
What is
VO
I
CE
biometrics ?
mobbeel

Índice de contenidos

01.
¿Qué es la biometría de voz?

La biometría permite determinar la identidad de una persona mediante el análisis de uno o más **rasgos físicos** (cara, voz, huella, iris, patrón venoso...) o de **comportamiento** (firma, marcha, interacción con aplicaciones móviles...).

La **biometría de voz** es una tecnología que utiliza la voz humana para identificar y autenticar personas. Parte de la premisa de que la voz humana es única, y que cada persona tiene un patrón de frecuencias y características distintivas en su voz.

Para poder utilizar la biometría de voz se graba una muestra de la voz de una persona y se analiza para obtener un conjunto de características que se utilizan para identificar a ese sujeto. **Estas características pueden incluir el tono, el timbre, la entonación, la frecuencia o ritmo de la voz.**

Los sistemas de biometría de voz utilizan **algoritmos de aprendizaje automático y bases de datos de muestras de voz.** Estos algoritmos analizan y comparan las características de una voz conocida con las de una voz desconocida.

Si hay suficiente coincidencia entre las dos voces, el sistema puede determinar con una cierta confianza quién está hablando.

El adecuado entrenamiento de los modelos con suficientes muestras de voz durante el proceso de registro es crucial para obtener un **patrón o template biométrico vocal** de calidad.

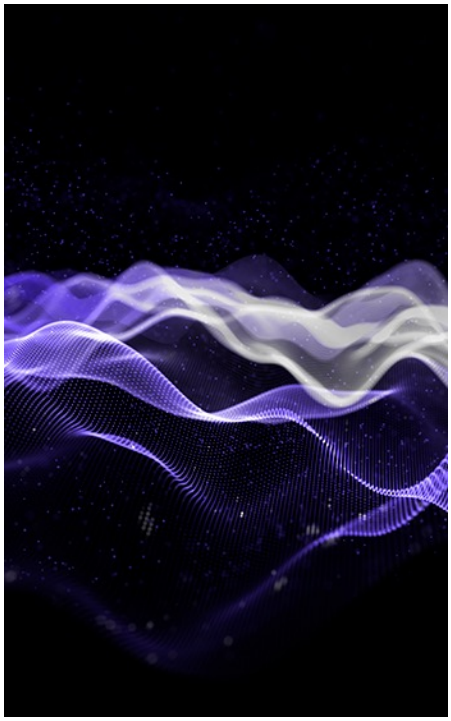
Este patrón debe servir de referencia para comparar con otras muestras o patrones para determinar si pertenecen a la misma persona.

Es posible que la precisión de la biometría de voz genere interrogantes debido a los cambios en la voz que pueda causar una enfermedad, la fatiga o el paso del tiempo. Sin embargo, gracias a la experiencia de nuestros ingenieros y la utilización de tecnología basada en aprendizaje profundo, se pueden superar estos desafíos e identificar la voz de un usuario en gran variedad de situaciones.

Entre las más comunes se encuentran **la verificación de la identidad de una persona en un sistema de seguridad, la autenticación de usuarios o la identificación en llamadas** telefónicas en call centers como en Santalucía

02.

¿Qué es el reconocimiento de voz?



El reconocimiento de voz es una tecnología que permite a una computadora o dispositivo electrónico identificar palabras habladas por una persona. Sus usos son diversos. Entre ellos, destacan la entrada de texto en dispositivos móviles, la transcripción automática de conferencias o reuniones, el control de dispositivos domésticos inteligentes o el acceso a servicios de información por teléfono. Su uso también aumenta en el campo de la asistencia virtual con el fin de que los usuarios interactúen con los sistemas de voz a través de comandos de voz.

El reconocimiento de voz se basa en la biometría de la voz, es decir, en la medida y el análisis de características únicas de la voz humana Reconocimiento y biometría de voz no son lo mismo.

Es cierto que utilizan tecnologías similares. Sin embargo, no comparten el mismo propósito: la biometría de voz se utiliza para distinguir a una persona de otra, centrándose en la verificación de la identidad de dicha persona, mientras que el reconocimiento de voz se emplea para facilitar la comunicación entre personas y dispositivos digitales.

03.

Diferencia entre biometría y reconocimiento de voz

La biometría de voz es el uso de las características únicas de la voz de una persona para identificarla de manera fiable. Se puede utilizar para autenticar a un usuario en un sistema, para proteger la privacidad de una persona al asegurar que solo ella puede acceder a cierta información o para realizar ciertas acciones.

El reconocimiento de voz, por contra, es el proceso de convertir el habla en texto para que pueda ser procesado por un ordenador o dispositivo digital. Es utilizado comúnmente en sistemas de asistentes virtuales, como **Google Assistant, Alexa o Siri**. Estos sistemas permiten a los usuarios realizar acciones y obtener información mediante el uso de comandos de voz.

Por lo tanto, la biometría de voz se utiliza para identificar a una persona, mientras que el reconocimiento de voz se utiliza para procesar el habla y convertirlo en texto que una computadora pueda entender.

04.

Ventajas de la biometría de voz

1

Robustez

La señal de voz puede considerarse casi estacionaria cuando se analiza en intervalos de tiempo reducidos. Esta circunstancia permite extraer características con alto poder discriminativo para diferenciar entre personas.

2

Bajo carácter intrusivo

A diferencia de otros métodos que requieren de una colaboración activa del individuo o el uso de hardware específico, para el análisis vocal basta con la captura de audio a través de un micrófono.

3

Disponibilidad

La grabación de un corte de voz es un método común de identificación de hablantes al que el usuario medio está acostumbrado. Además los sistemas biométricos que analizan esta característica son de fácil integración en muchas soluciones: call centers, asistentes de voz y dispositivos móviles.

4

Autenticación de voz segura

La voz es una característica biométrica única que puede ser utilizada para autenticar la identidad de una persona de manera segura.

5

Fácil de usar

El reconocimiento de voz es fácil de usar y no requiere de ningún tipo de dispositivo adicional. Basta con hablar en un micrófono para que el sistema pueda reconocer la voz.

6

Accesibilidad

Puede ser de gran ayuda para las personas con discapacidades que puedan tener dificultades para usar dispositivos táctiles o para escribir.

7

Comodidad

Permite a los usuarios realizar tareas sin tener que escribir o usar dispositivos táctiles, lo que puede ser más cómodo y menos cansado.

8

Eficiencia

Posibilita a los usuarios realizar tareas de manera más rápida y eficiente, ya que no es necesario escribir o usar dispositivos táctiles.

9

Precisión

La biometría de voz puede ser más precisa que el tecleo o el uso de dispositivos táctiles, lo que evita errores y aumentar la productividad.

05.

Evolución de la biometría de voz

La tecnología de biometría de voz ha evolucionado significativamente en las últimas décadas. Algunos hitos importantes en su evolución son:

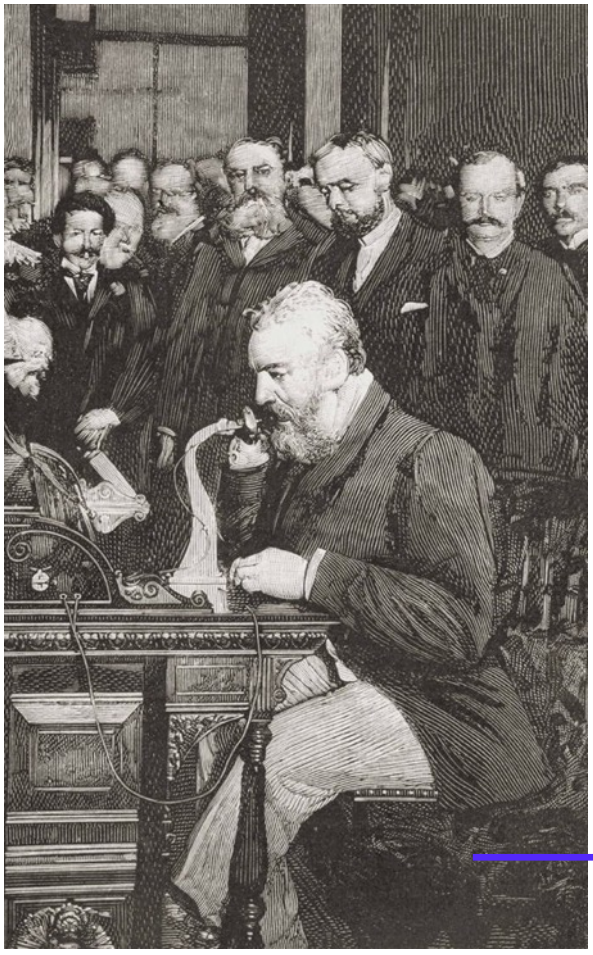
Década de 1970: se comienza a **investigar** la posibilidad de utilizar la voz como medio de autenticación, pero las limitaciones tecnológicas impiden el desarrollo de soluciones prácticas.

Década de 1980: se introducen los **primeros sistemas de reconocimiento de voz**, que utilizan técnicas de procesamiento de señales para identificar patrones en la voz del usuario. Estos sistemas son muy rudimentarios y tienen una tasa de error elevada.

Década de 1990: se producen importantes **avances en la tecnología**

de procesamiento de señales, lo que permite mejorar la precisión de los sistemas de reconocimiento de voz. Se comienzan a utilizar técnicas de aprendizaje automático para entrenar a los algoritmos de reconocimiento de voz.

Década de 2000: se desarrollan **sistemas de biometría de voz** que utilizan múltiples características de la voz, como la entonación, el ritmo y la velocidad, para mejorar la **precisión** del reconocimiento. También se comienzan a utilizar técnicas de análisis de emociones para detectar posibles fraudes.



Década de 2010: se desarrollan **sistemas de biometría de voz** que pueden funcionar en **tiempo real**. Esto hace que sean ideales para aplicaciones móviles y de seguridad en línea.

En la actualidad, la tecnología de biometría de voz sigue evolucionando, y se están explorando nuevas técnicas para mejorar su precisión y eficacia.

Por ejemplo, **se están investigando sistemas que puedan detectar enfermedades a través de la voz, como el Parkinson o la depresión**. Además, se espera que la tecnología de biometría de voz se integre con otros sistemas de autenticación. La integración y combinación con otras biometrías como la **huella dactilar o el reconocimiento facial** permitirá ofrecer soluciones de autenticación multimodal más robustas y seguras.

06.

Casos de uso Biometría de voz

La voz humana forma parte de nuestro día a día. Es un mecanismo para acceder a múltiples servicios, aplicaciones y dispositivos debido a su facilidad de uso. Algunos ejemplos de la utilización de la tecnología de voz son:

Verificación de la identidad

Muchos sistemas de seguridad, como los sistemas de inicio de sesión en dispositivos móviles o servicios en línea, utilizan la tecnología de voz para verificar la identidad de un usuario. Al escuchar la voz de un individuo, pueden compararla con una muestra de voz de referencia almacenada en una base de datos y determinar si la persona es la misma.

Seguridad en el transporte

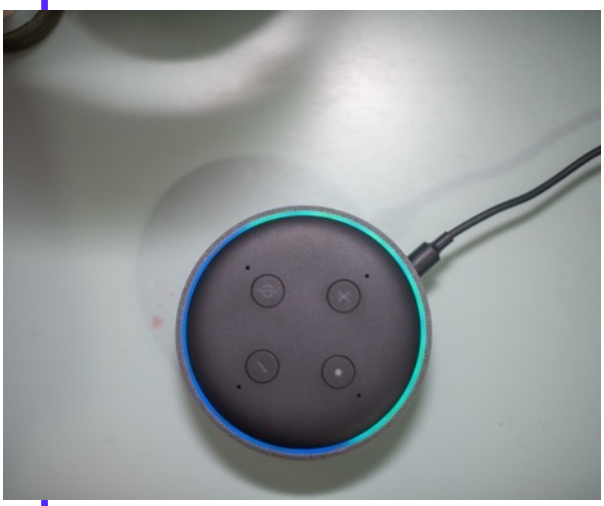
Algunos aeropuertos y compañías de transporte utilizan la biometría de voz para verificar la identidad de los pasajeros y trabajadores. Esto garantiza que sólo las personas autorizadas accedan a aviones, trenes o autobuses.

Análisis del estado emocional

La biometría de voz también se utiliza para evaluar el estado emocional de las personas. Por ejemplo, se puede utilizar para determinar si una persona está cansada, enfadada o feliz basándose en el tono y la entonación de su voz.

Transcricpión de dictado y control de dispositivos

Los sistemas de dictado y control de dispositivos a menudo utilizan el reconocimiento de voz para permitir a las personas dictar texto o controlar dispositivos mediante comandos de voz.



Asistencia personal

Los asistentes virtuales a menudo utilizan la biometría de voz para reconocer a sus usuarios y personalizar la experiencia de usuario. Por ejemplo, un asistente virtual puede utilizar la biometría de voz para adaptar su respuesta y acciones en consecuencia.

07.

La biometría de voz mejora la experiencia de Santalucía

Como hemos adelantado, la biometría de voz ofrece **altos niveles de seguridad** y mejora la experiencia de usuario al simplificar los procesos de interacción entre clientes y call centers.

El número de clientes comprometidos con su proveedor de servicios de protección, ahorro y asistencia familiar no superar el 19% según el **Índice STIGA de Experiencia de Clientes.**

Santalucía, empresa aseguradora española, consiguió superar ese índice gracias a la incorporación de biometría de voz en sus procesos de centro de llamadas. La compañía detectó que uno de los canales más utilizados por sus clientes era el teléfono.

Sin embargo, el proceso de atención al cliente por esa vía no estaba 100% optimizado ni totalmente ajustado a las necesidades de los asegurados.

Para optimizarlo, **introdujo la biometría de voz de Mobbeel en su servicio de call center.** Ahora sus **clientes pueden identificarse** mediante su voz cuando llaman al call center pronunciando una **frase fija** previamente registrada en el sistema: **"En Santalucía, mi voz es mi contraseña".**

Cuando el cliente llama, dice esa frase y **automáticamente la llamada** se **pasa a un agente** que no tiene que identificar al usuario. Nuestra solución mejora la relación con los clientes, protege a los consumidores de personas no autorizadas que quieren acceder a sus datos y acaba con la frustración de responder a preguntas de identificación.

08.

Funcionamiento de un sistema biométrico de voz

Un **sistema biométrico de voz completo debe permitir verificar la identidad de la persona** que se muestra ante él. Además debe asegurar que el proceso se lleva a cabo de **manera legítima**. En otras palabras, debe garantizar que no existen intentos de ataque para interferir en su correcto funcionamiento.

El estándar **ISO/IEC 30107-11** define una arquitectura que ha sido adoptada por Mobbeel, permitiendo aportar la máxima confianza a la hora de verificar de manera segura la identidad de los usuarios.

Para que un sistema biométrico de voz pueda funcionar necesita una serie de componentes clave como:

1. **Un micrófono**: para capturar la voz humana

2. **Un procesador de señales**: para convertir la señal de audio en una forma digital que pueda ser procesada por la computadora. La parte más crítica de esta etapa es el modelado vocal que da como resultado un vector de características de la muestra de voz.

3. **Una base de datos de muestras de voz**: para comparar la voz desconocida con las voces conocidas almacenadas en la base de datos.

4. **La toma de la decisión y una interfaz de usuario**: para permitir que el usuario interactúe con el sistema y proporcionar resultados tras la toma de decisión sobre la identidad del usuario o realizar acciones en consecuencia tras su identificación.

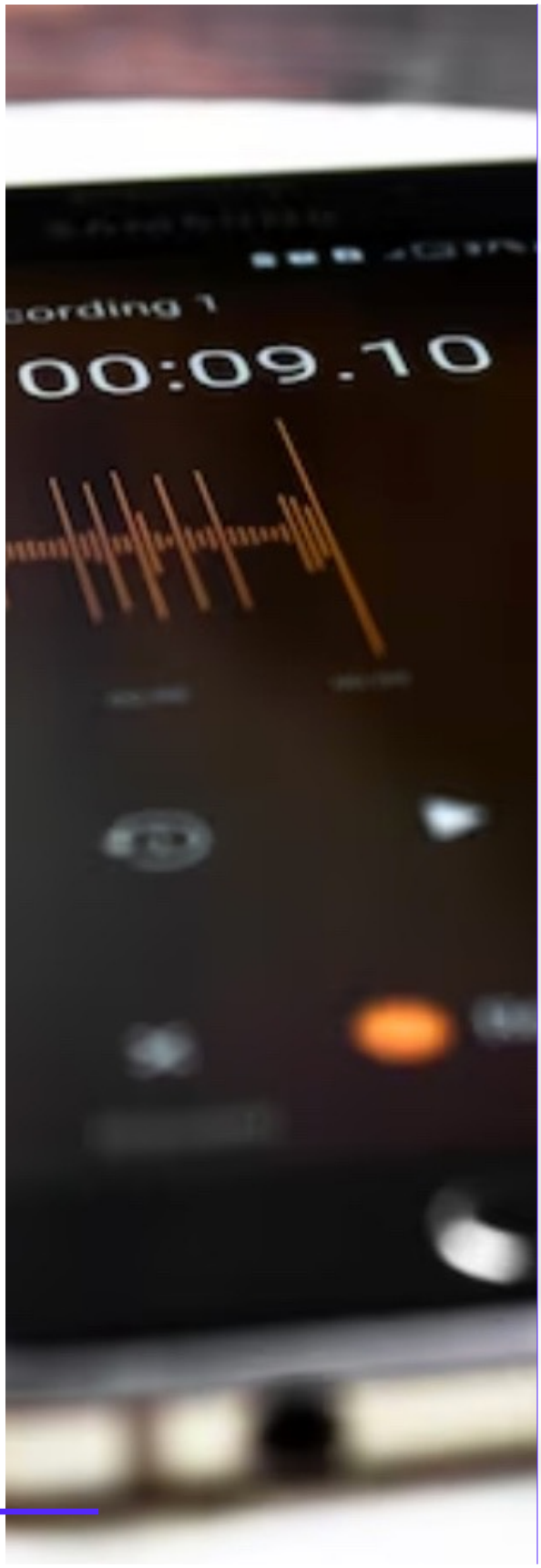
Cuando se habla en el micrófono de un sistema biométrico, la señal de audio es captada y convertida en una forma digital por el procesador de señales. Luego, el algoritmo de procesamiento de la señal compara el audio con las muestras de voz almacenadas en la base de datos. Si hay suficiente coincidencia entre la voz desconocida y alguna de las voces conocidas, el sistema puede determinar con una cierta confianza quién está hablando.

A. Sistema de captura

El primer paso dentro de un proceso de verificación biométrica de la identidad consiste en capturar la característica física o de comportamiento a analizar. En el caso de la voz, se procederá a grabar un corte de audio que contenga una frase pronunciada por el usuario.

El sistema desarrollado por Mobbeel ofrece gran versatilidad siendo capaz de operar independientemente del idioma y del tipo de frase (tanto fija como libre).

Esto permite implementar casos de uso en los que se pida al usuario pronunciar un texto fijo o simplemente reconocer su identidad de manera transparente y en tiempo real mientras mantiene una conversación.



Su diseño también permite la utilización **multicanal**. Soporta audios provenientes de **canal telefónico** (redes fijas, móviles e IP) así como de **alta calidad**. Los resultados en términos de prestaciones están relacionados con el canal utilizado, ya que algunos como la red telefónica convencional utilizan filtros que eliminan información de la señal con implicaciones en las tasas de precisión del sistema.

La tecnología incorpora como parte del módulo de captura una serie de algoritmos encargados de **evaluar la calidad de los audios** de entrada, determinando si cumplen con las condiciones mínimas para llevar a cabo las operaciones biométricas. Estos controles analizan tanto la calidad objetiva del audio (relación señal/ruido o **SNR**) como la presencia de un contenido mínimo de voz mediante la estimación de **regiones activas de voz (VAD).**

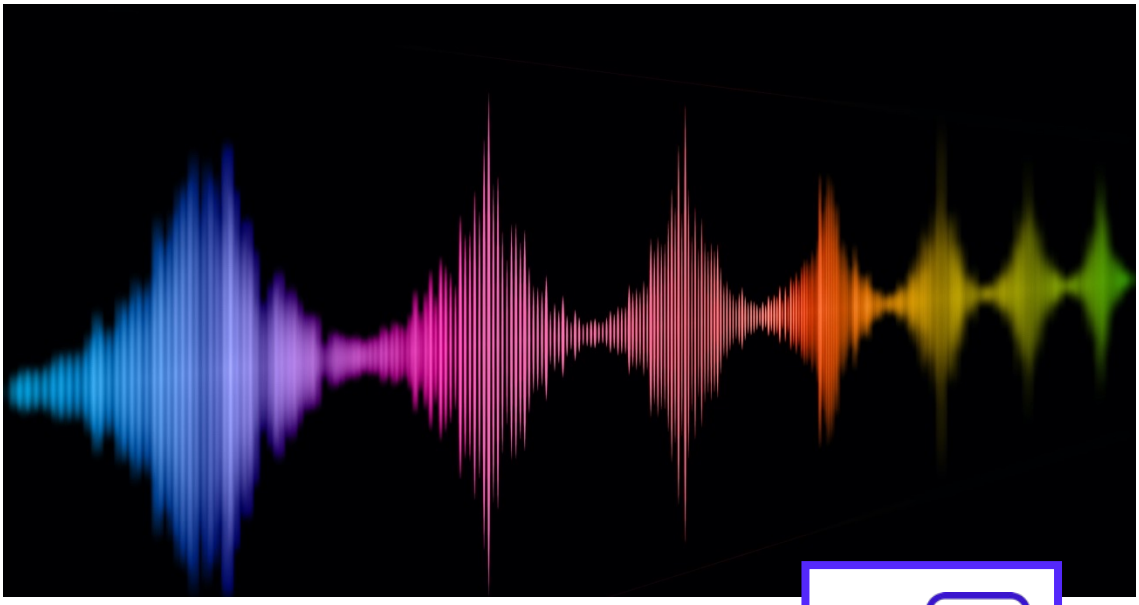
B. Detección de ataque de presentación

Según la ISO/IEC 30107, un ataque de presentación consiste en la **presentación premeditada al sistema de captura de un rasgo falseado** para interferir en el correcto funcionamiento del sistema biométrico. En los casos de uso habituales de la tecnología de Mobbeel, un ataque de suplantación puede darse en alguna de las siguientes situaciones.

- **Reproducción de una grabación con la voz de la persona a suplantar**. Este tipo de ataques se conocen como ataques de acceso físico (PA).

- **Reproducción de audios de voz generados de manera sintética**. Este tipo de ataques se conocen como ataques de acceso lógico (LA).

Cada uno de los elementos indicados anteriormente se define según el estándar **como instrumento de ataque de presentación (PAI)** y tendrán por tanto que ser reconocidos por el **sistema de detección de ataques de presentación (PAD).** Este módulo incluye una serie de medidas que analizan el audio de entrada para encontrar trazas de ataques físicos y lógicos, en ambos casos de manera transparente para el usuario, sin necesidad de colaboración activa por su parte.



C. Procesado de señal

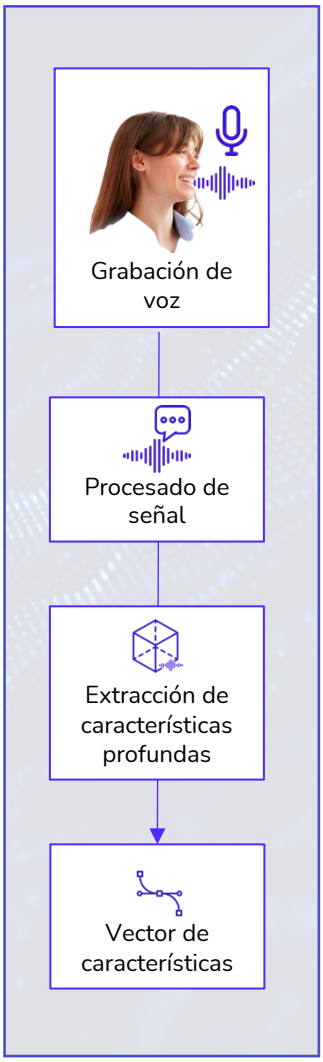
Una vez capturada la señal de voz y comprobado que no ha existido un intento de ataque de presentación es momento de continuar con el proceso de verificación de identidad. En la etapa genérica de procesado de señal tienen lugar todas **aquellas operaciones encaminadas a convertir la información de entrada en datos** que puedan ser utilizados **para** una posterior **comparación**.

El elemento central de esta etapa es el **modelado vocal**.

¿Qué es el modelado de vocal?

El modelado vocal es el proceso mediante el cual **una grabación de voz se transforma en un conjunto de valores numéricos conocido como vector de características**. Estos vectores modelan los rasgos más significativos de la voz, de manera que comparando varios de ellos será posible llevar a cabo operaciones de verificación de identidad.

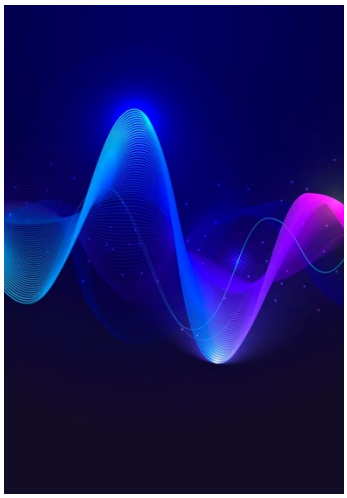
Proceso de generación de vectores

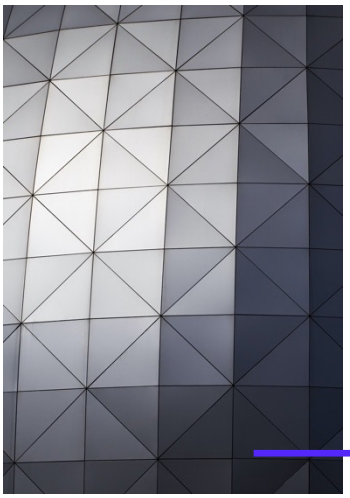


El proceso de generación de vectores de características vocales comienza con el preprocesado de la señal de audio. Estas señales contienen información sobre las ondas sonoras generadas por el tracto vocal de una persona. Los algoritmos de preprocesado dividen la señal de voz en pequeñas regiones sobre las que se calculan una serie de valores en el dominio de la frecuencia.

Una vez que la señal de audio se convierte en un conjunto de características de entrada, los algoritmos de aprendizaje automático comienzan a detectar patrones en ellos.

Las arquitecturas de aprendizaje profundo refinan los vectores obtenidos en la etapa de preprocesado y consiguen representaciones robustas de la biometría vocal de cada usuario. **Los vectores son irreversibles, por lo que no es posible volver al audio original.**



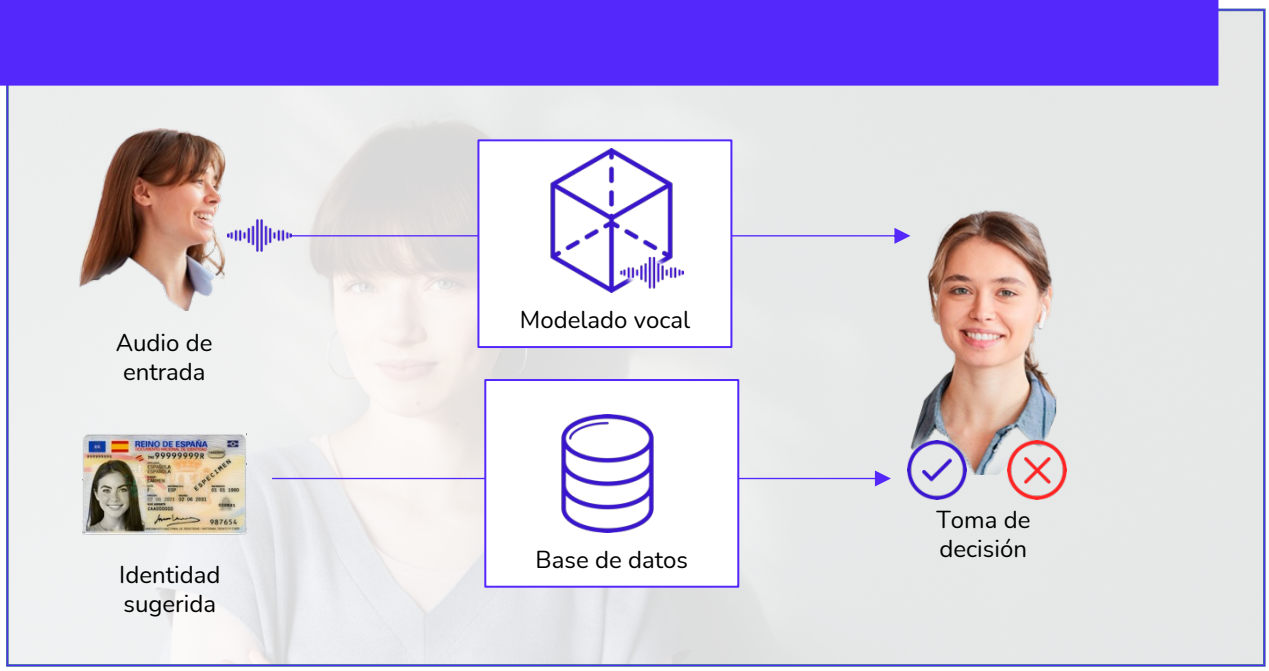


D. Comparación

A partir del vector de características obtenido en la etapa anterior es posible llevar a cabo diferentes operaciones biométricas para determinar la identidad del usuario. Cada operación biométrica busca responder a una pregunta específica, y por tanto la elección de una u otra dependerá de la aplicación concreta.

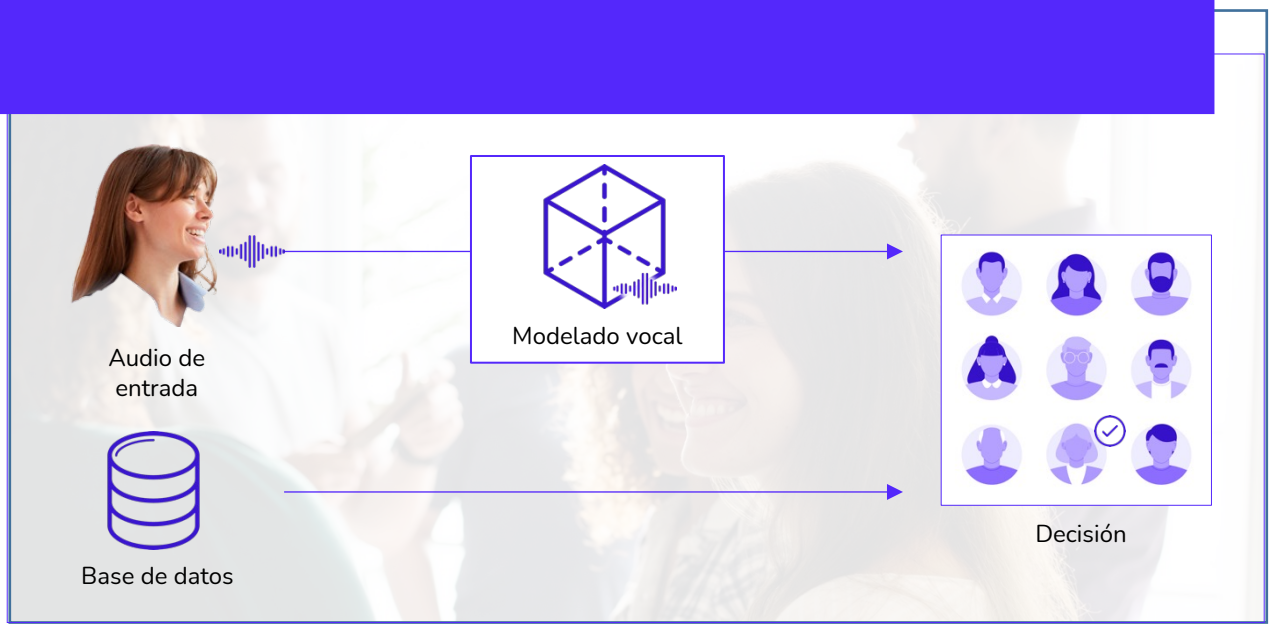
Verificación ¿soy yo?

Dado un audio de entrada y una etiqueta de identidad, el sistema deberá determinar **si la persona es quién dice ser** mediante el análisis del parecido entre el audio de entrada y otro vector de características almacenado previamente en el sistema. Esta operación requiere de un proceso de registro previo y se denomina **verificación 1:1 de biometría de voz.**



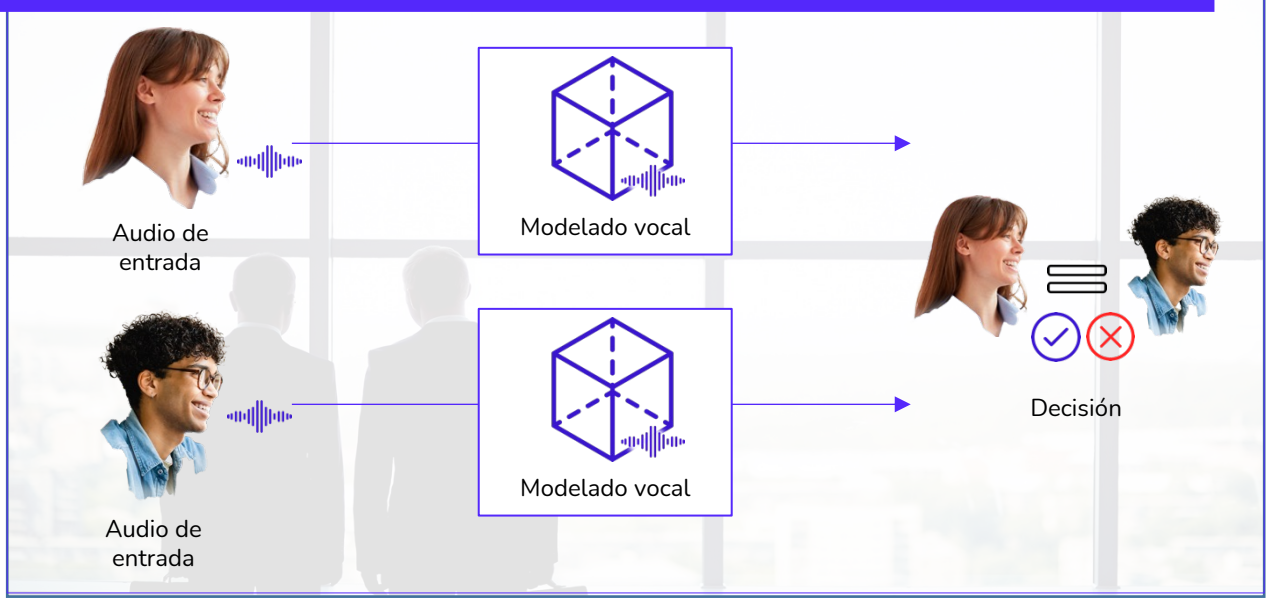
Identificación ¿Quién soy?

Dado un audio de entrada el sistema deberá **determinar la identidad** del usuario comparando la muestra de voz con una base de datos de muestras de voz de diferentes personas previamente registradas. A este tipo de identificación se le conoce como **identificación 1:N.**



Correspondencia: ¿Son la misma persona?

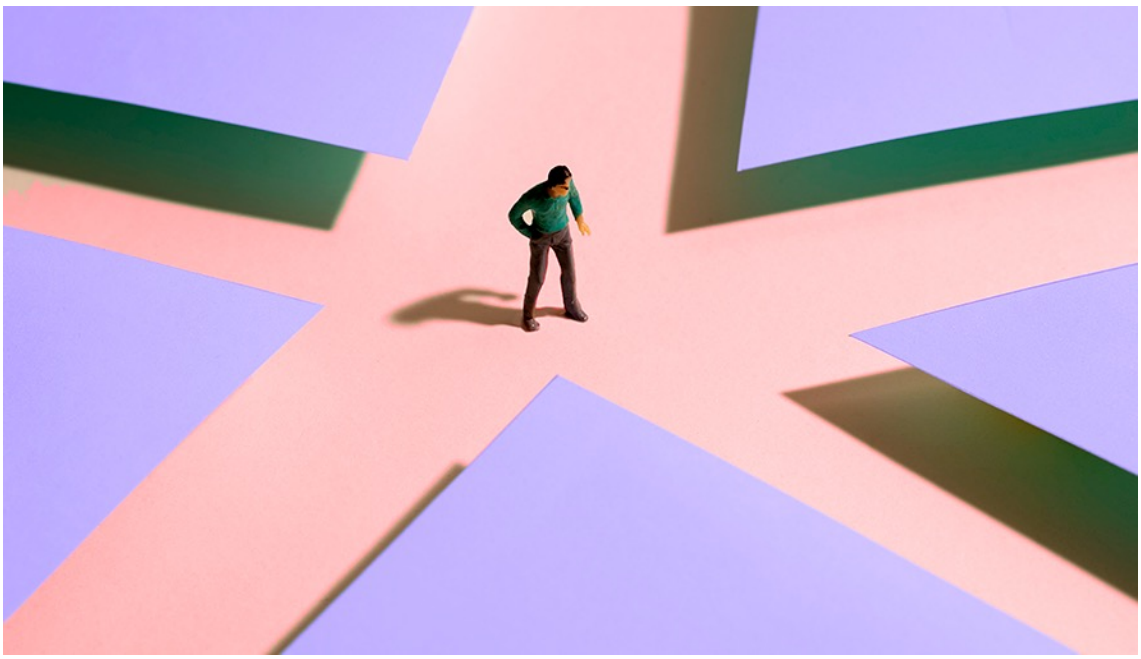
Dados dos audios de entrada el objetivo es **determinar el parecido** entre ambos.



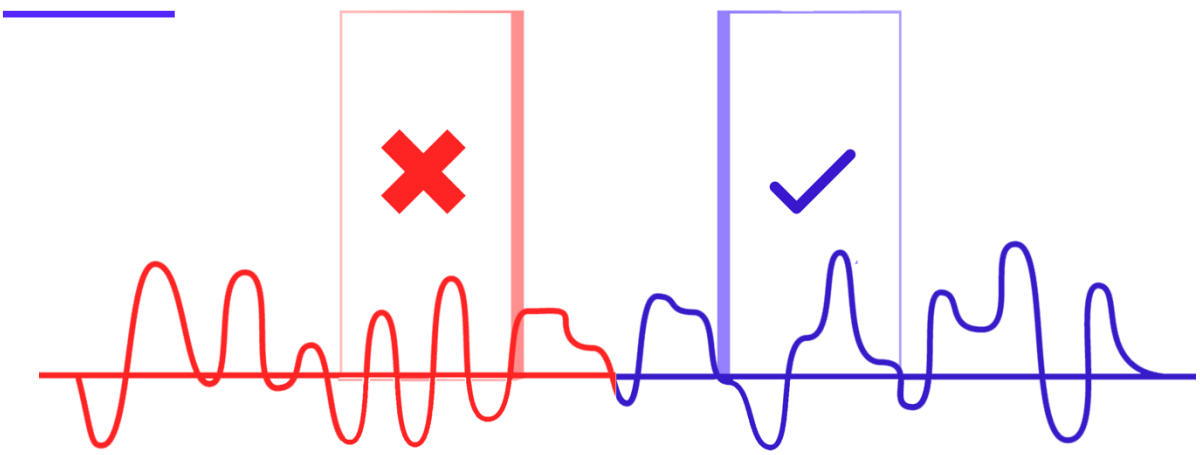
E. Toma de decisión

El flujo de trabajo de un sistema biométrico termina con la toma de decisión sobre la identidad del usuario. En cualquiera de las tres operaciones descritas anteriormente el proceso es el mismo: la tecnología calcula la distancia entre vectores de características y devuelve un valor numérico que se interpreta como el grado de parecido entre ambos.

Ese dato es por tanto la base de la decisión, pero en la mayoría de las ocasiones la información buscada debe expresarse en términos binarios: **es o no es la misma persona.**



Para ello es necesario establecer un **umbral de decisión**, es decir, marcar un valor numérico a partir del cual se determina que dos audios de voz corresponden a la misma persona.

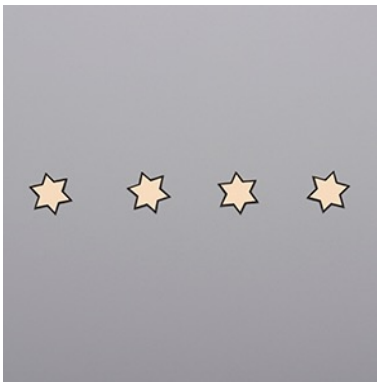


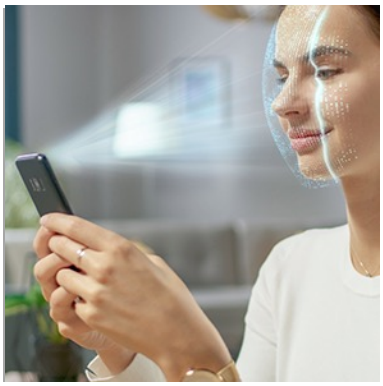
Para ello es necesario establecer un umbral de decisión, es decir, marcar un valor numérico **a partir del cual se determina que dos audios de voz corresponden a la misma persona.**

Elegir el umbral de decisión más conveniente es una tarea fundamental ya que tiene consecuencias en el funcionamiento del sistema. Valores demasiado estrictos pueden hacer que se rechace a un número alto de usuarios legítimos (problemas de usabilidad o accesibilidad), mientras que otros demasiado laxos pueden dejar pasar a demasiados impostores (problemas de seguridad). La elección final deberá considerar fundamentalmente los requisitos de seguridad de la aplicación donde se integre el módulo de biometría.

09.

¿Cómo mejorar el funcionamiento del sistema biométrico?





Utilizar una muestra de voz de calidad

Para minimizar el riesgo de suplantación de identidad, es importante utilizar una muestra de voz de alta calidad al registrar la identidad de una persona. Esto significa que la muestra debe ser clara y nítida, y no debe tener ruido de fondo o distorsión. Tal y como ya hemos comentado, nuestra tecnología incorpora como parte del módulo de captura algoritmos que evalúan la calidad de los audios.

Actualizar regularmente las muestras de voz

Es conveniente actualizar regularmente las muestras de voz para reflejar cualquier cambio en la voz de una persona. Por ejemplo, si una persona ha tenido una enfermedad o ha experimentado un cambio significativo en su voz debido al estrés o al envejecimiento, habría que actualizar su muestra de voz para asegurar que el sistema de reconocimiento de voz puede reconocerla con precisión.

Usar múltiples factores de autenticación

A veces, cuando se trata de ofrecer una mayor seguridad en procesos críticos, se pueden utilizar varios factores de autenticación para verificar la identidad de una persona. Esto puede incluir contraseñas, preguntas de seguridad o autenticación de dos factores, que pueden ayudar a evitar ataques de presentación y suplantación de identidad.

10.

Sesgos de la biometría de voz

Al igual que cualquier otra tecnología, la biometría de voz puede presentar sesgos. Algunos de los sesgos más comunes que pueden afectar la precisión de este tipo de biometría son:

- **Bases de datos**: el sesgo más importante parte de la base de datos con la que se ha entrenado nuestro modelo, donde nos podemos encontrar bases de datos poco equilibradas en cuanto género, idiomas o razas. Por ello, es fundamental entrenar a los modelos de inteligencia artificial con bases de datos de audios lo más heterogéneas posibles.
- **El acento:** la tecnología puede ser menos precisa para personas que hablan con acento, ya que el sistema puede tener dificultades para reconocer palabras o frases que no se corresponden con el idioma o el acento esperado.
- **La pronunciación**: el sistema puede ser menos preciso para personas que tienen problemas de pronunciación o que hablan de manera poco clara.
- **La falta de datos**: Si el sistema no tiene suficientes muestras de voz de una determinada persona o grupo de personas, puede tener dificultades para reconocer con precisión sus voces.

Hay que tener en cuenta que dependiendo del proveedor y de cómo haya entrenado sus modelos, pueden aparecer distintos sesgos. **En Mobbeel trabajamos constantemente para minimizarlos y mejorar la precisión de la tecnología.**

Transparencia

Es fundamental ser transparente sobre cómo se está utilizando la tecnología para la **autenticación de voz** y cómo se están recopilando y utilizando los datos de voz. Las personas han de ser conscientes del uso que se está haciendo con su biometría y deberían tener la opción de optar por no utilizarla si no están cómodos con ello, con lo que se debería ofrecer un método alternativo de autenticación.

A.

Resposabilidad

Los desarrolladores y usuarios deben ser responsables de cómo se utiliza la tecnología y de sus posibles consecuencias, tomando medidas para minimizar cualquier posible daño o perjuicio.

B.

11. Ética de la tecnología de biometría de voz

Privacidad

la privacidad de las personas debe ser respetada en todo momento. Los audios de voz o las plantillas biométricas se han de proteger y no deben compartirse sin el consentimiento explícito de las personas. **En Mobbeel cumplimos de manera estricta con el RGPD.**

C.

Equidad

Es vital asegurarse de que la tecnología no excluye o discrimina a ciertos grupos de personas evitando en la medida de lo posible sesgos. Por ejemplo, si la tecnología es menos precisa para personas con acentos o voces poco comunes, o para personas de un determinado sexo, habría que trabajar para mejorar la precisión para estos grupos.

D.

12.

Regulación y normativas que afecta al uso de las tecnologías de voz

Existen diversas normativas y regulaciones que rigen la utilización de las tecnologías biométricas en diferentes jurisdicciones, atendiendo a la protección de datos, privacidad y seguridad:

- **Ley de Protección de Datos Personales:** en muchos países, existen leyes que regulan la recopilación, el almacenamiento y el uso de datos personales, incluyendo datos de voz. Estas leyes establecen los derechos de las personas en cuanto a sus datos personales y establecen las obligaciones de las empresas y los gobiernos al recopilar y utilizar estos datos.
- **Normativas de protección de la privacidad:** muchos países tienen normativas específicas que protegen la privacidad de las personas y regulan cómo se pueden utilizar y compartir los datos de voz. Estas normativas pueden incluir requisitos de consentimiento explícito para la recopilación y el uso de datos de voz, así como requisitos para proteger la seguridad y la confidencialidad de estos datos.
- **Normativas de seguridad:** algunas normativas establecen requisitos de seguridad para proteger los datos de voz y minimizar el riesgo de ataques de presentación y suplantación de identidad. Estos requisitos pueden incluir medidas de seguridad como contraseñas y autenticación de dos factores para proteger el acceso a los datos de voz.

Hay que tener en cuenta que las regulaciones pueden variar según el país o la jurisdicción, por lo que es conveniente asegurarse de cumplir con las normativas y regulaciones específicas aplicables en cada mercado.

13.

¿Cómo evolucionará la tecnología de biometria de voz?

Se espera que la tecnología de voz continúe evolucionando y mejorando en los próximos años. Algunas de las tendencias y aplicaciones futuras que se pueden esperar son:

A.

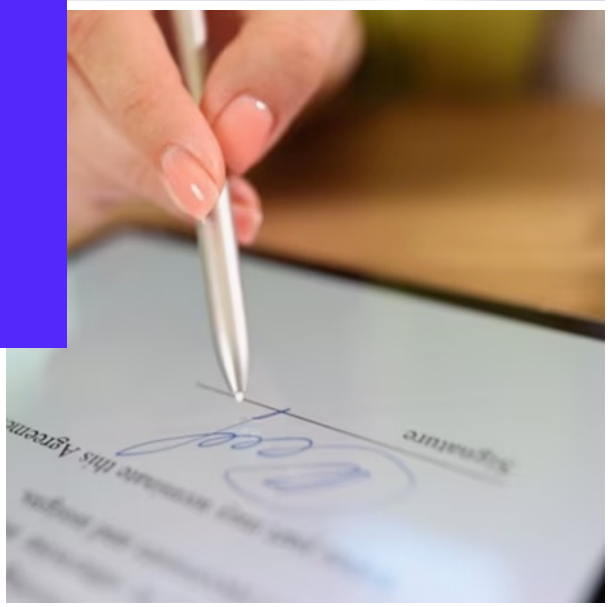
Mejoras en la precisión y la capacidad de adaptación

Se espera que la precisión mejore gracias a la utilización de modelos de deep learning más avanzados y a la mayor cantidad de datos disponibles para el entrenamiento de los modelos. A su vez, se espera que la tecnología sea capaz de adaptarse mejor a las diferencias individuales en la voz y al entorno de uso.

B.

Integración con otros sistemas de autenticación

La biometría de voz se integre con otros sistemas de autenticación, como la biometría de huellas dactilares y el reconocimiento facial, para ofrecer soluciones de autenticación multimodal más seguras y robustas.



C.

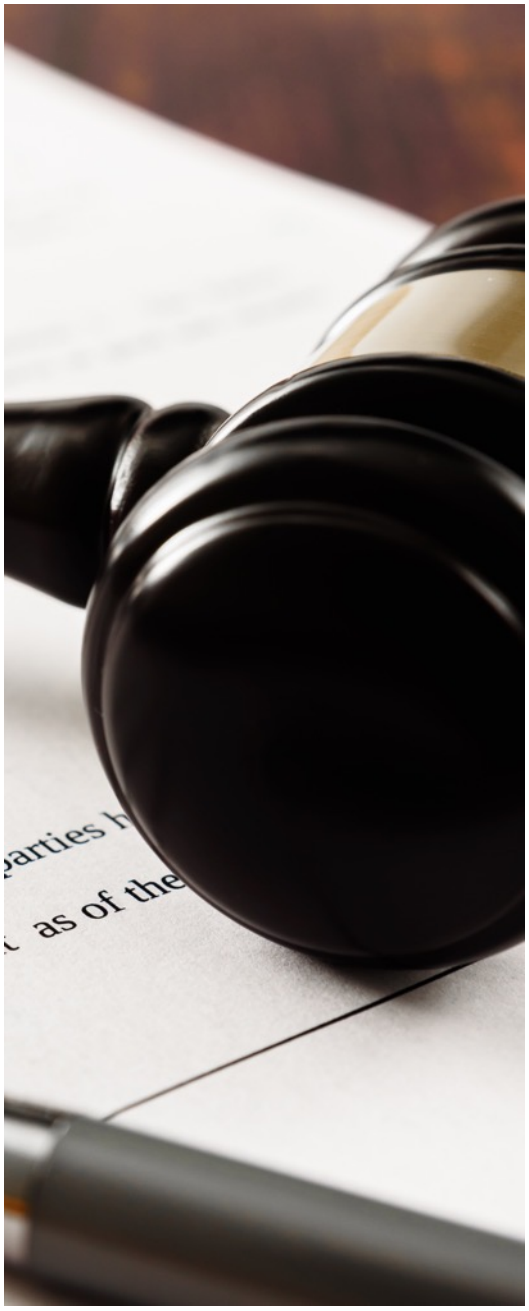
Mayor adopción en el mercado

Su uso aumentará a medida que se vuelva una tecnología más precisa y se desarrollen más aplicaciones para su uso. Esto podría incluir el uso de la biometría de voz en servicios financieros, servicios gubernamentales y servicios de atención médica, entre otros.

D.

Enfoque en la detección de emociones y enfermedades

Este tipo de biometría encontrará nuevas aplicaciones relacionadas con la detección de emociones y enfermedades, como la depresión, la ansiedad y el Parkinson. Esto podría permitir una detección más temprana de estas condiciones y un tratamiento más eficaz.



E.

Mayor atención a la privacidad y la seguridad

Se espera que se desarrollen nuevas medidas de seguridad para proteger los datos biométricos de los usuarios y que se establezcan marcos regulatorios para garantizar el uso responsable de esta la tecnología.

C/ Santa Cristina 2, 10195, Cáceres, España
+34 927 209 242
info@mobbeel.com