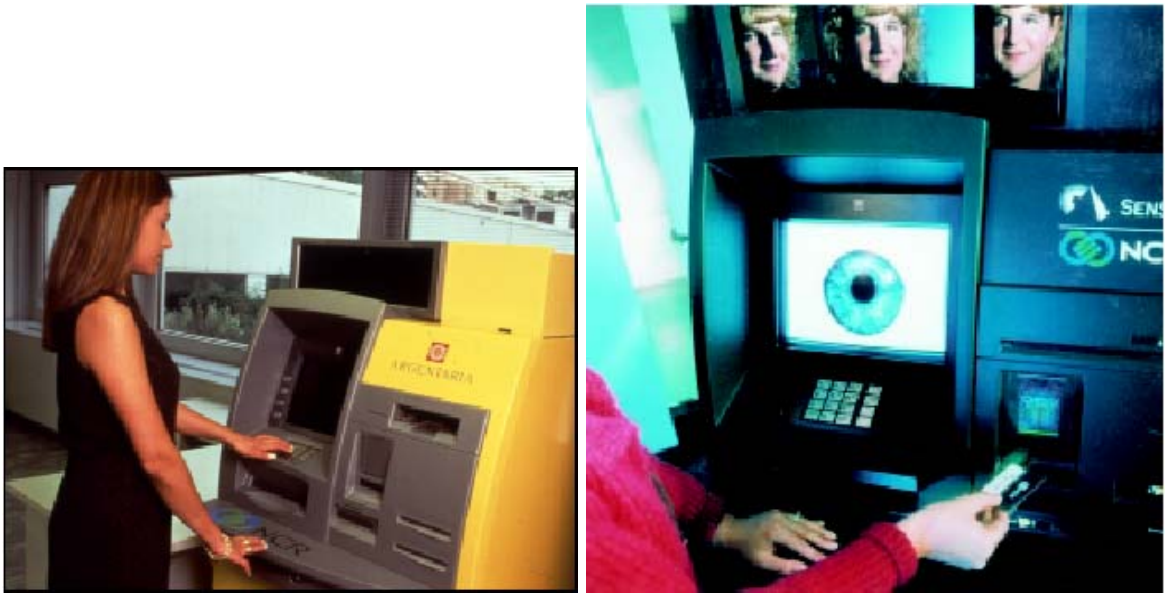
## 4.4 RECONOCIMIENTO DEL IRIS APLICADO EN LOS CAJEROS AUTOMÁTICOS

El iris es un componente de la anatomía realmente estable e inalterable que permite identificar a un individuo de una forma tan precisa como la huella dactilar. Alguna de sus aplicaciones mas interesantes se ha llevado acabo en cajeros automáticos, para verificar la identidad de los clientes de un banco, es como el caso del nuevo dispensador puesto en marcha recientemente por Argentaria en una de sus sucursales de Madrid. Se trata de un cajero automático que, diseñado por la compañía NCR, incorpora un sistema de reconocimiento de iris que sustituye la tradicional identificación mediante el numero secreto personal ó PIN.

Para realizar cualquier transacción, el cliente ha de situarse frente a este cajero, el primero de este tipo instalado en España, para que el sistema de identificación del iris lo reconozca. El sistema, por tanto, fotografía el ojo y transforma la imagen en dígitos. Una vez convertida en un código, esa información es contrastada con los datos almacenados en el archivo, que confirma si el usuario es o no el propietario de la tarjeta. El sistema genera así una imagen digital del iris del cliente y graba la tarjeta de banda magnética o chip con la nueva funcionalidad integrada. De esta forma, se obtiene una gran seguridad en cuanto al acceso a datos financieros ya que, si la huella del iris del usuario no coincide con la existente para ese cliente,

no se le ofrece ese servicio. Hay que tener en cuenta que la probabilidad de encontrar dos iris iguales es prácticamente nula.

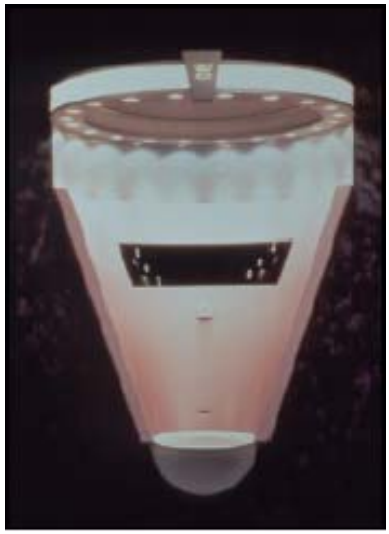
**Figura 39. Cajero automático Argentaría utilizando el sistema de reconocimiento del iris diseñado por la NCR**



El Royal Bank de Canadá es otra de las entidades que dispone de un cajero automático de este tipo desarrollado por NCR, denominado STELLA. Este dispensador es capaz de reconocer al usuario, saludarlo por su nombre, escucharlo, hablarle, ofrecerle un menú personal con sus servicios y funciones favoritas, e incluso felicitarle el día de sus cumpleaños si decide realizar cualquiera transacción en esta fecha. Las nuevas tecnologías en las que se basan STELLA

incluyen la biometría ó el sistema de reconocimiento del iris, el reconocimiento de la voz, que permite hablar con el terminal como con un empleado del banco, y un sistema integrado capaz de comunicarse con el teléfono móvil del usuario y descargar la información de las ultimas operaciones realizadas en el asistente personal digital (PDA).

**Figura 40. Cajero automático STELLA del Royal Bank de Canadá**



Por tanto, las posibilidades que ofrece esta nueva tecnología son apreciadas por la mayor parte de sus usuarios. De hecho, la aceptación del sistema de reconocimiento del iris en las pruebas piloto de cajeros automáticos que NCR tiene instalados en el banco británico Nationwide Building Society ha sido masiva.

Según un estudio realizado por Pegram Walters Group, realizado entre 1.000 clientes durante seis meses en el Reino Unido, la totalidad de los usuarios de este dispensador consideran que el sistema es fiable y seguro.

# 5. DISPOSITIVOS

La demanda creciente para las medidas de seguridad ha llevado a la creación de dispositivos capaces de brindar un mejor vivir. Es así como ***iridian technologies*** junto con una determinada familia de distribuidores brinda sus servicios con los sistemas de reconocimiento de iris, los cuales después de los atentados del 11 de septiembre  estos dispositivos son los mas seguros en cuanto al acceso se refríe.

## 5.1 CÁMARAS PANASONIC BM-ET300 Y BM-ET500

**Figura 41. cámaras panasonic BM-ET300 Y BM-ET500**

### 5.1.1 ESPECIFICACIONES DEL PRODUCTO

**Tabla 5. comparación de las cámaras BM-ET300 Y BM-ET500**

| | BM-ET300 | BM-ET500/ED500 |
|---|---|---|
| APARIENCIA |  |  |
| DETECCIÓN DEL IRIS | INCLINACIÓN DE LA CÁMARA MANUAL | CÁMARA AUTOMÁTICA |
| Tiempo mínimo de reconocimiento | 1.5 Sec | 3.0 Sec |
| Máx. Datos registrados por la cámara | 1000 usuarios | 1000 usuarios |
| Máx. Datos registrados por el sistema | 5000 usuarios | 2000 usuarios |
| Manejo de cerradura eléctrica | No | Si |
| Peso | Aprox. 5 Kg. | Aprox. 10 Kg. |
| Dimensions (W×H×D) | 210 x 215 x 63 mm | 430 x 211 x 80 mm (ET500), 380 x 410 x 90 mm (ED500) |
| Rendimiento de la alarma | Bajo poder de rechazo, falsa aceptación de reconocimiento | Alto poder de rechazo, falsa aceptación de reconocimiento |

| | | |
|---|---|---|
| **Power** | **DC12V or AC 24V** | **DC 32V or DC 24V (AC 100V – 220V for ED500)** |
| **Temperatura** | **0 – 40 grados C** | |
| **Humedad** | **30% - 80%** | |
| **Lugares en los que son imposible de instalar** | • **Luz de sol directa a la cámara**<br>• **Cerca de alta potencia en vatios y lámparas de halógeno**<br>• **La reflexión ligera hacia la cámara (los espejos)**<br>• **Luz extrema u oscuro**<br>• **Los niveles de ruido alto**<br>• **Vibraciones de superficie alta** | |
| **Funcionamiento** | **Tarifa de la identificación: 99,9% o más alto**<br>**Tarifa falsa de la aceptación: 0,000083% o menos**<br>**(* depende de calidad capturada de la imagen)** | |
| **(Ref.) Fuerza infrarroja del tablero delantero** | **Con 500 micro W / cm2** | **Con 150 micro W / cm2** |

### 5.1.2 CONFIGURACIÓN DE RED BÁSICA

**Figura 42. Configuración de la red básica para un control de acceso**

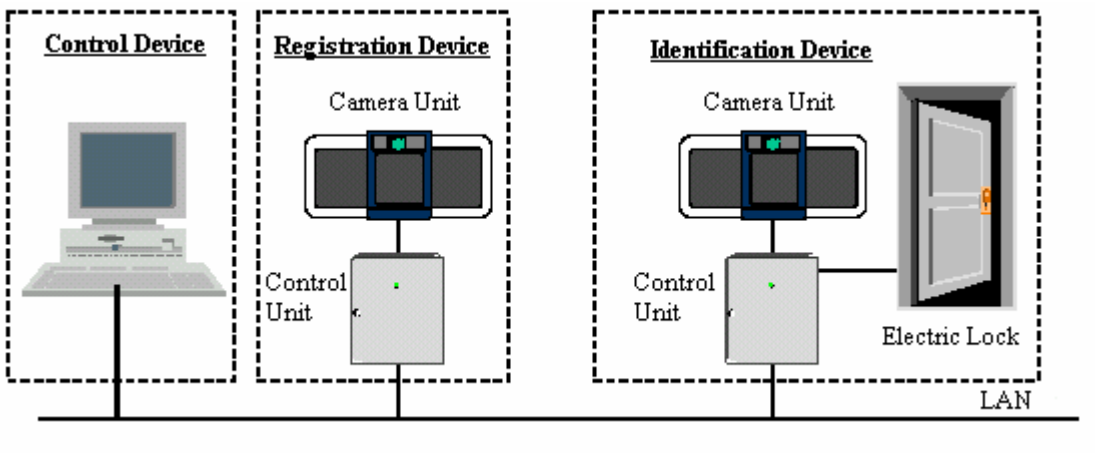



**Figura 43. Dispositivo del registro de la identificación**

Es posible utilizar una unidad de control para el dispositivo del registro y el dispositivo de la identificación. (nota: ambiente y operación de la instalación limitada).

El máximo 2 unidades de la cámara fotográfica se puede conectar con el dispositivo de la identificación. (nota: operación limitada)

## 5.2 CÁMARA IRISPASS – h

**Figura 44. Cámara OKI IRISPASS-h**

Irispass-h es un dispositivo de bolsillo conveniente, el peso es ligero, fácil operar y permite construir un sistema seguro y ha bajo costo.

### 5.1.3 ESPECIFICACIONES DEL PRODUCTO

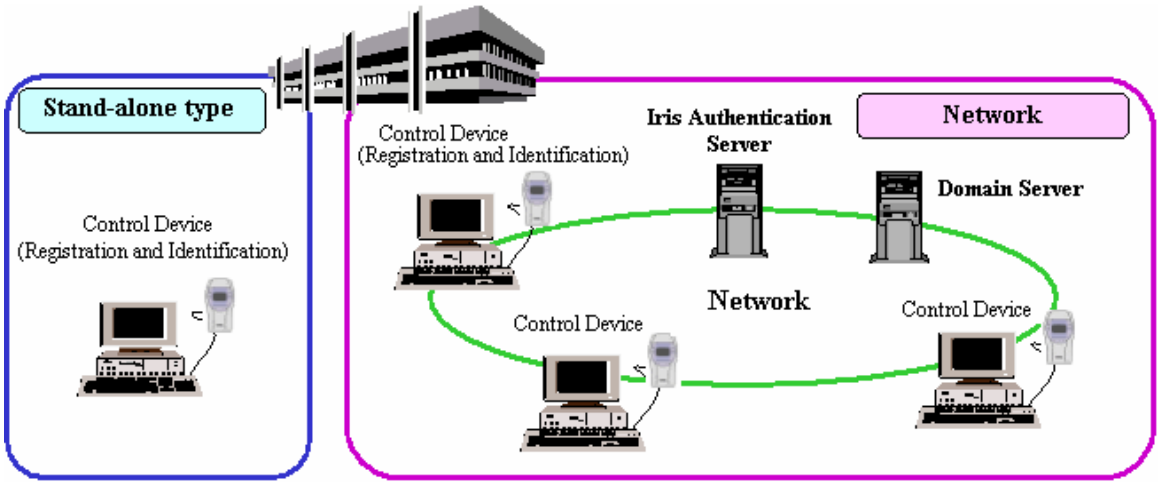
**Tabla 6. Especificaciones de la cámara OKI IRISPASS-h**

| Producto | | Especificaciones |
|---|---|---|
| Actuación | Rata de identificación | 99.9% or higher |
| | Rata de falsa aceptación | 0.000083% or less |
| Velocidad de identificación | | 1 segundo aprox. el Software en la computadora con Pentium III 600MHz procesador |
| Nombre del producto | | IRISPASS-h |
| Modelo No. | | EQ5009A |
| Interface | | Connectivity: USB |
| Energía proporcionada | | Conexión vía USB |
| Energía consumida | | 300mA, máxima |
| Ambiente | Temperatura de operación | 5°C~35°C |
| | Humedad que opera | 30%~85%(30°C) |
| Tamaño (mm) | | 59(Ancho) x 121(alto) x 52(profundidad) |

| | | |
|---|---|---|
| **Peso** | | 160g (incluyendo cables) |
| **Apoyo** | **Servidor** | Windows NT 4.0 Server (*1) |
| | **Cliente autónomo** | Windows 2000 (*1) |
| **Requerimientos del sistema** | **CPU** | Pentium II 400 MHz or faster |
| | **Memoria** | 128 MB, minimo |

### 5.1.4 CONFIGURACIÓN DE LA RED BÁSICA

**Figura 45. Configuración de una red básica para el control de acceso**



## 5.2 CÁMARA LG 3000

**Figura 46. Cámara reconocedora del iris LG 3000**

IRIS ACCESS 3000 de LG utiliza el elemento más individual del cuerpo humano, el iris. Una vez usted registra su iris en la unidad de enrolamiento **EOU 3000** esta es grabada en una base de datos que transmite remota a unidades **ROU 3000** para permitir el acceso.

La unidad Óptica de Registro debe ser colocada sobre un escritorio o mesa adyacente al Servidor o PC. Contiene todos los elementos necesarios para iniciar el proceso de registro, iluminar el iris y adquirir la imagen de iris; la unidad de registro provee un mensaje de voz y un indicador de luz informando que el registro del iris está completo. * **Unidad Óptica Remota:** Debe ser instalada adyacente a la puerta que será controlada. Esta unidad esta compuesta de dos partes, la unidad óptica de imagen y el panel para montaje; esta unidad contiene los elementos necesarios para la adquisición de la imagen, el mismo provee un mensaje de voz y una indicación de luz informando si la unidad esta funcionando o no. * **Unidad de Control de Identificación:** Esta unidad debe ser instalada en la pared en un área protegida y de seguridad. Este equipo compara el Iris Code con un grabado pre-memorizado del Iris. Si un Iris Code está registrado, la unidad ICU 3000 genera una señal para abrir la puerta. Esta unidad de Control de identificación puede controlar hasta 4 puertas. * **Tarjeta Interfaz con la Puerta:** Tarjeta de video Análogo que digitaliza la imagen para procesar en el servidor.

## 5.3 CAMARA PANASONIC BM-ET100US

**Figura 47. Cámara panasonic BM-ET100US reconocedora del iris**


La cámara incluye el IDTM Cliente Software Privado para el software-PC de protección autosuficiente.

La multifunción de la Cámara puede proporcionar una seguridad alta con un control de acceso ó vigilancia de software.

El primer producto de la alianza de Panasonic con Iridian es Panasonic AuthenticamTM, introducido en el tercer cuarto del 2001. Panasonic AuthenticamTM emplea la tecnología de reconocimiento del iris Tecnología de Iridian para las aplicaciones de acceso de información, como el acceso de la red y autorización de tarjeta de crédito. Panasonic Authenticam viene atado con un programa llamado IDTM Privado para las aplicaciones autosuficientes en las computadoras individuales. Los productos de reconocimiento de iris como el Panasonic Authenticam no requieren ningún contacto o procedimientos de contacto para la identificación.

**Figura 48. Panasonic Authenticam TM sistema de control de acceso para computadoras portátiles**

# 6. SISTEMAS DE CONTROL DE ENTRADA A RECINTOS EN COLOMBIA

El creciente mejoramiento en los procesos productivos y de seguridad han generado la necesidad de mantener bajo el mas estricto control y confiabilidad el desplazamiento de seres humanos al interior de las empresas. Los tiempos desperdiciados, los accesos no deseados y los costos de liquidación de horas laboradas son aspectos a mejorar día a día dentro de los estándares competitivos actuales.

En a la Actualidad en nuestra país existen varias empresas que han optado por adquirir un sistema de reconocimiento biométrico como lo es el de reconocimiento de la hulla digital ya que en estos momentos es el mas barato según su confiabilidad. Algunas de estas empresa y entidades son:

**Bancafé:** Transacciones seguras para banca por Internet utilizando la huella digital como validador de la transacción.

- Proyecto Cajeros: Transacciones bancarias seguras desde cajeros automáticos, utilizando como medio de verificación de identidad la huella digital de los clientes.

- Masificación de oficinas: infraestructura de enrolamiento y verificación de identidad de sus clientes.
- Integración de Licencias de uso para intercambiar información entre lectores de diferentes marcas con la plataforma Escribano.

**Cadena Impresores S.A:** Verificación de identidad en procesos que demandan niveles de seguridad considerables.

**Hermeco S.A:** Verificación de identidad de los empleados en la compra de artículos en los almacenes. Marcación de entrada y salida de los obreros de sus lugares de trabajo.

**SETT Secretaria de Transito de Bogotá:** Validación de personas que autorizan tramites.

**Municipio de Santa Marta:** Matrícula de huella digital de la población de la ciudad (350.000 personas) para verificar las transacciones de salud del municipio, evitar duplicados y administrar la base de datos en línea.

**Notaria 19 Bogotá D.C:** Verificación de identidad de los clientes y empleados por medio del Software Bio Notaría en el cual se registran las transacciones tales

como autenticaciones, traspasos, matrimonios y permiten que la autenticidad de dichos acontecimiento cuenten con total la transparencia.

**Área Metropolitana del Valle de Aburrá e Instituto Nacional Penitenciario INPEC:** Desarrolló de software de reseña de visitantes a la cárcel Bella vista de Medellín.

En todas estas empresas entre otras se a prestado el servicio de identificación biométrico utilizando la huella digital. Una de las principales razones por la que se utilizado esta tecnología es que no se conocen otras. Todavía no han entrado al comercio colombino, como por ejemplo la de reconocimiento de iris. La cual para la mayoría de los colombiano es prácticamente una fantasía de ciencia fisión.

Viendo todas las ventajas que pueden proporcionar un sistema de identificación biométrico nos preguntamos porque las entidades aun no se acogen a este sistemas. En particular los centros penitenciarios que son una de la empresas del estado donde se necesita tener un sistema de identificación de personas confiable y rápido, Como por ejemplo el instituto penitenciario y carcelario de nuestra ciudad (Cartagena) el cual no cuenta con un sistema de reseña y menos de identificación de personas realmente aceptable. En la actualidad el sistema de reseña de esta institución se basa en la tablilla de tinta en la que se coloca el dedo para resaltar las minucia que van a ser pasadas al documento como la hulla digital. Y el sistemas de base de datos es un cantidad de documentos archivados,

en el que relativamente se lleva un control de los internos que hay en la institución pero mas de una ves se ha presentado el problema de que no encuentran los datos de algún reo ocasionando que se tenga que buscar al individuo en los patios (cárceles) y traerlo para tomarle todos los datos nuevamente. Todo esto se puede corroborar por medio de las siguientes imágenes.

**Figura 49. Oficina de Dactiloscopia y reseña del INPEC sede Cartagena.**

En este lugar se toman las huellas digitales y los datos personales de los reos para luego ser archivados, el guardián que vemos en la foto es el encargado de tomar la huella y llenar los documentos pertinentes para la identificación del individuo posteriormente.

**Figura 50. Mesa para la toma de la huella digital.**

Aquí es donde se obtiene la tinta para resaltar las minucias e impregnarlas como huella dactilar en el respectivo documento.

**Figura 51. Obtención de los datos personales del individuo.**

Aquí el guardia esta llenado lo documentos con los datos personales y rasgos físicos del reo.

**Figura 52. Toma de la huella dactilar del sindicado**

**Figura 53. Archivos donde se encuentran la base de datos de los reos**


Analizando las anteriores imágenes se llega a la conclusión de que el sistema de reseña necesita una actualización urgente. Esta entidad seria el lugar idóneo para instalar un sistema de identificación biométrico en particular el de reconocimiento de iris ya que actualmente es el de mayor seguridad y el que contienen los últimos avances tecnológicos con relación a la seguridad de acceso a recinto.

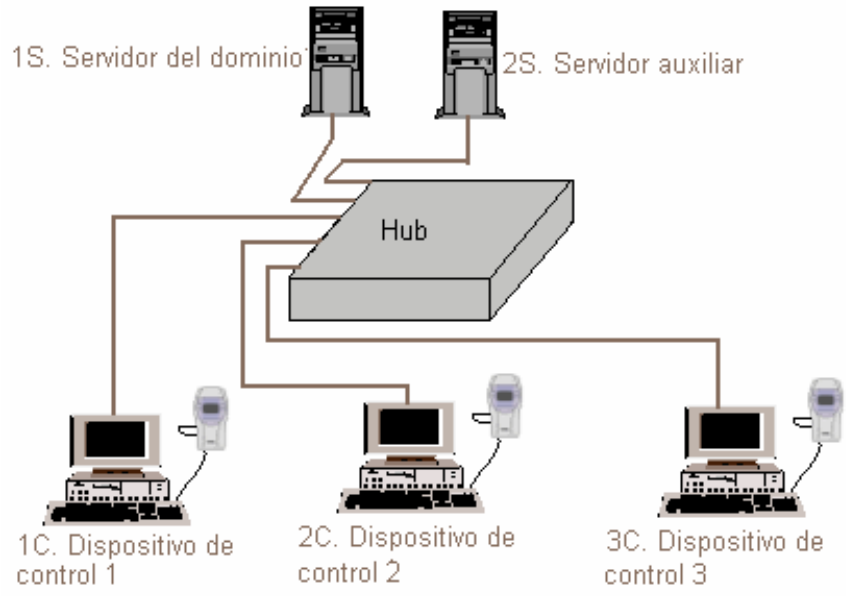
Viendo esta necesidad nos propusimos armar un sistema teórico para esta institución, el cual esta interconectado por una red LAN formada por tres computadores de control y dos servidores uno principal y el otro de respaldo.

El dispositivo que usamos para este propósito fue el de OKI IRISPASS-h cuyas especificaciones podemos encontrar en la Tabla 7. Se escogió este dispositivo por su grado de seguridad el cual es del 99.9% y su capacidad de almacenamiento de datos, ya que por el echo de utilizar una computadora de respaldo podemos acumular tanta información como la memoria fija (disco duro) lo permita. La única desventajas de este dispositivo es que cada cámara necesita un computador para el manejo del software que controla la cámara y también permita la interconexión a la red.

El anexo A. muestra el sistema de interconexión entre los puntos donde realmente es necesaria la identificación de personas.

La conexión de la red de computadoras mas conveniente para interconectar el sistema es la de anillo, pero como en la institución se cuenta con un concentrador (Hub) se aconseja utilizar la conexión en estrella para utilizar la red que existe actualmente. En la siguiente figura se muestra la conexión completa para tres puntos de control.

**Figura 54. Conexión de la red LAN del sistema OKI IRISPASS-h en la institución nacional penitenciaria y carcelaria de Cartagena.**



La distribución de los sistemas de control son los siguientes:

**1C dispositivo de control 1:** Se localiza en la oficina de reseña, con el propósito de remplazar el mecanismo de reseña actual por este sistema para crear y manejar la base de datos de los reclusos en formato digital.

**2C dispositivo de control 2:** Se ubica en la entrada de la guardia interna con el propósito es llevar un control de los empleados a si como las respectivas personas ajenas al plantel que entran a la sección de oficinas, como: jueces y visitantes.

**3C dispositivo de control 3:** Se ubica en la guardia externa con el propósito controlar el acceso a todas las personas que quieran ingresar al plantel así tanto a la región de oficina como a la dirección. O los alojamientos.

**1S Servidor del dominio:** Se ubica en el departamento de dactiloscopia, este computador se utiliza como servidor de dominio de la red actual.

**2S Servidor auxiliar:** Se ubica en la oficina de trabajo social, en esta sitio esta el punto de concentración de todos los computadores aquí de se encuentra ubicado el Hub. Y se puede utilizar el equipo de esta oficina como servidor auxiliar.

# 7. CONCLUSIONES

Como hemos visto en este trabajo, parece ser que en un futuro no muy lejano, los sistemas de reconocimiento de iris serán los que se van a imponer en la mayoría de las situaciones en las que se haga necesario autentificar a un usuario. Estos sistemas son más amigables para el usuario ya que este, no va a necesitar recordar passwords o números de identificación complejos, y como se suele decir, el usuario puede olvidar una tarjeta de identificación en casa, pero nunca se olvidará su ojo.

Además, estos sistemas, son mucho más difíciles de falsificar que una simple contraseña o una tarjeta magnética, lo que los hace mucho más eficientes. Es conveniente desmentir uno de los grandes mitos de estos sistemas; *la vulnerabilidad a ataques de simulación*. En muchas películas o libros de espías, siempre se consigue `engañar' a autentificadores biométricos para conseguir acceso a determinadas instalaciones. Se simula la parte del cuerpo a analizar mediante un modelo o incluso utilizando órganos amputados a un cadáver o al propio usuario vivo. Evidentemente, esto sólo sucede en la ficción: hoy en día cualquier sistema biométrico; con excepción, quizás, de algunos modelos basados en voz, son altamente inmunes a estos ataques en especial el de reconocimiento de iris. Los analizadores de iris son capaces, aparte de decidir si el miembro

pertenece al usuario legítimo, de determinar si éste está vivo o se trata de un cadáver.

Un sistema biométrico permite hacer una inversión inicial única, ya que en el futuro, no hay costos de consumo, sólo de mantenimiento y operación, sin embargo las principales razones por la que no se han impuesto en nuestros días, es su elevado precio, fuera del alcance de muchas organizaciones, y su dificultad de mantenimiento. En un sistema biométrico no hay chequeos fraudulentos, lo cual baja los costos de operación anuales en forma considerable.

Debido a la extrema seguridad con la que operan estos tipos de sistemas, las empresas que los implementan; que en la mayoría de los casos son entidades muy prestigiosas y no a la tienda propiamente tal, nos fue imposible obtener información sobre referencia a problemas y los costos de implementación de los estos sistemas.

Como futura aplicación, se piensa que sería bastante útil, el uso de dispositivos biométricos, en particular el uso del reconocimiento de iris, para controlar el acceso a las diferentes instalaciones de la Corporación Universitaria Tecnológica de Bolívar, ya sea en biblioteca, laboratorios de computadores, acceso nocturno a facultades, control de horarios, entre otros.

## BIBLIOGRAFIA


Daugman Jhon. G. “High Confidence Visual Recognition of Persons by a Test of Statistical Independence”. IEEE Transection On Pattern Analysis And Machine Intelligence. Nov. 1993. PAMI, vol 15, No 11: 1148-1162.

Benjamin Miller. “Vital Signs of Identity”; IEEE Spectrum; February 1994; pp. 22 – 30.

M. Faúndez. “Reconocimiento de personas mediante características biométricas: Acceso seguro a recintos, informaciones, y control de personas”. Mundo electrónico, Diciembre de 1998, Nº 293,

Nievergelt, Y. Wavelets Made Easy. Birkhäuser, Boston, MA. EUA, 1999.

Alberto Domingo Ajenjo. Tratamiento Digital de Imágenes. Anayaultimedia,1994

Rafael C. Gonzalez - Paul Wintz. Digital Image Processing. Addison-Wesley. 1987.

Trasformada Wavelet, Teoría y Aplicación - Jorge Osmar Lugo -Trabajo de Laboratorio IIFaCENA 1999

Richard W. Hamming. Coding and Information Theory. Segunda edición, Prentice Hall, 1986

Hinton, G.E. (1992) Redes neuronales que aprenden de la experiencia. Investigación y ciencia Noviembre 1992.

Trabajo de investigación sobre Biometría.
http://209.227.231.229/novita/biometria.pdf

Análisis de la textura de El iris Humano Para la Autenticación de Alta Seguridad.
http://www.cim.mcgill.ca/~mcmordie/iris_recognition.html

Consorcio de Biometria. investigación, desarrollo, comprobación, evaluación, y aplicación de identificación de personal basado en la biometria.
http://www.biometrics.org/

Tecnologías Iridian, Inc. de Moorestown, NJ investigación, desarrollo y mercadeo de tecnologías de la autenticación basados en el reconocimiento del lirio.
http://www.iriscan.com/

Sistemas lectores de reconocimiento biométricos.
http://www.insys.com.mx/biometria/lectores.htm

Aplicación de la Wavelets en la identificación biométrica.

http://www.polyboy.net/akademisches/diplomarbeit/html/node26.html

Empresas que arman y comercializan los sistemas de reconocimiento de iris.

http://www.iridiantech.com/

http://www.panasonic.com/medical_industrial/iris.asp

http://www.cnn.com/2002/TECH/science/02/08/airports.eyes/index.html

http://www.idg.net/go.cgi?id=647567

http://www.lgiris.com/

http://www.oki.com/en/press/2002/z02011e.html

Conceptos básico sobre la Iridologia.

http://www.aamenat.org.ar/iris.htm

Conceptos sobre la iridiologia.

http://www.proyectopv.org/1-verdad/iridiologia.htm

Artículos del FBI sobre la seguridad biométrica.

http://www.securitymanagement.com/library/fbi_aug01.pdf

# ANEXO

**Anexo A. Plano de interconexión del sistema OKI IRISPASS-h en la institución nacional penitenciaria y carcelaria de Cartagena.**