Sistema de autenticación biométrica por reconocimiento de rostro

Giovanni Francisco Acosta Henríquez
Máster en Dirección Estratégica de Ingeniería de Software
ghenriquez@catolica.edu.sv
Docente, Facultad de Ingeniería y Arquitectura
Universidad Católica de El Salvador, El Salvador

Resumen

La seguridad es una constante que históricamente ha preocupado a las sociedades. Actualmente es un tema de gran importancia a nivel mundial, especialmente en países con altos índices de criminalidad como El Salvador1, en el cual el aumento de la delincuencia ha hecho que muchas empresas e instituciones opten por el uso de sistemas sofisticados de seguridad, entre ellos: circuitos cerrados de cámaras de video, controles vehiculares, personal de seguridad y otros. Ello incrementa sus costos de operación, causando molestias en los usuarios, y en muchos casos no logran proveer el nivel de seguridad requerido en las empresas o instituciones, tales como: aeropuertos, bancos, hospitales, instituciones de gobierno, etc.

En los últimos años se ha incrementado el uso de sistemas biométricos como métodos efectivos de seguridad. La biometría es un campo tecnológico que consiste en identificar personas a través de características físicas únicas. Esta investigación propone la creación de un sistema de autenticación biométrica por reconocimiento de rostro, definiendo la autenticación como el proceso a seguir para determinar la identidad de uno o varios individuos autorizados para acceder a un determinado recurso o servicio. Para esto se analizaron y compararon las técnicas de reconocimiento facial existentes en el mercado, se desarrolló un prototipo del sistema para la realización de pruebas, se calibraron parámetros y se validó un algoritmo, obteniendo resultados que podrían beneficiar a las empresas e instituciones que demanda este tipo de seguridad.

Palabras clave: Biometría, reconocimiento de rostros, autenticación por reconocimiento de rostro

1 Fuente: Observatorio de datos seguridad pública por país de la Organización de Estados Americanos.

Abstact

Security is a constant that has historically troubled societies. In the current days this is an issue of huge importance worldwide, especially in countries with high criminality rates as El Salvador1, in which the arise of delinquency has pushed many enterprises and institutions to opt for the use sophisticated security systems, among them: closed-circuit television, vehicular controls, security guards and others. These options increase the cost of operation and cause some troubles to the users. Which is worse, sometimes these options can't provide the security level required in the enterprises or institutions such as: airports, banks, hospitals, government institutions, etc.

In the last years the use of biometric systems has increased as an effective security method. Biometric is a technological field that helps to identify people through unique physical characteristics. This research proposes the creation of a biometric authentication system by face recognition, defining authentication as the process to be followed to determinate the identity of one or more authorized people who can access to a target resource or service. Some recognition techniques available in the market were analyzed and compared. A prototype of the system was developed for testing. Parameters were calibrated and an algorithm was validated. The results that were obtained could help enterprises and institutions that demand this type of security.

Key words: Biometry, face recognition, authentication by face recognition

1 Source: Observatory of data about public security per country of the Organization of American States.

1. Introducción

La biometría en una ciencia que nace a finales del siglo XX e investiga la identificación de personas. Se basa en el principio de que no hay dos seres humanos iguales. El concepto proviene de las palabras *bio* (vida) y *metría* (medida). "Es un estudio mensurativo o estadístico de los fenómenos o procesos biológicos".[1] Todo equipo biométrico mide e identifica alguna característica propia de la persona. Esta tecnología de seguridad se basa en el reconocimiento de una característica física e intransferible de las personas. La forma de la cara, la geometría de partes del cuerpo como las manos, ojos y la huella digital son algunos rasgos que diferencian a los seres humanos.

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 de la huella digital no se extrae la imagen de ella, sino una secuencia de números que la representan. Sus aplicaciones abarcan una gran cantidad de sectores: desde el acceso seguro a computadoras, redes, protección de ficheros electrónicos hasta el control de horario y control de acceso físico a una sala de acceso restringido. Por esta razón, también se define como "una rama de las matemáticas estadísticas que se ocupa del análisis de datos biológicos y que comprende temas como población, medidas físicas y tratamientos de enfermedades" (Ferando Prada, 2007, pág. 560).

Entre los métodos de identificación biométrica existentes de voz, huella digital, iris, retina, rostro, etc., se deben considerar ciertas ventajas y desventajas al desarrollar un sistema de este tipo tales como: fiabilidad, flexibilidad, precio, entre otras.

En algunos casos se opta por sistemas multi-biométricos para ayudar a soportar estos requerimientos tan discrepantes, pero son de un elevado costo y difícil implementación.

La creación de un sistema de autenticación biométrica por reconocimiento de rostro es una alternativa importante para seleccionar y desarrollar un sistema biométrico óptimo. Una de sus principales ventajas es que no requiere de contacto físico de la persona con un dispositivo (sensor) de captura, además, no requiere un hardware muy sofisticado, puede ser utilizado con sistemas de captura de datos como webcams, cámaras de seguridad, etc.

Un rostro no tiene tantos puntos de medición como las huellas digitales o el iris, por lo que la precisión en el reconocimiento de rostro es menor que en otros métodos de reconocimiento biométrico. Sin embargo, es muy útil para aplicaciones, especialmente cuando se toma en cuenta la conveniencia para el usuario.

2. Metodología

La investigación fue de tipo descriptiva explicativa, pues se analizaron, compararon y describieron las características de la tecnología biométrica por reconocimiento de rosto.

La propuesta de autenticación biométrica por reconocimiento de rostro se conforma de:

Figura 1. Componentes del sistema propuesto de autenticación por rostro

Fuente: Elaboración propia

1 Fuente: Diccionario en línea, Real Academia Española, febrero 2013.

• *Webcam*. Se utilizó un dispositivo de gama media/alta de 640 x 480 pixeles, con capacidad de generar 30 fotogramas por segundo, con conexión inalámbrica por puerto USB.

• *Verilook SDK*. Se trabajó con el *framework* Verilook SDK, creado para integradores de sistemas de reconocimiento facial. Este ofrece una identificación rápida y confiable con detección de rostro vivo y la habilidad de procesar múltiples rostros en un solo cuadro. El software es independiente de la cámara y es compatible con webcams, disponible en la versión *Verilook Standard SDK*. Utilizada para desarrollar aplicaciones biométricas basadas en computadora. Ella incluye componentes de comparación y extracción, software de administración de cámaras y documentación, compatible con las plataformas: Microsoft Windows, GNU/Linux o Mac OS X. También, disponible en la versión Verilook Extended SDK, que sirve para desarrollar aplicaciones biométricas sobre redes y ambientes basados en la web. Este incluye características de la versión Standard SDK y contiene un servidor de comparación.

• Equipo de procesamiento. Se utilizó el algoritmo de reconocimiento de rostro VeriLook versión Standard SDK y se ejecutó en una computadora portátil con la plataforma Microsoft Windows versión 8, con un procesador Intel CORE i5 y 4GB de RAM.

• **Database engine**. Con Verilook SDK se estableció una conexión con el motor de base de datos de SQL Server 2008 R2, y se almacenaron plantillas en la base de datos utilizando datos binarios para ahorrar espacio de almacenamiento.

La tecnología de reconocimiento facial utiliza facciones de la cara humana para verificar o identificar individuos. Para esto, fue necesario que el sistema fuera lo más confiable posible. Asimismo, el procesamiento debió ser:

• Estado del arte. Estudió del estado de la técnica de reconocimiento facial en fuentes primarias y secundarias de información.

• Montaje de equipo. Instalación del hardware y software necesario para la investigación: computadora, cámara, base de datos y VeriLook SDK para reconocimiento de rostro.

• Estudio de algoritmo. Análisis de los diferentes algoritmos disponibles en el mercado. Para el caso se profundizó en el estudio del algoritmo VeriLook para el reconocimiento facial.

• Base de datos. Elaboración de una base de datos con fotografías del rostro de 20 personas diferentes. A todos ellos se le matriculó en la base de datos y se almacenaron varias fotografías de cada persona con diferentes expresiones y ángulos del rostro, para la posterior realización de pruebas de verificación y análisis del algoritmo.

• Estadísticas. Configuración de las estadísticas en la aplicación, el FAR (*False Acceptance Rate*), porcentaje de intentos no autorizados que serán aceptados y el FRR (*False Recognition Rate*)[2], porcentaje de intentos no autorizados que serán rechazados para determinar la confiabilidad del sistema.

• Desarrollo de software. Utilización de un sistema prototipo para la autenticación de personas por reconocimiento de rostro, con características de fácil manejo y bajo costo.

• Pruebas y depuración. Realización de diferentes pruebas para conocer las respuestas generadas por el software y realización de ajustes pertinentes.

• Validación. Verificación del funcionamiento del prototipo propuesto del sistema de autenticación por reconocimiento de rostro.

2 Mas adelante el autor se referirá a estos procesos mediante sus siglas

2.1 Configuración de software

Para utilizar el sistema biométrico se activaron los componentes *Face Extractor* y *Face Matcher* que provee VeriLook SDK. Ellos permiten obtener la plantilla de la cara para ser almacenada en la base de datos, y luego hacer una comparación del rostro con las plantillas registradas en la base de datos. Para ello, se utilizó la aplicación Activation Wizard, provista por el fabricante del SDK.

Para configurar las características *Face Detection*, *Face Extraction*, *Enrollment* e Identificación se ingresó en el menú Herramientas y dio clic en *Opcion* de la aplicación de reconocimiento de rostro.

Face Detection configura el *threshold* que es un tipo de referencia, orientada a la puntuación que determina la consistencia de un patrón. Este se puede ajustar dependiendo del nivel de seguridad que se desee aplicar, pero se recomienda utilizarlo a un 50% lo que proporciona un sistema no muy restrictivo; y utilizar un ángulo de 15º el ángulo de rotación e inclinación del rostro.

Face Extraction, habilita o deshabilita la detección de atributos como sexo, expresiones faciales, parpadeo, boca abierta y anteojos o lentes oscuros. El *threshold* recomendado para esta opción es de 128 fotogramas por segundo.

Enrollment permite el almacenamiento de imágenes en la base de datos, para el uso del ID de la plantilla para el nombre del archivo. El tamaño de la plantilla puede ser *small, medium o large*. Se recomienda el tamaño *large*, ya que provee mayor fiabilidad a la hora de realizar la identificación de la cara. También se debe configurar el número máximo de registros por plantilla y cuántas imágenes serán permitidas en la inscripción por generalización.

Por último en la opción de Identification debe configurarse el tamaño de la plantilla a generar, este puede ser: *small, medium* o *large*.

Para tener una mejor optimización del sistema durante la identificación, se recomienda que el tamaño de la plantilla sea *medium*.

El parámetro biométrico FAR se refiere a la probabilidad de que una persona no autorizada sea aceptada. Es decir el rango de error o falla en el sistema. Este debe ajustarse para evitar el fraude en los sistemas biométricos. Para que el sistema posea el mayor nivel de seguridad, se puede utilizar un FAR de 0.1% y para un sistema menos restrictivo, un FAR de 0.01% con velocidad baja, que es el porcentaje recomendable de aceptación de personas no autorizadas para el sistema.

2.2 Proceso de inscripción de personas

La matriculación es el proceso por el cual la persona provee inicialmente sus datos biométricos. Estos datos son adquiridos y procesados con el objetivo de formar una plantilla que se usará para realizar posteriormente la autenticación en el sistema.

La calidad del proceso de matriculación es uno de los factores más críticos cuando se implementa un sistema biométrico. La precisión del sistema se verá seriamente afectada si este paso no conlleva la creación de plantillas fidedignas de calidad. La extracción de características biométricas es el proceso automatizado de localizar y codificar las características biométricas distintivas de un individuo con el fin de generar una plantilla. Esta última es un archivo binario pequeño (menor a 1000 bytes) que se genera de las características biométricas de la persona con el fin de igualar los resultados.

Los sistemas biométricos comparan plantilla, no imágenes. Si la plantilla es pequeña permite comparar los resultados rápidamente, utilizando menos espacio de almacenamiento, facilitando la transmisión y encriptación de la misma. El diseño de la plantilla es propiedad intelectual de la empresa proveedora del algoritmo biométrico que la genera, lo que produce serios problemas de interoperabilidad.

Es importante destacar que las plantillas no pueden reconstruir exactamente la imagen original de las cuales fueron derivadas, ya que ellas no solo son compresiones de imágenes, sino que son el resultado de algoritmos de procesamiento matemáticos complejos, realizados sobre la imagen adquirida por el sensor biométrico. Por lo tanto, si la misma persona provee la misma muestra biométrica (cara, huella, etc.) es altamente probable que se generen dos plantillas distintas, dado que siempre hay pequeñas variaciones en: posición, distancia, luminosidad, ángulo, etc. Sin embargo, la diferencia no produce un resultado negativo al momento de realizar la autenticación de la persona.

El sistema propuesto de autenticación biométrica por reconocimiento de rostro, provee dos métodos de matriculación:

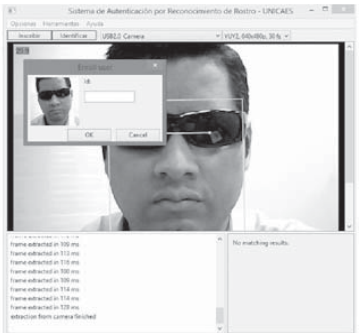
Figura 2: Aplicación propuesta para la autenticación de personas por reconocimiento de rostro en el proceso de matriculación

Método A

Se utiliza para matricular una persona en la base de datos adquiriendo para ello una única imagen (plantilla)

Fuente: Elaboración propia

Figura 3: Aplicación propuesta para la autenticación de personas por reconocimiento de rostro en el proceso de matriculación generalizada



Método B

Se utiliza para matricular una persona en la base de datos, adquiriendo para ello múltiples imágenes y utilizando diferenciadores como: lentes, bigote, sombrero, barba, etc.

Fuente: Elaboración propia

3. Resultados

El *Biometric Matching* es el acto de comparar plantillas biométricas para determinar el grado de similitud, conocido también como igualación biométrica. El resultado de la comparación de plantillas produce un puntaje o resultado basado en una escala predefinida en el sistema (ejemplo de 1 a 100).

La mayoría de sistemas biométricos de autenticación por rostro permiten al administrador de la aplicación biométrica programar el límite de manera que si este se sobrepasa, el resultado es una igualdad. Si el puntaje no llega al límite, el resultado es negativo. Dicho límite puede ser configurado en la aplicación propuesta para la autenticación de personas por reconocimiento de rostro.

Las comparaciones biométricas están basadas en el puntaje cuyo número indica el grado de igualdad o correlación que resulta de la comparación de la plantilla de matriculación contra la plantilla que se provee a la hora de autenticarse en el sistema. No existe una escala estandarizada entre los diferentes fabricantes. Los equipos biométricos casi nunca basan sus decisiones en una igualdad del 100%

porque diferentes plantillas son generadas por el mismo sujeto y casi nunca existe una correlación en este nivel.

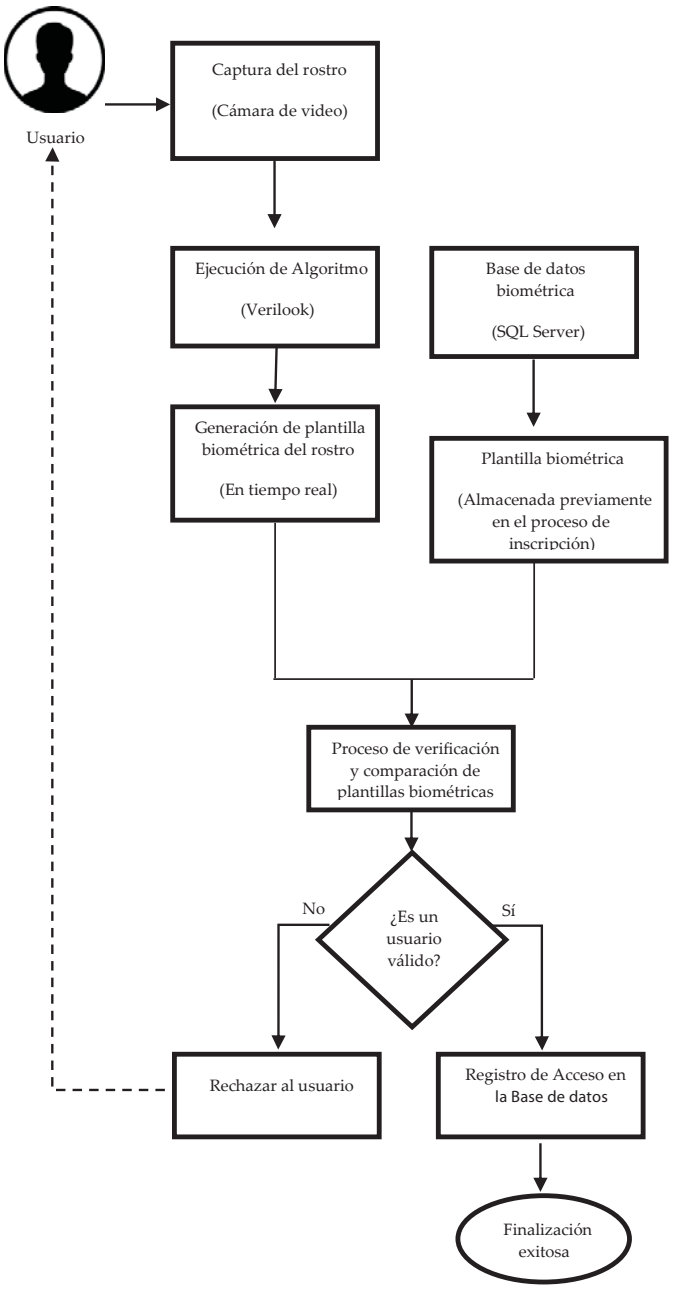
El sistema biométrico está diseñado para autenticar y determinar que un usuario está autorizado para acceder a un determinado recurso físico (edificios, oficinas, etc.), lógico (computadora, redes de cómputo, etc.) o servicio (transporte, comunicación, salud, etc.). Estas pueden ser colocadas de manera local, en redes LAN o por Internet.

Figura 4: Aplicación propuesta para la autenticación de personas por reconocimiento de rostro en el proceso de identificación de una persona

Fuente: Elaboracción propia

Entre las posibles aplicaciones biométricas que se pueden implementar en una empresa o institución se encuentran: control de acceso a zonas restringidas, control de presencia en lugares físicos y virtuales (computadora, redes, etc.); control de entradas/salidas laborales para generar la planilla de pago, control de visitas, medio de autenticación de usuarios para transacciones financieras, sistemas de fidelización de clientes, trámites migratorios, entre otros.

La aplicación de autenticación biométrica por reconocimiento de rostro funciona de acuerdo al siguiente diagrama:



Fuente: Elaboración propia

El sistema podría combinarse con otros mecanismos como alarmas, cerraduras eléctricas, etc. que permitan restringir el acceso a los usuarios no autorizados. Además, se cuenta con un instalador del sistema biométrico para la plataforma Microsoft Windows, versiones 7 y 8.

Para la implementación del sistema biométrico propuesto se requiere el siguiente presupuesto:

N°	Concepto	Precio
1	Webcam de gama media/alta de al menos 640 x 480 pixeles, con capacidad de generar 30 fotogramas por segundo, de conexión alámbrica vía puerto USB o la red local	$20
2	Licencia Verilook Standard 5.4	$600
3	Aplicación biométrica de reconocimiento de rostro (*)	$1 000
4	Computadora con Sistema Operativo Windows 8 o posterior	$800
5	Gastos de instalación (Cableado de red y eléctrico)	$50
6	Dispositivo de almacenamiento externo de información (4 TB)	$200
	Total	**$2 670.00**

Fuente: Elaboración propia

** De otorgar licenciamiento gratuito en el uso de la aplicación biométrica de reconocimiento de rostro, el costo de implementación se reduce a $1 670 y si ya se posee el equipo de cómputo y almacenamiento, se reduce a $670.*

Se puede explicar con base en los resultados obtenidos en las pruebas realizadas en un entorno controlado y con buena luminosidad, que la aplicación propuesta de autenticación biométrica por reconocimiento de rostro funcionó correctamente, de acuerdo a los parámetros en que fue diseñada. La aplicación es eficaz y fácil de utilizar. Esto la convierte en una solución de autenticación biométrica por reconocimiento de rostro de bajo costo y alta funcionalidad, que puede ser implementada para entornos específicos.

4. Discusión

La experimentación de la aplicación de autenticación de personas por reconocimiento de rostro permitió las siguientes conclusiones y recomendaciones:

- No puede incorporarse la misma tecnología biométrica en todas las aplicaciones. Se debe realizar un análisis que determine cuál es la más adecuada, ya que dependerá del escenario que se posea para su implementación.

- La biométrica es única y solo puede pertenecer a un individuo. Aun cuando existen combinaciones distintas para cada persona, la tecnología es capaz de discriminar propiamente esas diferencias. Sin embargo, las tecnologías biométricas de identificación de personas tienen limitaciones, dependiendo de los grados de libertad que se utilicen en el sistema.

- Todo sistema tiene tolerancias que se introducen normalmente y permiten que el ruido y otras variaciones temporales no afecten las mediciones. Existen probabilidades significativas de que los datos de una persona puedan eventualmente ser compatibles con los datos de otra persona.

- En el diseño de un sistema biométrico de autenticación de personas, se deben considerar los diferentes tipos de errores FRR y FAR, manejándolos según el nivel de seguridad que se necesite aplicar en cada caso.

- El sistema propuesto de autenticación de personas por reconocimiento de rostros puede dar buenos resultados utilizando los recursos con las

características descritas en este documento, pero la fiabilidad y rendimiento del sistema se puede incrementar o disminuir según las condiciones reales de cada contexto. Es necesario programar el sistema con muestras reales de población de acuerdo a las circunstancias ambientales específicas donde se usará.

- Al adquirir equipo biométrico se debe realizar un estudio minucioso de las características técnicas y de funcionamiento del equipo, ya que los fabricantes pueden omitir algunos datos por conveniencia. Además se debe considerar que los datos arrojados por el fabricante -en muchos casos- son tomados como datos colectados en condiciones extremadamente ideales de laboratorio.

- Los sistemas biométricos no pueden garantizar al 100% la seguridad, ya que no existe una biométrica perfecta, aunque si existen niveles muy altos de aceptación en algunos casos arriba del 95%.

- Para seleccionar la tecnología biométrica adecuada se deben considerar los siguientes factores: costo, tasa de error, velocidad de procesamiento, exactitud, privacidad y facilidad de uso.

- De las tecnologías biométricas actuales se recomienda el uso del reconocimiento de rostro por ser una tecnología de bajo costo, con excelente velocidad de respuesta, buena fiabilidad y sobre todo la facilidad de uso para el usuario, ya que no requiere contacto directo con el equipo biométrico. El prototipo desarrollado, se recomienda únicamente en entornos controlados donde no se requiere grandes niveles de seguridad, en donde el usuario pueda posar frente a la cámara con buena luminosidad para realizar el proceso de autenticación.

- Incorporar el tema de "Sistemas de Autenticación de Personas" a la asignatura Seguridad Informática de la carrera de Ingeniería en Sistemas Informáticos, de la UNICAES.

- Implementar el prototipo propuesto en esta investigación para la autenticación de personas que ingresan a la Universidad Católica de El Salvador, aprovechando el proceso de carnetización que se realiza durante la inscripción de materias para matricular, al mismo tiempo, a los alumnos en la base de datos del sistema biométrico. Es recomendable actualizarla al menos una vez al año.

- A futuro se puede mejorar el sistema biométrico integrándolo a la red de cámaras web instaladas en la Universidad Católica de El Salvador, para contar con un sistema centralizado y remoto de monitoreo que alerte a la seguridad al identificar personas no autorizadas dentro del campus.

- Se recomienda escalar el prototipo propuesto a un producto comercializable de tecnología de autenticación de personas por reconocimiento de rostro, que pueda ser utilizado en instituciones y empresas que requieran el servicio.

5. Referencias

Biometric Consortium. (2013). About The Biometric Consortium. Recuperado de http://www.biometrics.org

Bolle M. R. (2005). Guide to Biometrics. New York, Estados Unidos: Springer.

Chirillo, J. y Blaul S. (2005). Implementing Biometric Security. Indiana, Estados Unidos: Wiley.

Gate, A. K. (2011). Our Biometric Future. New York, Estados Unidos: New York University Press.

Jain, K. A. (2009). Encyclopedia of Biometrics. Michigan, Estados Unidos: Stan Z Li.

Jain, K. A. (2007). Handbook of Biometrics. New York, Estados Unidos: Springer.

Leeland, B. K. (2008). Face Recognition New Research. New York, Estados Unidos: Nova.

Neuro Technology (2013). Biometric and Artificial Intelligence Technologies. Recuperado de http://www.neurotechnology.com

Rakover, S. S. (2000). Face Recognition: Cognitive and computacional process. Philadelphia, Estados Unidos: John Benjamins Publishing Company.

Wechsler, H. (2007). Reliable Face Recognition Methods. New York, Estados Unidos: Springer.