Universidad de Buenos Aires

Facultades de Ciencias Económicas,

Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final de Especialización

Tema

Estudio de Falsa Aceptación y Falso Rechazo en Tecnologías de Autenticación Biométrica

Autor: David E. Guerrero M.

Tutor: Pedro Hecht

Año de Presentación: 2020

Cohorte: 2018

Declaración jurada de contenidos:

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual".

_____

David E. Guerrero Médicis

DNI: 95.870.595

RESUMEN

La autenticación biométrica son tecnologías que forman parte vital en los sistemas de seguridad actuales, su objetivo es identificar o verificar la identidad de una persona, basándose en sus características biométricas, estas pueden ser físicas, químicas o de comportamiento.

Para realizar un proceso de identificación o verificación en una persona, las tecnologías biométricas hacen uso de puntajes o también conocidos como pesos, para expresar la similitud entre un patrón biométrico de la persona y una plantilla biométrica almacenada en el sistema, cuan mayor el puntaje, mayor la similitud.

Los mencionados puntajes, son un cálculo que se realiza a partir de las tasas de falsa aceptación (FAR) y de falso rechazo (FRR), las cuales son la probabilidad de aceptar el acceso de un usuario no autorizado o de rechazar incorrectamente el acceso de un usuario autorizado respectivamente.

Si bien, permitir el acceso de una persona no autorizada es un grave problema de seguridad, no sería conveniente denegar erróneamente el acceso a un volumen considerable de usuarios, esto provocaría a los usuarios rechazar el sistema, para ello es necesario ajustar la ubralización de FAR y FRR midiendo el rendimiento del sistema.

Palabras clave: Biometría, falsa aceptación (FAR) y falso rechazo (FRR)

TABLA DE CONTENIDO

PROLOGO

En primer lugar, doy gracias a mi Dios todo poderoso, por poner en mi camino experiencias y personas que han hecho de mí una mejor persona, a mis padres que son mi apoyo incondicional.

Además, me gustaría agradecer a la Ciudad Autónoma de Buenos Aires y como no, a la Universidad de Buenos Aires por ofrecer un ambiente sano y agradable al extranjero para el libre progreso profesional.

INTRODUCCIÓN

En los sistemas de seguridad actuales es normal encontrar el uso de tecnologías de autenticación biométricas, estás brindan un nivel de seguridad adicional, porque son las encargadas de autenticar la identidad del usuario que solicite acceso al sistema.

Un sistema biométrico es un conjunto de hardware y software, capaz de autenticar a las personas, basándose en los rasgos biométricos de la misma, estos rasgos pueden ser físicos (como la huella dactilar, iris, forma de la mano), químicos (ADN, Olor corporal) o de comportamiento (como la forma de firmar, forma de caminar).

Cabe resaltar que cada sistema biométrico tiene dos fases, la primera es conocida como “Enrolamiento”, fase donde se registran las plantillas biométricas de los usuarios al sistema, la segunda fase conocida como “Autenticación”, puede darse de dos formas, como “Identificación”, que a partir de los rasgos capturados de una persona, busca en sus registros la identificación de la misma, la segunda forma “Verificación”, donde conociendo previamente la identidad de la persona verifica que sus rasgos coincidan con los almacenados en el sistema.

Hay que tener en cuenta que los rasgos biométricos de las personas y la captura de estos pueden verse afectados o ser alterados de varias formas, desde cambios de temperatura, uso de accesorios, cicatrices hasta el mismo paso del tiempo. Por lo mismo hay que tener presente siempre un margen de error en el sistema.

Por lo tanto, para evaluar o comparar el rendimiento de los sistemas de seguridad biométrica es necesario tener presente variables como, FAR (Tasa de falsa aceptación) y FRR (Tasa de falso rechazo) para ser analizadas y ajustadas en beneficio del sistema.

OBJETIVOS

Objetivo general:

Conceptualizar la evaluación de rendimiento de los sistemas de autenticación biométrica, partiendo del uso de la herramienta estadística AUC-ROC.

Objetivos específicos:

1. Construir un breve marco teórico de los mecanismos de autenticación biométrica.
2. Definir conceptos de Tasa de Falsa Aceptación (FAR) y Tasa de Falso Rechazo (FRR) y la importancia de estos en la evaluación de los sistemas de autenticación biométrica.
3. Definir concepto de AUROC (Área bajo las características operativas del receptor) y uso de este para el cálculo de valores umbrales para la medición de rendimiento en los sistemas biométricos.

CAPITULO I – BIOMETRÍA

Definición de Biometría

El significado etimológico de la biometría proviene de las palabras griegas “bio” (vida) y “métrica” (medida), es la ciencia encargada de investigar características fisiológicas, químicas y de comportamiento de las personas para la identificación y autenticación de estas.

Ha formado parte de la historia de la humanidad, en civilizaciones antiguas como china, babilónica y egipcia se tiene registro de creación sistemas y mecanismos para la identificación de las personas, a lo largo del tiempo estos mismos han evolucionado, hoy en día, a causa del crecimiento poblacional y el avance tecnológico, su estudio se encuentra en auge [1].

Sistema Biométrico

Se entiende por sistema biométrico como un conjunto de hardware y software encargado de autenticar a las personas, basándose en los diferentes rasgos que las identifique, pueden ser fisiológicos como huella dactilar, voz, iris, rostro, de igual forma identificar patrones de comportamiento como firma, voz, modo de teclear.

La conveniencia de uno u otro rasgo para determinada aplicación se estudia teniendo en cuenta características de los usuarios como:

- Universalidad: Todos los usuarios deben poseer el rasgo a identificar.
- Unicidad: El rasgo de un usuario debe ser diferente al de los demás usuarios.

- Permanencia: El rasgo no se debe ver alterado con el tiempo u otros factores.

Además, el sistema biométrico debe cumplir con características como:

- Mensurabilidad: Los rasgos deben ser sistemáticamente medibles.
- Aceptabilidad: Los usuarios deben sentirse cómodos usando el sistema.
- Rendimiento: El sistema debe ser preciso y veloz.
- Evitabilidad: El sistema debe garantizar confianza y seguridad.

Cabe resaltar que ningún sistema biométrico cumple a cabalidad con todas estas características, no obstante, esto no quiere decir que dejen de ser confiables, como ya se mencionó anteriormente, son punto crítico en un sistema de seguridad, es decir tiene que ir acompañado de otros factores de autenticación, o incluso sumar un segundo sistema biométrico como sistema de verificación [2].

Rol de la Biometría en la Seguridad de la Información

En la actualidad, cumple rol más enfocado en la seguridad de la información, forma parte de los niveles críticos de la seguridad [3], entre ellos encontramos:

- “algo que el usuario conoce”, puede ser una contraseña o un PIN.
- “algo que el usuario posee”, como una tarjeta de acceso.
- “algo que el usuario es o hace”, características o acciones únicas del usuario.

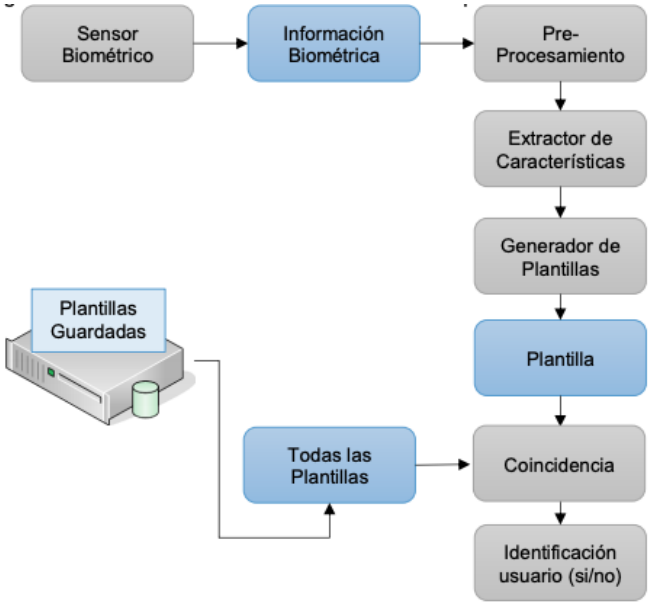
Teniendo en cuenta lo anterior, la biometría nos permite autenticar y validar que el usuario que solicitase el acceso sea en realidad quien asume

ser, esto representa grandes ventajas a las medidas de seguridad tradicionales [4], por ejemplo:

- No-Repudio: Evita que el perpetrador pueda negar haber cometido un crimen objetando que su clave o tarjeta de acceso ha sido robada o se ha visto comprometido; debido a que los sistemas biométricos se encuentran relacionados estrictamente a cada individuo.
- Seguridad y Verificación: Evita que los sistemas sean vulnerados por ataques de fuerza bruta o uso de diccionario de palabras, porque estos sistemas además de precisar de presencia física, las técnicas descritas anteriormente se vuelven inoperables.
- No-Duplicación: En muchas aplicaciones es necesario prevenir que un usuario asuma múltiples identidades, actualmente la biometría brinda la única solución posible a este problema.

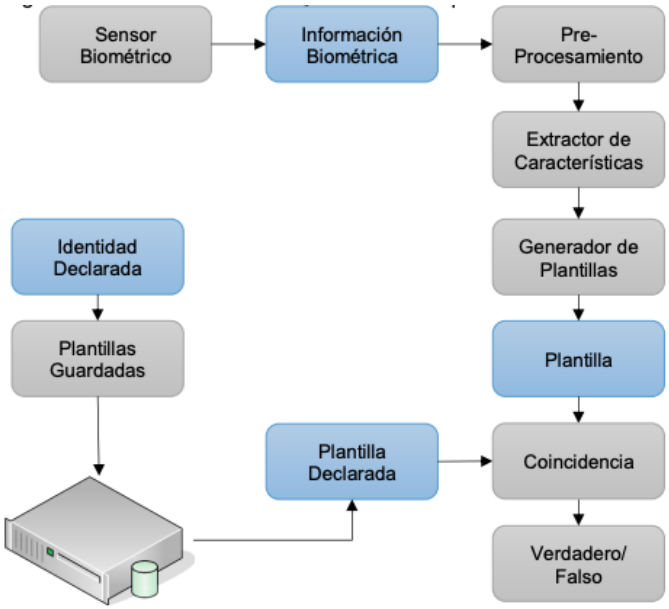
Poniendo en contexto, en un contexto funcional, un sistema de autenticación biométrico puede optar dos modos, el primero, modo identificación (Ver ilustración 1), donde los rasgos biométricos son comparados con un conjunto de patrones ya guardados, también conocidos como uno-para-muchos, este proceso no implica conocer previamente la identidad del individuo, la nueva muestra tomada es comparada una a una con los patrones ya existentes, el resultado es la identidad del individuo. Por otro lado, el segundo, modo de verificación (Ver ilustración 2), da como resultado un valor verdadero o falso, no obstante, es necesario conocer previamente la identidad de la persona.

Ilustración 1 - Proceso Identificación en autenticación para Sistemas Biométricos



Fuente: Estudio sobre las tecnologías biométricas aplicadas a la seguridad, disponible en: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/65877225F2975B3F05257E6E006A2C3D/$FILE/EstudioSobreTecnologíasBiométricasASeguridad.pdf

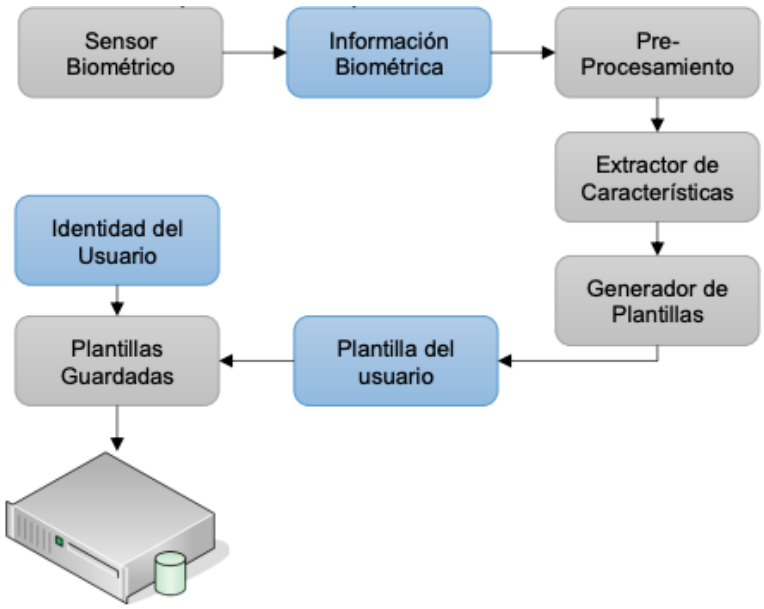
Ilustración 2 - Proceso verificación y autenticación para los Sistemas Biométricos



Fuente: Estudio sobre las tecnologías biométricas aplicadas a la seguridad, disponible en: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/65877225F2975B3F05257E6E006A2C3D/$FILE/EstudioSobreTecnologíasBiométricasASeguridad.pdf

Independientemente de la modalidad del sistema biométrico, es necesario disponer de una base de datos que almacené los patrones que se registren, el proceso encargado de lo mismo es conocido como, proceso de inscripción (Ver Ilustración 3), de igual forma es necesaria una red que permita la comunicación entre el sistema de almacenamiento de la información de los usuarios y cada uno de los puntos de reconocimiento.

Ilustración 3- Proceso de Inscripción de datos para todos los Sistemas Biométricos



Fuente: Estudio sobre las tecnologías biométricas aplicadas a la seguridad, disponible en: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/65877225F2975B3F05257E6E006A2C3D/$FILE/EstudioSobreTecnologíasBiométricasASeguridad.pdf

Es oportuno tener en cuenta que, un proceso de identificación biométrico demanda mayor volumen de procesamiento que, un proceso de verificación, esto se debe al volumen de comparaciones a realizar, por su parte, el primero se ve afectado por los siguientes dos casos:

- Identificación en conjunto cerrado: en este caso, el resultado del proceso es una asignación de identidad a uno de los individuos modelados por el sistema, y conocidos como usuarios. Existen, por tanto, N posibles decisiones de salida posibles.

- Identificación en conjunto abierto: aquí debemos considerar una posibilidad adicional a las N del caso anterior: que el individuo que pretende ser identificado no pertenezca al grupo de usuarios, con lo que el sistema de identificación debería contemplar la posibilidad de no clasificar la realización de entrada como perteneciente a las N posibles.

Mientras que el proceso de autentificación o verificación resulta ser rápido, principalmente cuando el número de usuarios es elevado, debido a que su volumen de comparaciones es más reducido, porque se limita a validar los rasgos biométricos de un usuario, no obstante, cabe destacar que se necesita fijar un umbral para medir el grado de diferencia existente entre el vector de características y el patrón almacenado [5].

Actualmente la biometría se encuentra en dos grupos de investigación y desarrollo, un grupo enfocado en estudiar las características corporales de las personas llamada Biometría Estática y otro grupo enfocado en el estudio de las características de comportamiento de las personas llamada Biometría Dinámica.

Biometría Estática

Es la encargada de estudiar las características fisiológicas de las personas, cuenta varias ramas de estudió entre las principales se encuentran el reconocimiento de huella dactilar, reconocimiento facial, geometría de manos, reconocimiento de retina e iris [6].

Huella dactilar:

Sistema de autenticación biométrica basada en huellas dactilares es la técnica más usada y popular, las huellas dactilares se forman a partir de la sexta semana de vida intrauterina y no se alteran a lo largo de la vida, esta técnica cuenta con varias formas de captura e identificación (óptico, campo eléctrico, por presión, entre otras) [7], la comparación de estas puede realizarse por las siguientes dos técnicas:

a) Basadas en minucias: se basa en identificar las minucias (formas particulares) de la huella dactilar (Ver ilustración 4), su posicionamiento dentro de ella y la separación entre las mismas, la extracción precisa de estos datos se ve influenciada en la calidad de las muestras.

Ilustración 4 - Minucias de huella dactilar

Fuente: Tecnologías biométricas aplicadas a la ciberseguridad, disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

b) Basadas en correlación: Se basa en identificar el patrón global (Ver ilustración 5) que sigue la huella dactilar, esta técnica requiere de un registro preciso de la misma, por lo cual se ve afectada por la traslación y rotación de la imagen.

Ilustración 5 - Patrones de huella dactilar

Fuente: Tecnologías biométricas aplicadas a la ciberseguridad, disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf

Entre las principales ventajas se encuentra la facilidad de uso, se suma su bajo costo de implementación, el sensor óptico se lo considera un dispositivo barato, su sistema de autenticación no requiere de tanta potencia de procesamiento, incluso puede ser implementado en un entorno móvil, siendo la técnica de autenticación más deseable.

Su principal desventaja se ve reflejada en, la complejidad de obtener imágenes de calidad que identifiquen los patrones de los dedos, a causa de problemas de suciedad, cortes, rasgaduras y desgastes en el sensor que pueden afectar con facilidad las minucias de la yema del dedo [8].

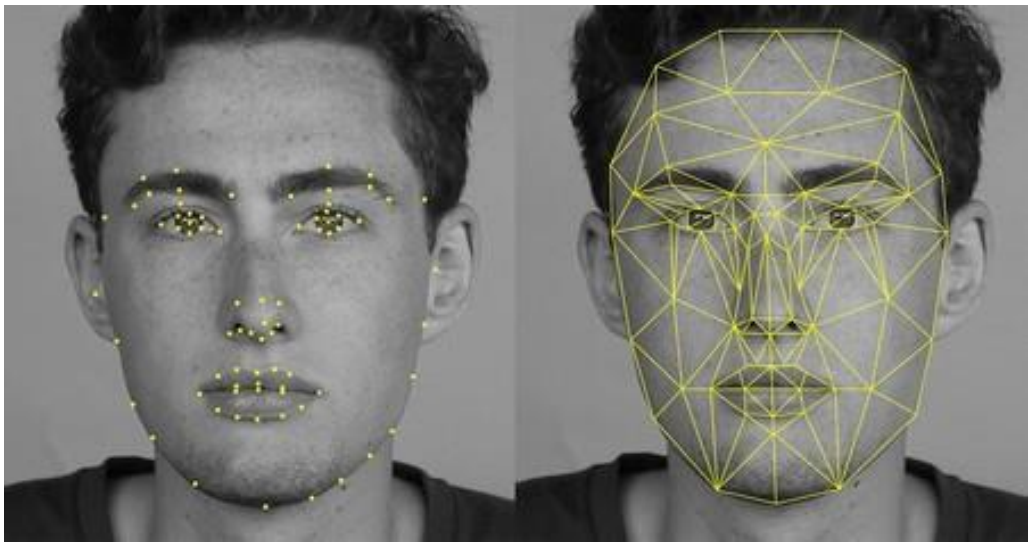
Reconocimiento facial:

Por sus siglas en ingles FRS, el sistema de reconocimiento facial es una técnica de reconocimiento se encarga de identificar las características faciales de las personas a partir de una imagen digital del mismo, su funcionamiento se basa en realizar cálculos y medidas de los aspectos faciales, como distancia entre ojos, longitud de nariz, ángulo de mandíbula entre otras (Ver ilustración 6).

Este sistema tiene la particularidad de ser aplicado en vigilancia general, porque puede realizar autenticación en tiempo real, sus ventajas

son la facilidad de uso y bajo costo de implementación. Posee varias desventajas, como la calidad de la imagen, condiciones de luminosidad, rotación de la cara, entro otros, además de las expresiones de las personas, resulta un gran desafío, sin dejar de lado el uso de accesorios o el mismo paso del tiempo [9].

Ilustración 6 - Reconocimiento facial



Fuente: Las claves de los sistemas de reconocimiento facial: ¿cuál es su verdadero nivel de seguridad?, disponible en: https://www.xataka.com/seguridad/las-claves-de-los-sistemas-de-reconocimiento-facial-cual-es-su-verdadero-nivel-de-seguridad

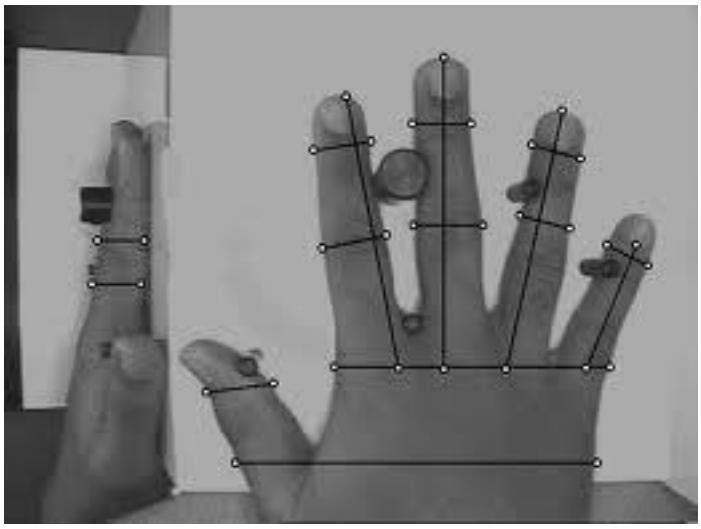
Es un sistema que se encuentra en constante evolución, se fundamenta el uso de cámaras tridimensionales, aumentar precisión en la captura de imágenes capaces de identificar características distintivas de la persona, como lunares, machas y líneas de expresión [8].

Geometría de geometría de manos:

La geometría de la mano humana no es una característica única, sin embargo, este método es aplicado en la verificación de un usuario, se capturan determinados datos y características de la mano del usuario como, el ancho, la longitud, su área (Ver ilustración 7), buscado patrones en la misma, su captura puede realizarse en dos o tres dimensiones, tiene la capacidad que al mismo tiempo que autentican, actualizan su base de datos

con cambios que pueda producir en la muestra, esto además de su rapidez le han permitido recibir buena aceptación entre los usuarios [10].

Ilustración 7 - Geometría de las manos



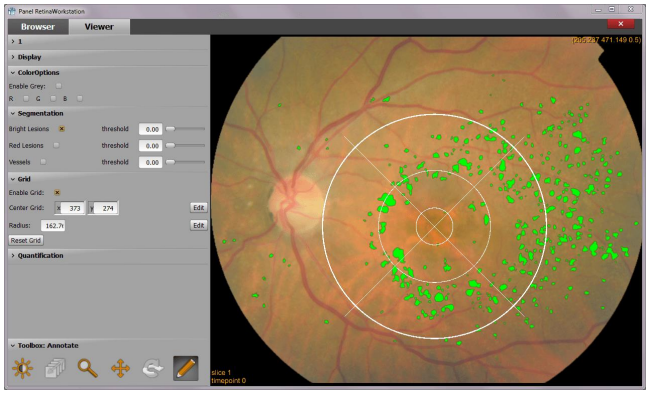
Fuente: Sistemas Biométricos – Geometría de la mano, disponible en: https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

Su facilidad de uso y su amplia aceptación hacen que este método de autenticación sea más amigable que los demás sistemas biométricos, no obstante, es considerado costoso, por requerir de un dispositivo hardware especial, encargado del escaneo de la mano, que a su vez necesita de gran espacio de almacenamiento, además de ser considerado un sistema biométrico costoso, actualmente se trabaja en la simplificación del sensor para reducir el costo general [8].

Reconocimiento de Retina:

La retina es un tejido fotorreceptor (sensible a la luz) que se encuentra en la parte posterior del ojo, el reconocimiento de retina se basa en identificar el patrón de los vasos sanguíneos dentro de la retina (ver ilustración 8), requiere el uso de luz de baja intensidad, aunque el sistema puede ser sumamente preciso, no es conveniente con el uso de lentes además de ser proceso intrusivo y de contacto cercano con el dispositivo de lectura [11].

Ilustración 8 - Reconocimiento de retina



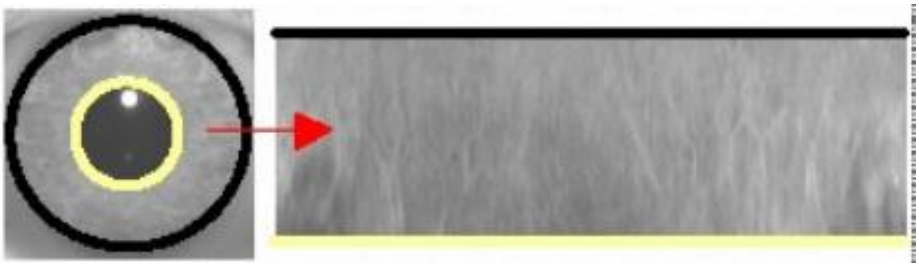
Fuente: Línea de Código – Modelo de la retina, disponible en: https://www.lineadecodigo.es/biometra-aplicada-a-la-seguridad-introduccin

Se ha prestado gran atención a esta técnica de autenticación biométrica, a causa del alto nivel de precisión de las muestras que se puede obtener de los individuos, no obstante, es un proceso incómodo para el mismo, además, su precisión puede verse afectada por factores médicos como la presión arterial alta, actualmente se encuentra en estudio el desarrollo de una implementación en dispositivos móviles [8].

Reconocimiento de Iris:

El iris es una membrana circular que separa las cámaras anterior y posterior del ojo, cuenta con más de 400 características para su identificación (ver ilustración 9), este no cambia a lo largo de la vida, el escaneo de iris se realiza con una cámara de infrarrojos de alta resolución, cabe aclarar que este mecanismo no representa un riesgo para la salud de la persona, los lentes de contacto y los lentes no afectan la identificación, se ha establecido como una de las tecnologías biometrías más resistente al fraude además que su reconocimiento es veinte veces más rápido que otro sistema biométrico [12].

Ilustración 9 - Reconocimiento de iris



Fuente: Sistemas Biométricos – Geometría de la mano, disponible en: https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

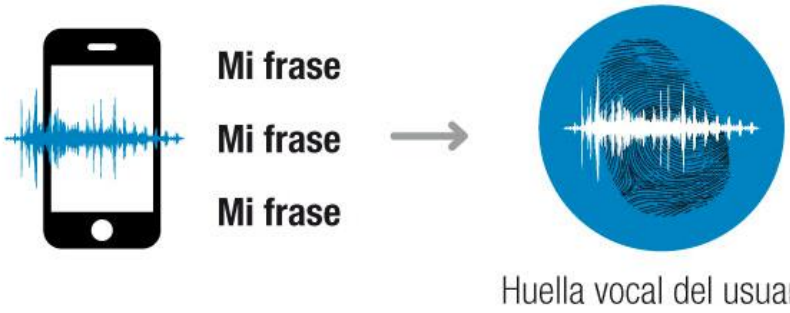
Biometría Dinámica

La Biometría Dinámica, si muy bien no son características únicas, incluso difíciles de realizar con exactitud para la misma persona, este grupo investiga los patrones que conviertan estas caracteº1rísticas en únicas [13]; entre sus principales ramas de estudio podemos encontrar las siguientes ramas de estudio:

Reconocimiento de Voz:

En la voz de una persona se puede detectar patrones dentro del espectro de frecuencia de la misma, llegando a una distinción similar a la de huella dactilar, este mecanismo no se basa en identificar qué es lo que dice el usuario, sino más bien identificar una serie de sonidos (tonos bajos y agudos, vibración de laringe, tonos nasales y de garganta) con sus características para decidir si el usuario es quien dice ser, este sistema debe estar acorde a ciertas condiciones para su correcto funcionamiento, como la ausencia de ruidos y ecos [14].

Ilustración 10 - Entrenamiento del sistema de reconocimiento de voz



Fuente: ¿Cómo funciona la biometría de voz?, disponible en: https://biometricvox.com/blog/biometria-de-voz/como-funciona-la-biometria-de-voz/

Ilustración 11 - Proceso de verificación de reconocimiento de voz

Fuente: ¿Cómo funciona la biometría de voz?, disponible en: https://biometricvox.com/blog/biometria-de-voz/como-funciona-la-biometria-de-voz/

Escritura Manuscrita:

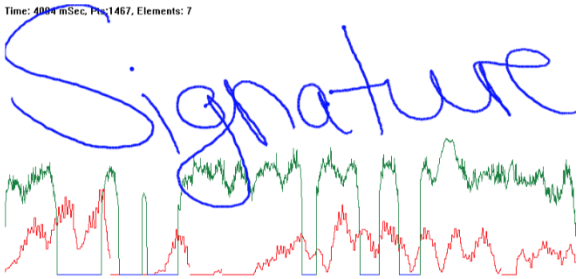
Es un método de reconocimiento biométrico tipificado como dinámico, su objetivo confirmar la identidad de la persona, realizando un análisis de la firma manuscrita, no se busca la exactitud de esta, debido a que cada firma sufre ligeras variaciones, la naturalidad del movimiento al firmar y el número de repeticiones le permite al sistema determinar y reconocer un patrón. [15]

El reconocimiento de firma es apropiado para validar la emisión de mensajes, cheques, transacciones bancarias, además, es un mecanismo de identificación más usado, existen dos variantes a la hora de identificar a las personas según su firma:

- Comparación simple: Se considera el grado de semejanza entre dos firmas, la original y la que está siendo verificada.
- Verificación dinámica de firma: Se analizan variables como: la forma, la velocidad, la presión de la pluma o bolígrafo y la duración del proceso de firma (Ver ilustración 12).

La firma es y ha sido durante muchos años una de las técnicas más habituales de identificación de las personas, es por ello por lo que goza de una gran aceptación entre la ciudadanía.

Ilustración 12 - Verificación de firma

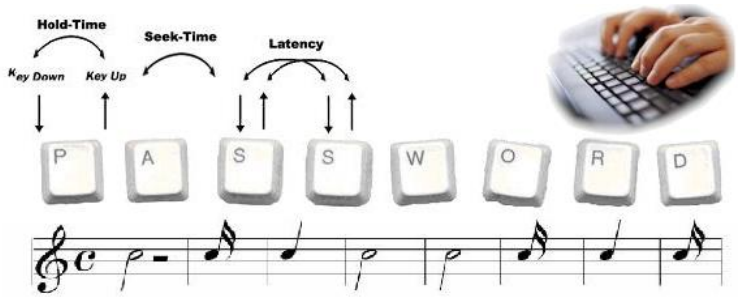


Fuente: Biometric-API (Signature Verification), disponible en: https://en.signotec.com/portal/seiten/biometric-api-signature-verification--900000110-10002.html

Dinámica del tecleo:

En ingles mejor conocida como *"typing biometrics"*, se basa en identificar la velocidad con la que un individuo teclea un número de identificación o su misma contraseña (Ver ilustración 13), siendo un método de autenticidad de la persona, actualmente usada en aplicaciones de comercio electrónico, sus principales ventajas son que no requiere de equipamientos especiales, por lo tanto mantiene un bajo costo, además de no ser intrusivo, no obstante sus índices de falsa aceptación y falso rechazo son el 0,1%, pero requieren de una complementarse con un sistema de identificación y clave del usuario, además de verse sus mediciones se ven afectadas cuando el usuario sufre lesiones o en las manos del usuario [16].

Ilustración 13 - Reconocimiento de tipeo



Fuente: Keystroke Recognition, disponible en: https://deepnetsecurity.com/authenticators/biometrics/typesense/

Matrices de Comparación entre Sistemas Biométricos

Teniendo en cuenta, el estudio sobre las tecnologías biométricas aplicadas a la seguridad, desarrollado por el Observatorio de la Seguridad de la Información, en iniciativa por parte del Ministerio de Turismo y Comercio del Gobierno de España, se ha construido una matriz de cada sistema biométrico incluido en estudio de este documento (Ver Tabla 1), identificando los dispositivos de captura, muestra biométrica, característica a extraer, ventajas y desventajas de cada uno respectivamente [17].

Se puede destacar que, en su mayoría las técnicas hacen uso de imágenes, como son los casos de reconocimiento de huella dactilar, facial, iris retina, geometría de mano y firma manuscrita, factor para tener en cuenta al momento de adquirir dispositivos de captura, a mayor calidad mayor precisión, pero implica tener un mayor espacio de almacenamiento.

Además, se ha incluido una matriz del mismo estudio mencionado anteriormente, donde se observa una valoración comparativa de cada una de las técnicas biométricas (Ver Tabla 2), teniendo en cuenta los siguientes criterios de evaluación:

- Grado de aceptación: Disposición de los usuarios a utilizar una tecnología biométrica.
- Resistencia al fraude: Capacidad del sistema para permitir intentos de autenticación de usuarios permitidos y rechazar los usuarios no autorizados.
- Mensurabilidad: Determinar la capacidad de adquisición y medición precisa de las características de los usuarios, al igual que su nivel de intrusismo.
- Comportamiento: Precisión de reconocimiento que ofrece una técnica biométrica, sumando la madurez del método.
- Permanencia: Característica que determina el grado de variación de un rasgo biométrico a lo largo del tiempo
- Unicidad: Es la característica que determina la diferenciación entre individuos.
- Universalidad: Todo individuo que vaya a hacer uso de la tecnología ha de poseer la característica biométrica evaluada.

Cabe resaltar que, la valoración se ha realizado bajo tres variables, “A” para representar una valoración de nivel “Alto”, M para “Medio” y “B” para “Bajo” respectivamente [18].

Teniendo en cuenta la Tabla 2, se puede observar que la tecnología de reconocimiento de iris es quien posee una mayor calificación, no obstante, no posee un buen grado de aceptación, esto se debe al alto costo de implementación.

Siguiendo con la clasificación, se observa al reconocimiento de retina, sin embargo, esta no esta no posee un buen grado de aceptación al ser una medida altamente invasiva para los usuarios.

Para finalizar, se observa las tecnologías de huella dactilar y reconocimiento facial, compartiendo un alto grado de aceptación y un bajo costo de implementación, además cabe resaltar que la huella dactilar es la tecnología que posee el mayor grado de madurez con respecto a las demás.

Tabla 1 - Tabla comparativa de Sistemas Biométricos.

Tecnología	Dispositivo de captura	Muestra biométrica	Característica extraída	Ventajas	Inconvenientes
Huella dactilar	Periférico de escritorio, tarjeta PCMCIA o lector integrado.	Imagen o minucia de la huella dactilar	Ubicación y dirección del final de las minucias o formas de las huellas	Alto grado de madurez Costos bajos de implementación. Buena aceptación	Incompatibilidad con determinados trabajos manuales
Reconocimiento de voz	Micrófono o teléfono	Grabación de voz	Frecuencia, cadencia y duración del patrón vocal.	No requiere inversión en dispositivos Posibilidad de autenticación remota	Ruido. Dificultad para reconocer ciertas formas de hablar
Reconocimiento facial	Cámara de video o cámara integrada en un PC	Imagen facial	Posición relativa y forma de la nariz, posición de la mandíbula	Reconocimiento en multitudes Identificación a media distancia Buena aceptación	Escasa resistencia al fraude Unicidad limitada

Reconocimiento de iris	Cámara de infrarrojos	Imagen del iris	Surcos y estrías del iris	Patrones muy complejos Unicidad muy alta Alto grado de permanencia	Coste de implantación alto Menor grado de aceptación
Reconocimiento de retina	Unidad propietaria de escritorio o de pared	Imagen de la retina	Patrones de los vasos sanguíneos de la retina	Unicidad muy alta Alto grado de permanencia	Precisa de total colaboración del usuario
Reconocimiento de la geometría de la mano	Unidad propietaria de pared o de pie	Imagen en 2D o 3D de la parte superior y lateral de mano y dedos	Altura y anchura de los huesos y las articulaciones de los dedos y de la mano	Alto grado de permanencia Facilidad de uso	Unicidad limitada
Reconocimiento de firma	Tableta de firma, puntero sensor al movimiento	Imagen de la firma y registro de medidas relacionadas con la dinámica	Velocidad, orden de los trazos, presión y apariencia de la firma	Buena aceptación Facilidad de uso	Dificultad de captura por cambios de posición
Reconocimiento de escritura de teclado	Teclado	Registro de las teclas pulsadas y registro de medidas relacionadas con la dinámica	Secuencia de teclas y pausas entre pulsaciones	No requiere inversión en dispositivos Posibilidad de realizar	Tecnología emergente

				monitorización	

Fuente: Adaptación de Estudio sobre las tecnologías biométricas aplicadas a la seguridad - Ventajas e inconvenientes de las distintas tecnologías, disponible en: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/65877225F2975B3F05257E6E006A2C3D/$FILE/EstudioSobreTecnolog%C3%ADasBiom%C3%A9tricasASeguridad.pdf

Tabla 2 - Valoración comparativa de las distintas técnicas biométricas.

Tecnología	Grado de Aceptación	Resistencia al Fraude	Mensurabilidad	Comportamiento	Permanencia	Unicidad	Universalidad
Huella dactilar	M	A	M	A	A	A	M
Reconocimiento de voz	A	B	M	B	B	B	M
Reconocimiento facial	A	B	A	B	M	B	A
Reconocimiento de iris	B	A	M	A	A	A	A
Reconocimiento de retina	B	A	B	A	A	A	A

Reconocimiento de la geometría de la mano	M	M	A	M	M	M	M
Reconocimiento de firma	A	B	A	B	B	B	B
Reconocimiento de escritura de teclado	M	M	M	B	B	B	B

Fuente: Adaptación de Estudio sobre las tecnologías biométricas aplicadas a la seguridad - Ventajas e inconvenientes de las distintas tecnologías, disponible en: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/65877225F2975B3F05257E6E006A2C3D/$FILE/EstudioSobreTecnolog%C3%ADasBiom%C3%A9tricasASeguridad.pdf

CAPUTULO II – UMBRALIZACIÓN DE FALSA ACEPTACIÓN Y FALSO RECHAZO EN SISTEMAS BIOMÉTRICOS

Como ya se ha descrito anteriormente en este trabajo, los sistemas de autenticación biométrica deben cumplir con características como mensurabilidad, aceptabilidad, rendimiento, evitabilidad o resistencia al fraude.

Enfocándose en la última característica descrita, su objetivo es evitar el acceso de usuarios no autorizados, además de evitar denegar erróneamente el acceso de usuarios autorizados, cabe la posibilidad de presentarse ambos casos, causados por factores que afectan la captura del rasgo biométrico, pueden ser provocados por cambios climáticos, luminosos o hasta el mismo paso del tiempo.

Por la misma razón, es importante tener presente un margen de error presente en cada captura, para ello cada sistema biométrico manejan las siguientes variables [19]:

- Tasa de Falsa Aceptación (FAR) - Es la probabilidad de que un sistema vincule erróneamente a un individuo con la información biométrica existente de otra persona, de forma que este usuario no autorizado pase por alguien que sí lo estuviese. Sus valores suelen oscilar entre 0.0001% y 0.1% para ser aceptables.
- Tasa de Falso Rechazo (FRR) - Es la probabilidad de que el sistema no vincule a un individuo con su propia plantilla biométrica existente en el registro. Sus valores suelen estar entre el 0.00066 % y el 1 % para ser aceptables.
- Tasa de Error Equitativa (EER) - La FAR y la FRR son inversamente proporcionales y afectarán de manera creciente o decreciente a la sensibilidad del dispositivo. La Tasa de Error Equitativa es el punto de corte de las dos anteriores y corresponde a una indicación buena de la ejecución del método biométrico. Es mejor cuanto más pequeña.

Umbralización de Tasa de Falsa Aceptación (FAR) y Tasa de Falso Rechazo (FRR)

Como se ha expresado anteriormente un sistema de reconocimiento biométrico puede darse de dos formas, identificación y verificación, la primera busca encontrar la identidad de la persona, buscando en todos los registros del sistema y la segunda parte de ya tener a priori la identidad de la persona y se encarga de validar que esa identidad corresponda con la planilla biométrica del usuario almacenada en el sistema.

En cuestión ambas formas realizan una comparación de los patrones biométricos haciendo uso de puntajes (también llamados pesos) para expresar la similitud entre un patrón y una plantilla biométrica. Cuanto mayor es el puntaje, mayor es la similitud entre ellos. En otras palabras, el sistema logrará identificar o validar la identidad de esta solo si el puntaje obtenido logra superar un cierto valor umbral [20].

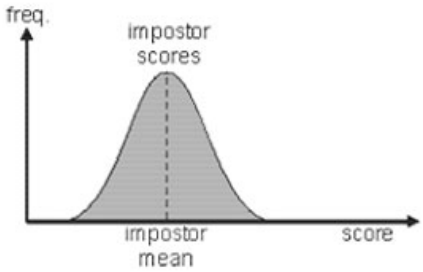
En teoría, los puntajes de los clientes (puntajes de patrones de personas conocidas por el sistema) siempre deben ser más altos que los puntajes de los impostores. Si esto fuera cierto, un único umbral, que separa los dos grupos de puntajes, podría usarse para diferir entre clientes e impostores.

Debido a varios factores, esta suposición en la vida real no aplica para los sistemas biométricos, cabe la posibilidad que patrones impostores generen puntajes más altos que los puntajes de algunos patrones de clientes. Por esa razón, es un hecho que, sin importar el umbral de clasificación elegido, se producen algunos errores de clasificación.

Por ejemplo, en un sistema de verificación biométrica se le procesa con una cantidad considerable de datos de prueba, clasificados previamente en patrones de usuarios impostores (Ver Ilustración 14) y usuarios válidos

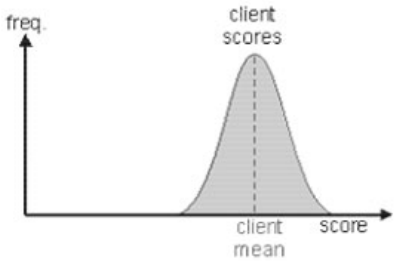
(Ver Ilustración 15), categorizados en poblaciones bajo una distribución normal gaussiana respectivamente.

Ilustración 14 - Distribución normal de impostores



Fuente: False Acceptance Rate (FAR) and False Recognition Rate (FRR) in Biometrics, disponible en: https://www.bayometric.com/false-acceptance-rate-far-false-recognition-rate-frr/

Ilustración 15 - Distribución normal de clientes

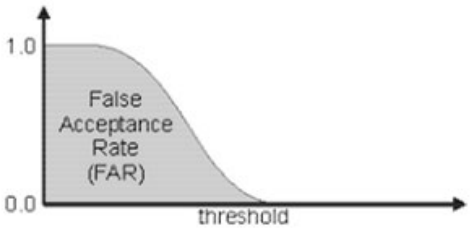


Fuente: False Acceptance Rate (FAR) and False Recognition Rate (FRR) in Biometrics, disponible en: https://www.bayometric.com/false-acceptance-rate-far-false-recognition-rate-frr/

Dependiendo de la elección del umbral de clasificación, entre todos y ninguno de los patrones impostores y validos son falsamente aceptados o erróneamente rechazados por el sistema.

- La fracción dependiente del umbral de los patrones falsamente aceptados dividida por el número de todos los patrones impostores se llama Tasa de aceptación falsa (FAR). Ver ilustración 16.

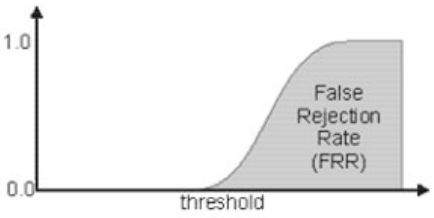
Ilustración 16 - Taza de aceptación falsa (FAR)



Fuente: False Acceptance Rate (FAR) and False Recognition Rate (FRR) in Biometrics, disponible en: https://www.bayometric.com/false-acceptance-rate-far-false-recognition-rate-frr/

- La fracción de la cantidad de patrones de clientes rechazados dividida por la cantidad total de patrones de clientes se denomina tasa de reconocimiento falso (FRR). Ver ilustración 17.

Ilustración 17 - Taza de falso rechazo (FRR)

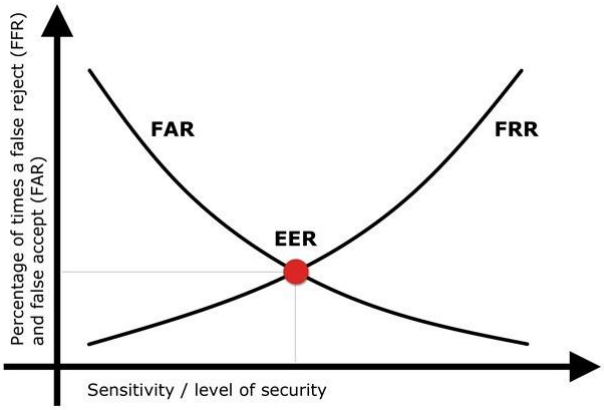


Fuente: False Acceptance Rate (FAR) and False Recognition Rate (FRR) in Biometrics, disponible en: https://www.bayometric.com/false-acceptance-rate-far-false-recognition-rate-frr/

A medida que disminuye el número de aceptaciones falsas (FAR), el número de rechazos falsos (FRR) aumentará y viceversa (Ver Ilustración 18). El punto en el que se cruzan las líneas se le conoce como, error igual

(EER). Aquí es donde el porcentaje de aceptaciones falsas y rechazos falsos es el mismo.

Ilustración 18 - Error igual de tazas de FRR y FAR



Fuente: Recogtech, FAR y FRR: nivel de seguridad versus comodidad del usuario, disponible en: https://www.recogtech.com/en/knowledge-base/security-level-versus-user-convenience

Desde otro punto de vista, si el sistema biométrico es configurado para no permitir el acceso de ningún intruso, puede resultar en el rechazo de acceso a clientes válidos, en cambio, cuando la prioridad es el ágil y fácil acceso del usuario el sistema resulta menos seguro, pero más conveniente en algunas ocasiones.

Por la misma razón, al momento de comparar un sistema biométrico teniendo en cuenta su taza de aceptación falsa (FAR), es necesario tener conocimiento de su tasa de reconocimiento falso rechazo (FRR), para para evaluar qué es lo más conveniente para el sistema.

CAPITULO III – PRUEBA DE RENDIMIENTO CON CURVAS ROC

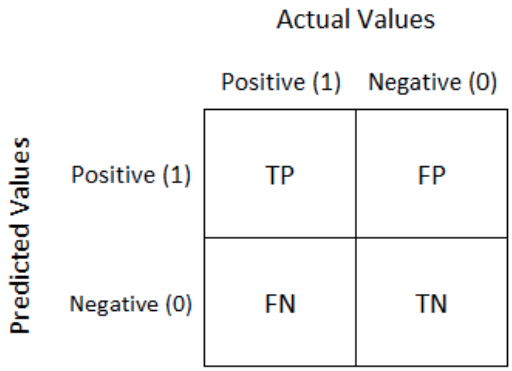
La importancia de elegir un valor umbral de aceptación para una tecnología biométrica, recae principalmente que, dependiendo del mismo, da resultado a la taza de falsa aceptación (FAR) y taza de falso rechazo (FRR) del sistema, importantes para medir el nivel de seguridad y conveniencia hacia el usuario.

Es por ello, para medir el rendimiento de una tecnología biométrica, se puede hacer uso de una herramienta estadística llama curva ROC (Características operativas del receptor), esta permite cuantificar la capacidad de un indicador diagnóstico, en otras palabras, nos permite medir el rendimiento en un problema de clasificación, para el caso, discriminar entre usuarios autorizados e intrusos [21].

Se define como, una curva de probabilidad y el área bajo esta curva representa el grado o medida de separabilidad, también conocido como estadístico C o por sus siglas en ingles AUC (Área bajo la Curva), conjuntamente puede ser expresada como AUC-ROC o AUROC (Área bajo las características operativas del receptor).

Para comprender mejor el funcionamiento y terminología que maneja la curva ROC, primero hay que entender el concepto de “Matrix de Confusión”, este se expresa como una medida de rendimiento para un problema de clasificación de aprendizaje automático donde la salida puede ser de dos o más clases, se puede graficar de la siguiente forma (ver Ilustración 19) [22].

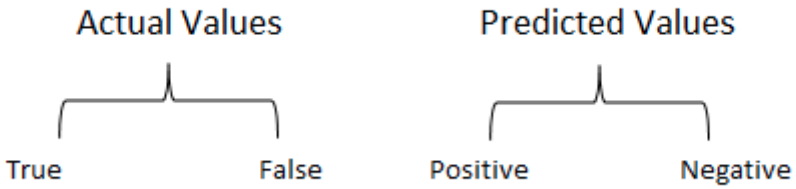
Ilustración 19 - Matriz de confusión



Fuente: Understanding Confusion Matrix, disponible en: https://towardsdatascience.com/understanding-confusion-matrix-a9ad42dcfd62

Nótese que, la matriz de confusión (Ver ilustración 19) clasifica los valores en dos clases, valores pronosticados y valores reales, el primero clasifica los valores como positivos y negativos y la segunda clase como verdaderos y falsos, como se ilustra a continuación (Ver ilustración 20).

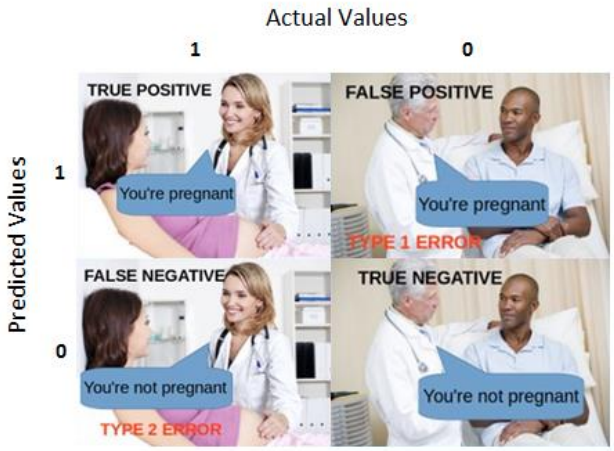
Ilustración 20 - Clasificación de valores



Fuente: Understanding Confusion Matrix, disponible en: https://towardsdatascience.com/understanding-confusion-matrix-a9ad42dcfd62

Para comprender mejor el concepto de estas dos clases tener en cuenta la siguiente analogía, donde se observan cuatro situaciones (Ver ilustración 21).

Ilustración 21 - Analogía embarazo (Matriz de confusión)



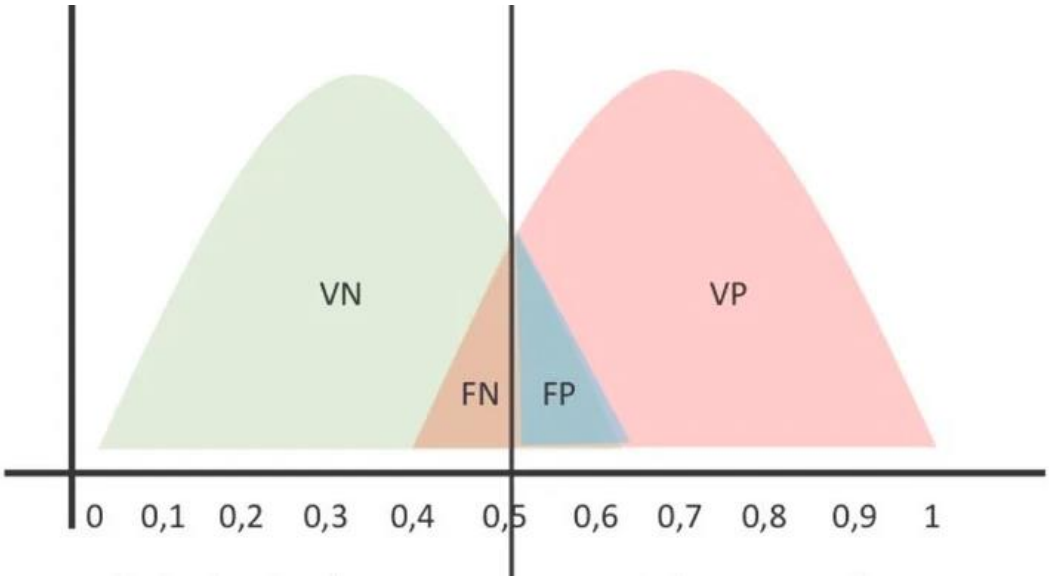
Fuente: Understanding Confusion Matrix, disponible en: https://towardsdatascience.com/understanding-confusion-matrix-a9ad42dcfd62

- La primera situación: Una doctora le comunica a una mujer evidentemente embarazada que está embarazada, este caso se lo conoce como un “Verdadero Positivo (TP)”, porque se predice algo positivo y es verdad.
- La segunda situación: Un doctor le comunica a un hombre que esta embarazado, algo naturalmente imposible, este caso se lo conoce como “Error Tipo 1” o “Falso Positivo (FP)”, porque se predice algo positivo y es falso.
- La tercera situación: Una doctora le comunica a una mujer evidentemente embarazada que no está embarazada, este caso se lo conoce como "Error Tipo 2" o “Falso Negativo (FN)”, porque se predice algo negativo y es falso.
- La cuarta situación: Un doctor le comunica a un hombre que no está embarazado, este cao se lo conoce como “Verdadero Negativo (TN)”.

Para brindar mayor claridad de estos conceptos, observar la siguiente imagen (Ver Ilustración 22), en ella, se identifican claramente donde se

encontraría cada una de estas variables en un gráfico donde dos poblaciones de clasificación se solapan.

Ilustración 22 - Variables de clasificación



Fuente: Curvas ROC y Área bajo la curva (AUC), disponible en: https://ligdigonzalez.com/curvas-roc-y-area-bajo-la-curva-auc-machine-learning/

Definición de términos utilizados en las curvas AUC y ROC.

Teniendo presente, las variables que manejadas por una matriz de confusión y como clasificaría cada uno de los casos planteados a una prueba realizada a una tecnología biométrica, procedemos a definir las fórmulas aplicadas por la curva ROC para medir el rendimiento de la tecnología [23].

La primera de ellas, denominada TPR (Tasa de verdaderos positivos) o también conocida como Sensibilidad, resuelve, de todas las clases positivas, cuánto se predijo correctamente (Ver ilustración 23).

Ilustración 23 - Formula de Sensibilidad

$$\text{TPR /Recall / Sensitivity} = \frac{TP}{TP + FN}$$

Fuente: Understanding AUC - ROC Curve, disponible en: https://towardsdatascience.com/understanding-auc-roc-curve-68b2303cc9c5

La segunda, conocida como Especificidad, resuelve, de todas las clases negativas, cuanto se predijo correctamente (Ver ilustración 24).

Ilustración 24 - Formula de Especificidad

$$\text{Specificity} = \frac{TN}{TN + FP}$$

Fuente: Understanding AUC - ROC Curve, disponible en: https://towardsdatascience.com/understanding-auc-roc-curve-68b2303cc9c5

La tercera, conocida como FPR o FAR (Tasa de Falsos Positivos), resuelve, de todas las clases negativas, cuanto se predijo erróneamente, en otras palabras, sería el complementario de la especificidad (Ver Ilustración 25).

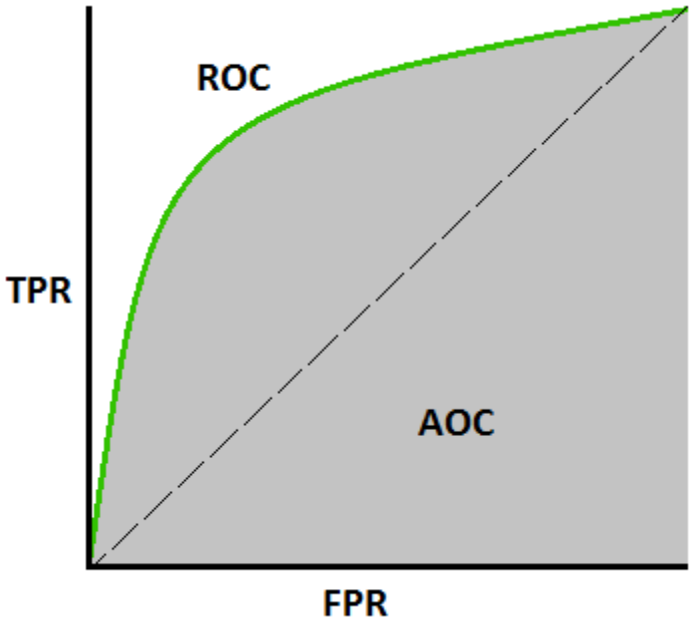
Ilustración 25 - Formula de FPR (Tasa de Falsos Positivos)

$$\text{FPR} = 1 - \text{Specificity} = \frac{FP}{TN + FP}$$

Fuente: Understanding AUC - ROC Curve, disponible en: https://towardsdatascience.com/understanding-auc-roc-curve-68b2303cc9c5

Comprendido lo anterior, para cada valor umbral se calculará las variables TPR (Sensibilidad) y FPR (1-Especificidad), cada par de resultados forma una coordenada en un plano cartesiano, ubicando TPR en ordenadas y FPR en abscisas (Ver Ilustración 26).

Ilustración 26 - Curva AUC - ROC



Fuente: Understanding AUC - ROC Curve by Sarang Narkhede (2018), disponible en: https://towardsdatascience.com/understanding-auc-roc-curve-68b2303cc9c5

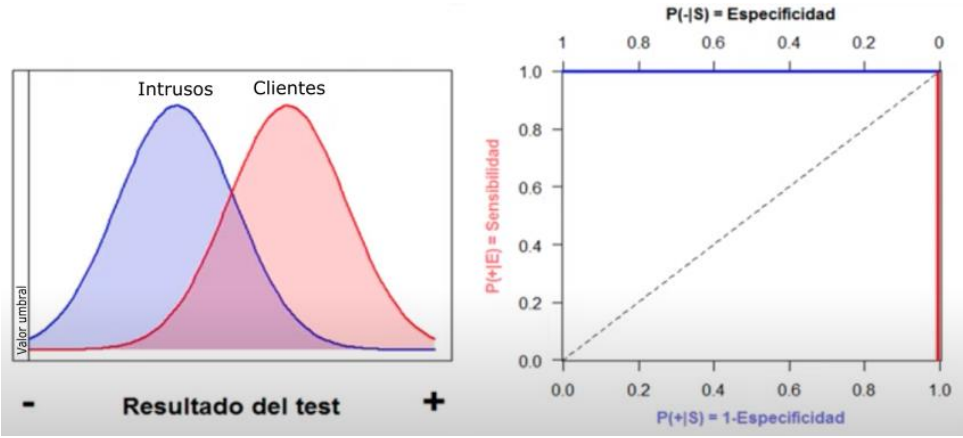
Especulación de Rendimiento Bajo Curva ROC

Teniendo claro que, la curva ROC es una curva de probabilidades y su AUC representa su grado de separabilidad, por ende, si su valor se acerca a 1 representa que tiene una alta medida de separabilidad, si su valor es 0.5 significa que el modelo no tiene capacidad de separación de clases, si el valor es próximo a 0 representa que el modelo predice incorrectamente el resultado.

Para brindar mayor comprensión en la lectura y especulación de una curva ROC, se han adaptado unas gráficas como ejemplo, en primera instancia ilustrando como se forma la curva a o partir del desplazamiento del valor umbral. Además, observar como el AUC se ve afectada dependiendo del solapamiento entre las dos poblaciones de estudio, para el caso, clientes e intrusos.

Para empezar, observar como en la siguiente imagen (Ver Ilustración 27), se encuentran dos gráficas, en el lado izquierdo se encuentra el solapamiento de las poblaciones de intrusos y clientes, además del punto de corte del valor umbral, por el lado derecho se encuentra un plano cartesiano, donde se formará la curva ROC, bajo las variables de Sensibilidad (marcada con una línea roja) en ordenadas, y FPR (Tasa de falsos positivos) o su inversa, la especificidad (marcada con una línea azul) en abscisas, ilustrada en la parte superior de plano [24].

Ilustración 27 - Curva ROC - Valor Umbral en 0

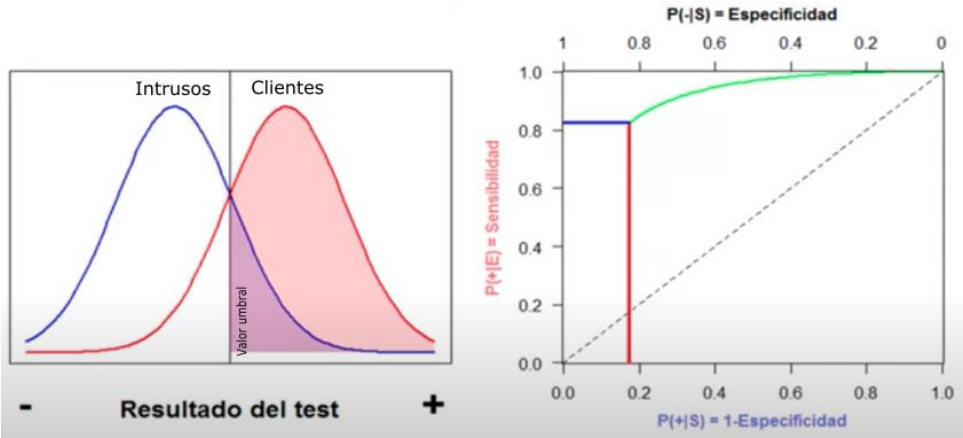


Fuente adaptada: Curva (2014), disponible en: https://www.youtube.com/watch?v=fsgDD0pNkZ0

En primera instancia, el valor umbral se ubica a la izquierda del solapamiento de poblaciones, en este punto, el sistema permitirá el acceso de los todos los clientes, no obstante, de igual forma, de todos los intrusos, en otras palabras, no se limita el acceso, a medida que este valor se

desplaza a la derecha, aumentará su especificidad y gradualmente disminuirá su sensibilidad.

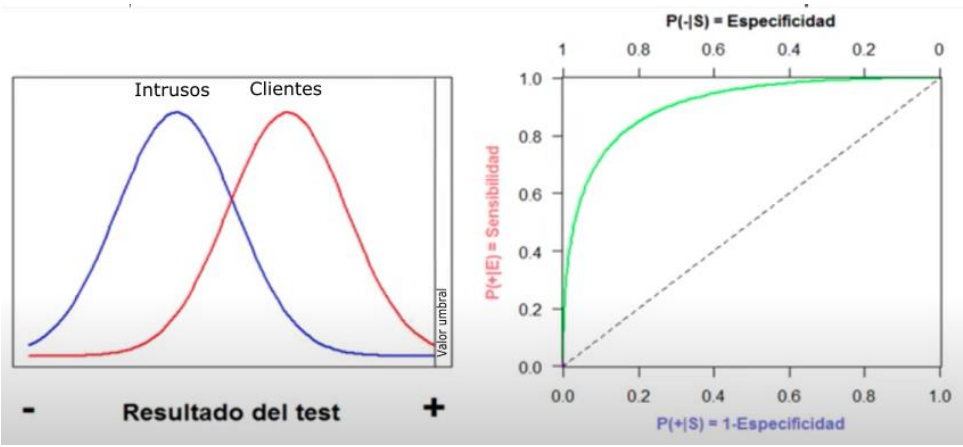
Ilustración 28 - Curva ROC, Valor Umbral en 0.5



Fuente adaptada: Curva (2014), disponible en: https://www.youtube.com/watch?v=fsgDD0pNkZ0

Nótese en la imagen anterior (Ver Ilustración 28), el valor umbral ahora se ha posicionado en un punto intermedio entre las dos poblaciones, este punto es especial, porque Sensibilidad y Especificidad tienen el mismo valor, en este caso en concretos a 0.82, se puede interpretar que, se ha ganado un 82 por ciento de especificidad a un costo de perder un 12% de sensibilidad, a partir de este punto, a medida que se desplace a la derecha el valor umbral, la sensibilidad empezará a descender más rápido hasta llegar a 0.

Ilustración 29 - Curva ROC, Valor Umbral en 1

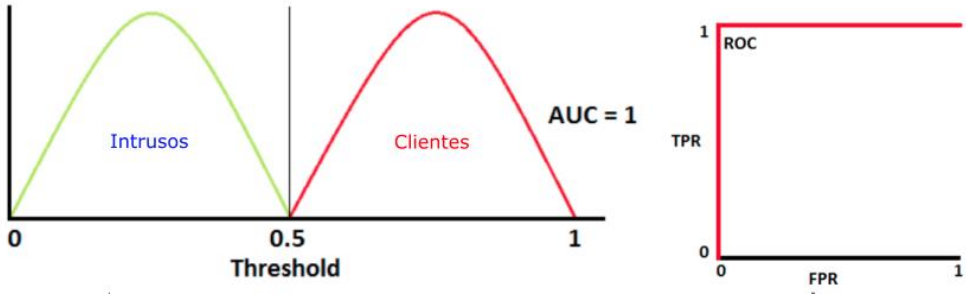


Fuente adaptada: Curva (2014), disponible en: https://www.youtube.com/watch?v=fsgDD0pNkZ0

Una vez el valor umbral se encuentre a la derecha del solapamiento de las poblaciones, se habrán calculado todos los niveles de sensibilidad y especificidad hasta ese punto, por ende, se encontrará completa la curva ROC, en la gráfica ilustrada con una línea verde (Ver ilustración 29), con ella, se podría calcular su AUC.

En una situación ideal, cuando las poblaciones no se superponen en lo absoluto (Ver ilustración 30), el modelo tiene una medida ideal de separabilidad, en otras palabras, puede distinguir sin problemas de entre intrusos y clientes, se interpretaría como un AUC del 100%.

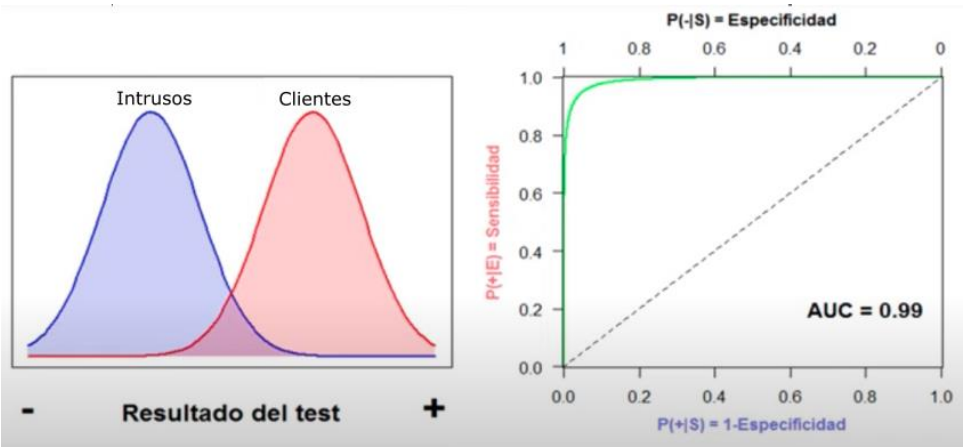
Ilustración 30 - Curva ROC, AUC de 100%



Fuente adaptada: Understanding AUC - ROC Curve (2018), disponible en: https://towardsdatascience.com/understanding-auc-roc-curve-68b2303cc9c5

En el momento que estas dos poblaciones se solapen, se introducirá a la gráfica, los errores tipo 1(falso positivo) y tipo 2 (falso negativo), dependiendo de umbral que se escoja se podrá minimizarlos o maximizarlos, cuando se tiene un AUC igual a 0,99 (Ver ilustración 31), representa que hay un 99% de posibilidades que le modelo sepa distinguir entre una clase y la otra.

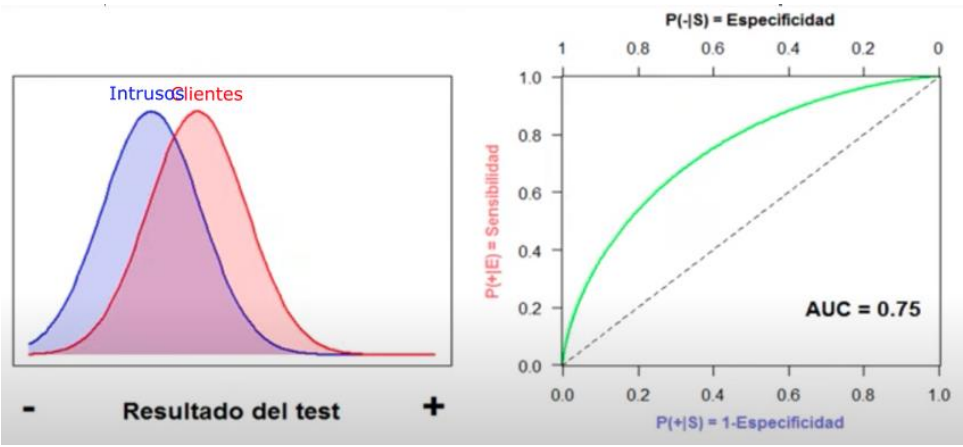
Ilustración 31 - Curva ROC, AUC de 99%



Fuente adaptada: Curva (2014), disponible en: https://www.youtube.com/watch?v=fsgDD0pNkZ0

A medida que, más se solapan las poblaciones, significa que los resultados entre clientes e intrusos son cada vez más se semejantes, por lo tanto, más baja la capacidad discriminatoria del indicador. Observar como en la siguiente imagen (Ver ilustración 32) se tiene una curva ROC con un AUC del 75%, se podría interpretar que en un 25% de los casos se rechazará erróneamente el acceso a un usuario o más grave aún, se permitirá el acceso a un intruso.

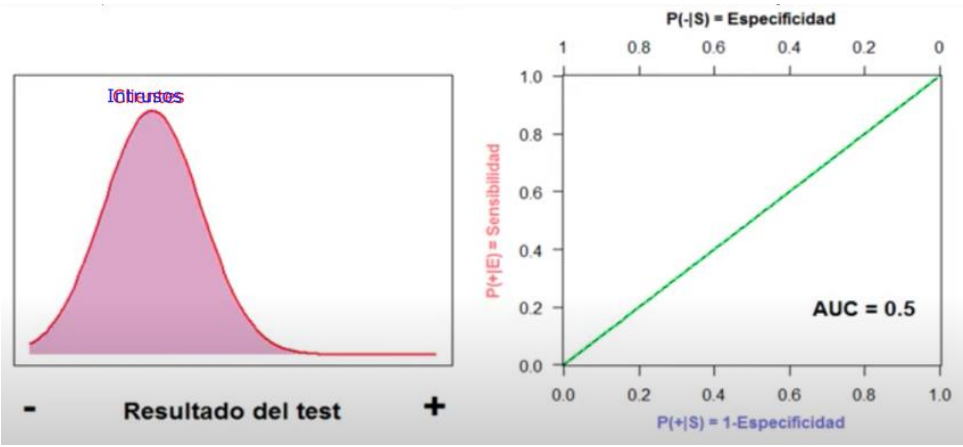
Ilustración 32 - Curva ROC, AUC de 75%



Fuente adaptada: Curva (2014), disponible en: https://www.youtube.com/watch?v=fsgDD0pNkZ0

En el momento que la curva ROC llegue a un valor de AUC de 0.5 como se muestra a continuación (Ver ilustración 33), significa que, el modelo discriminante no tiene la capacidad de diferenciar una clase de otra, entonces, el sistema no podría distinguir un cliente de un impostor, prácticamente su resultado sería aleatorio.

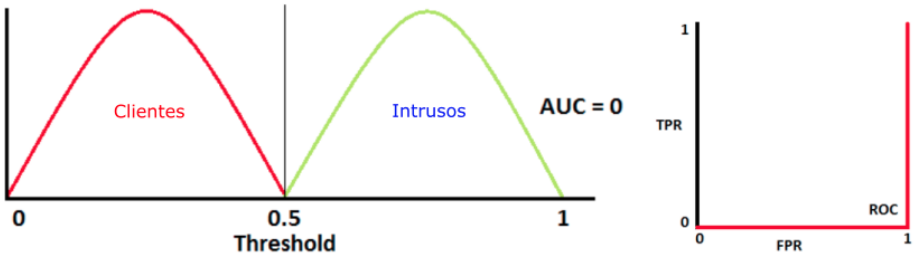
Ilustración 33 - Curva ROC, AUC de 50%



Fuente adaptada: Curva (2014), disponible en: https://www.youtube.com/watch?v=fsgDD0pNkZ0

Dado el caso que, el AUC resultante es 0, como se observa a continuación (Ver ilustración 34), se puede interpretar que el modelo está prediciendo las clases erróneamente, es decir el modelo o el sistema identificará a los clientes como intrusos y viceversa.

Ilustración 34 - Curva ROC, AUC de 0%



Fuente adaptada: Understanding AUC - ROC Curve (2018), disponible en: https://towardsdatascience.com/understanding-auc-roc-curve-68b2303cc9c5

Es así, como se ha observado en las gráficas anteriores, se puede resaltar que, la sensibilidad es inversamente proporcional a la especificidad, entonces, cuando se aumenta el valor umbral, obtenemos una mayor especificidad y una menor sensibilidad, caso contrario cuando se disminuya el mismo.

Además, la calidad diagnostica de un modelo, que es medida, por el AUC resultante de una curva ROC, se ve afectada directamente por, el solapamiento de las poblaciones de estudio, resultando en el incremento de alguna de las tasas de error, como son los falsos positivos y los falsos negativos

Para finalizar, en la intensión de comparar simultáneamente dos o más curvas ROC, se construye un estadístico basado en sus respectivas AUC y se estudia su distribución asintótica, análisis acompañando de, simulaciones que muestran su comportamiento.

Curva AUC ROC para modelo de varias clases

Para comparar dos o más curvas ROC, el cálculo de su AUC (área bajo la curva) permite medir la capacidad discriminante de cada modelo, determinando cuál es más eficaz.

El rango de valores de un AUC puede ir desde 0,5, siendo este valor es correspondiente a una prueba sin capacidad discriminante, hasta 1, que es representa que los dos grupos están perfectamente diferenciados por la prueba y, por lo tanto, se puede decir que cuanto mayor sea el AUC mejor será la prueba [25].

Observar como en la siguiente imagen (Ver ilustración 35), se clasifican los rangos de un estadístico AUC, dicta que valores menores a 0,7, el modelo posee una baja capacidad discriminante, para valores entre 0,7 y 0,9 el modelo resulta útil para algunos propósitos, con valores superiores a 0,9 se entiende que el modelo posee una alta exactitud discriminante.

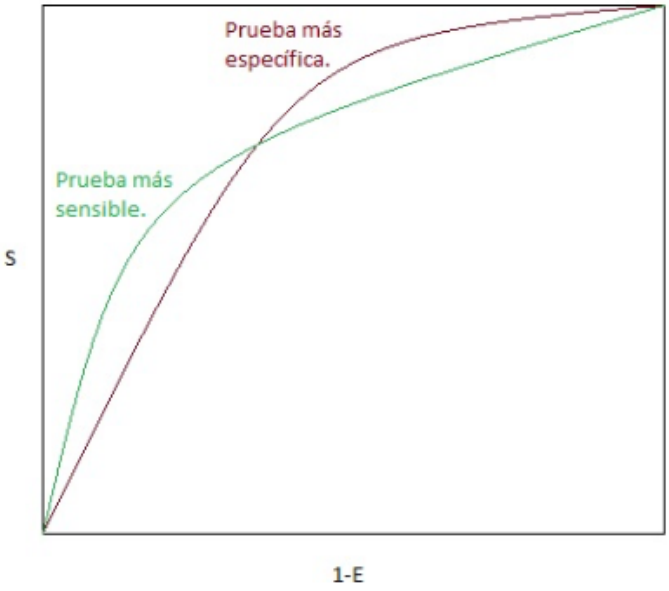
Ilustración 35 - Clasificación de valor AUC

Baja exactitud:$[0'5, 0'7)$
Útiles para algunos propósitos:$[0'7, 0'9)$
Exactitud alta:$[0'9, 1]$

Fuente adaptada: Understanding AUC - ROC Curve (2018), disponible en: https://towardsdatascience.com/understanding-auc-roc-curve-68b2303cc9c5

Dos curvas ROC iguales tendrán la misma área, no obstante, dos áreas iguales no representan curvas iguales (Ver ilustración 36), ambas curvas tienen igual área, no obstante, la curva verde proporciona una prueba más sensible, mientras que, la curva roja corresponde a una prueba más específica.

Ilustración 36 - Prueba específica vs prueba sensible

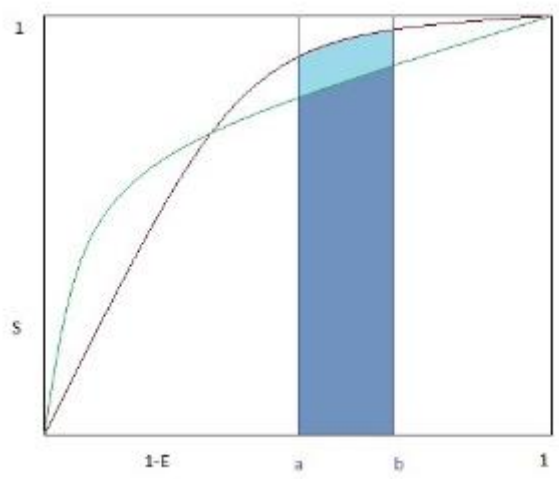


Fuente adaptada: Understanding AUC - ROC Curve (2018), disponible en: https://towardsdatascience.com/understanding-auc-roc-curve-68b2303cc9c5

Una prueba más sensible, representa una mayor proporción de falsos positivos, son principalmente usadas para propósitos preventivos. Por otro lado, una prueba específica, representa una mayor proporción de falsos negativos, mayormente aplicada en el tamizaje de enfermedades.

Otra forma para identificar si dos AUC iguales son resultado de una o dos curvas ROC es, calcular el área parcial bajo cada curva ROC, se define como, calcular el área de la región delimitada entre la curva, el eje horizontal y dos abscisas dadas “a” y “b" en el eje horizontal, donde “a” sea menor a “b” como se observa en la imagen a continuación (Ver ilustración 37).

Ilustración 37 - Área parcial bajo la curva ROC



Fuente adaptada: Understanding AUC - ROC Curve (2018), disponible en: https://towardsdatascience.com/understanding-auc-roc-curve-68b2303cc9c5

Observación, la diferencia de área parciales en distintos intervalos, no es un valor de interés, por lo tanto, para realizar un estudio comparativo de dos curvas dadas, hay que estudiar la diferencia del área parcial de las mismas.

No obstante, no olvidar que las pruebas van a tener variabilidad inevitable de muestreo, esto plantea una interrogante, ¿la prueba posee mayor área única y exclusivamente por poseer una capacidad discriminante mayor o es causa de la variabilidad de la muestra?

Ante este interrogante, Hanley y Mc Neil proponen un modelo estadístico (Ver ilustración 38), donde haciendo uso de unas correlaciones calculadas de las áreas entre la desviación estándar (SD) de las mismas.

Ilustración 38 - Coeficiente de correlación de dos áreas

$$r = \frac{cov(\widehat{AUC}_1, \widehat{AUC}_2)}{SD(\widehat{AUC}_1) \cdot SD(\widehat{AUC}_2)}$$

Fuente adaptada: Understanding AUC - ROC Curve (2018), disponible en: https://towardsdatascience.com/understanding-auc-roc-curve-68b2303cc9c5

Cabe aclarar que, el modelo solo es para discriminar entre la igualdad o la desigualdad de dos curvas. Sin embargo, los mismos autores plantean que esta prueba no es suficiente, por lo cual recomiendan, siempre acompañarla de un examen visual de curvas.

Para finalizar, se puede decir que la comparación entre dos curvas ROC o más, existe la posibilidad que posean un mismo valor de AUC, y no necesariamente significa que el resultado de las pruebas sea el mismo, si son comparadas gráficamente dependiendo de su punto óptimo darán como resultado una prueba con mayor sensibilidad o con mayor especificidad.

CONCLUSIONES

- La tecnología biométrica con mayor grado de resistencia al fraude es el reconocimiento de iris, seguida del reconocimiento de retina, no obstante, ambas poseen un bajo grado de aceptación, la primera por su alto coste de implementación y la segunda por ser altamente intrusivo con los usuarios.
- Ajustar el umbral de aceptación en un sistema biométrico influye directamente en la seguridad de acceso de este, la dificultad se origina en encontrar un punto de equilibrio que permita al sistema ser lo más seguro posible sin afectar al usuario o a la empresa, dificultando o retrasando en las funciones normales de los mismos.
- Las empresas distribuidoras de sistemas biométricos resaltan principalmente mantener una baja taza de falsa aceptación (FAR), si bien esto representa mayor seguridad en el sistema, solo es la mitad de la información, es importante conocer la taza de falso rechazo (FRR) del sistema, si este es muy alto representará mayor incomodidad para el usuario. Por lo tanto, al momento de querer adquirir una tecnología biométrica, informarse de ambas variables, además si es posible ajustar el umbral de selección de este.
- La herramienta estadística del AUC-ROC, permite medir el rendimiento de un modelo discriminante, definiendo la probabilidad de clasificar correctamente un caso, un ejemplo de ello, las tecnologías de autenticación biométrica, que partiendo del análisis de los rasgos biométricos de los usuarios determinan si se corresponden a un cliente o un intruso, su AUC-ROC representa su nivel de certeza.
- La sensibilidad es inversamente proporcional a la especificidad, dependiendo del ajuste del valor umbral, es posible aumentar la sensibilidad del modelo, sacrificando proporcionalmente su especificidad, o puede darse el caso contrario, dependiendo de lo más adecuado al sistema.

- En una tecnología biométrica, el valor de su AUC-ROC representa el nivel de acierto en la clasificación de los usuarios, a medida que este valor desciende o se acerca a 0.5, se interpreta que la tecnología está perdiendo su capacidad discriminante, puede ser causado por el aumento de las tasas de error como FAR y FRR.
- Una prueba con mayor sensibilidad representa una mayor proporción de falsos positivos, sus usos se dan principalmente sistemas de identificación y prevención, mientras que, una prueba específica, representa una mayor proporción de falsos negativos y aplicadas principalmente para sistemas de alta seguridad.
- En la comparación entre dos curvas o más ROC cabe la posibilidad que posean un mismo valor de AUC, y no necesariamente significa que el resultado de las pruebas sea el mismo, si son comparadas gráficamente dependiendo de su punto óptimo darán como resultado una prueba con mayor sensibilidad o con mayor especificidad.

BIBLIOGRAFÍA ESPECÍFICA

[1] GIRALDO A. y GOMEZ D., ESTADO DEL ARTE DE LA SEGURIDAD EN SISTEMAS BIOMETRICOS, https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/14348/1/52752700.pdf (2017) , p. 17 (consultada el 20/10/2019)

[2] INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA, Tecnologías biométricas aplicadas a la ciberseguridad (2016), https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf , p. 5 (consultada el 10/11/2019)

[3] CARDOSO MORENO A. M., Métodos Biométricos de Autenticación e Identificación, Trabajo Final de Especialización, (2014), p. 1.

[4] PUISOL G., Sistema de verificación de huellas digitales, https://rdu.unc.edu.ar/bitstream/handle/11086/12/14436.pdf;sequence=1 (2007), pp. 5-6 (consultada el 24/10/2019)

[5] CARDOSO MORENO A. M., Métodos Biométricos de Autenticación e Identificación, Trabajo Final de Especialización, (2014), p. 2-6.

[6] CARDOSO MORENO A. M., Métodos Biométricos de Autenticación e Identificación, Trabajo Final de Especialización, (2014), p. 7.

[7] INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA, Tecnologías biométricas aplicadas a la ciberseguridad (2016), https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf , p. 7 (consultada el 10/11/2019)

[8] ALSAADI I, Physiological Biometric Authentication Systems, Advantages, Disadvantages And Future Development: A Review, INTERNATIONAL

JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 4, ISSUE 12, DECEMBER 2015, ISSN 2277-8616

[9] BORJA TOLOSA C y GIZ BUENO A., Sistemas Biométricos - Reconocimiento Facial – Escáner de Rostro, https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf (consultada el 18/12/2019)

[10] ECURED, Geometría de la mano (2017), https://www.ecured.cu/Geometr%C3%ADa_de_la_mano (consultada el 10/12/2019)

[11] LÍNEA DE CÓDIGO, Biometría Aplicada a La Seguridad (2019), https://www.lineadecodigo.es/biometra-aplicada-a-la-seguridad-introduccin (consultada el 14/01/2020)

[12] BORJA TOLOSA C y GIZ BUENO A., Sistemas Biométricos - Reconocimiento de iris, https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf (consultada el 18/12/2019)

[13] CARDOSO MORENO A. M., Métodos Biométricos de Autenticación e Identificación, Trabajo Final de Especialización, (2014), p. 12.

[14] BIOMETRIC VOX, ¿Cómo funciona la biometría de voz? (2015), https://biometricvox.com/blog/biometria-de-voz/como-funciona-la-biometria-de-voz/ (consultada el 16/12/2019)

[15] OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN DE ESPAÑA, Estudio sobre las tecnologías biométricas aplicadas a la seguridad - Reconocimiento de firma (2016), http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/65877225F2975B3F05257E6E006A2C3D/$FILE/EstudioSobreTecnolog%C3%ADasBiom%C3%A9tricasASeguridad.pdf , p. 38 (consultada el 10/11/2019)

[16] DEEPNET SECURITY, Keystroke Recognition, https://deepnetsecurity.com/authenticators/biometrics/typesense/ (consultada el 16/12/2019)

[17] OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN DE ESPAÑA, Estudio sobre las tecnologías biométricas aplicadas a la seguridad - CONCEPTOS CLAVE (2016), http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/65877225F2975B3F05257E6E006A2C3D/$FILE/EstudioSobreTecnolog%C3%ADasBiom%C3%A9tricasASeguridad.pdf , p. 23-25 (consultada el 18/01/2020)

[18] OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN DE ESPAÑA, Estudio sobre las tecnologías biométricas aplicadas a la seguridad - COMPARATIVA DE TÉCNICAS Y TECNOLOGÍAS BIOMÉTRICAS (2016), http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/65877225F2975B3F05257E6E006A2C3D/$FILE/EstudioSobreTecnolog%C3%ADasBiom%C3%A9tricasASeguridad.pdf , p. 39-42 (consultada el 25/01/2019)

[19] RECOGTECH, FAR & FRR: SECURITY LEVEL VERSUS USER CONVENIENCE (2020), https://www.recogtech.com/en/knowledge-base/security-level-versus-user-convenience , (consultada el 8/02/2020)

[20] THAKKAR D., False Acceptance Rate (FAR) and False Recognition Rate (FRR) in Biometrics (2019), https://www.bayometric.com/false-acceptance-rate-far-false-recognition-rate-frr/ , (consultada EL 08/02/2020)

[21] NARKHEDE S., AUC-ROC CURVE (2018), https://towardsdatascience.com/understanding-auc-roc-curve-68b2303cc9c5 , (consultada el 14/03/2020)

[22] NARKHEDE S., Understanding Confusion Matrix (2018), https://towardsdatascience.com/understanding-confusion-matrix-a9ad42dcfd62 , (consultada el 14/03/2020)

[23] ARMESTO D., PRUEBAS DIAGNÓSTICAS: CURVAS ROC (2011), https://biomed.uninet.edu/2011/n1/armesto.pdf , (consultada el 15/03/2020)

[24] BIOESTADISTICA PARA NO ESTADISTICOS, Curva ROC (2014), https://www.youtube.com/watch?v=fsgDD0pNkZ0 , (consultada el 28/03/2020)

[25] DEL VALLE BENAVIDES A., Curvas ROC (Reciver-Operating-Characteristic) y sus aplicaciones, Trabajo Final de Grado en Matemáticas, Universidad de Sevilla, https://idus.us.es/bitstream/handle/11441/63201/Valle%20Benavides%20Ana%20Roc%C3%ADo%20del%20TFG.pdf?sequence=1 , Capítulo 3 Medidas de exactitud para un clasificacador 38 (consultada el 10/07/2020)

[26] Hanley JA, McNeil BJ (1983): 'A method of comparing the areas under receiver operating characteristic curves derived from the same cases'. Radiology; 148: 839-843.

BIBLIOGRAFÍA GENERAL

- Tecnologías biométricas aplicadas a la ciberseguridad (2016)
- Métodos Biométricos de Autenticación e Identificación (2014)
- False Acceptance Rate (FAR) and False Recognition Rate (FRR) in Biometrics (2019)
- Understanding AUC - ROC Curve (2018)
- Curvas ROC (Reciver-Operating-Characteristic) y sus aplicaciones

INDICE DE ILUSTRACIONES

INDICE DE MATRICES