WHITEPAPER

EL IMPORTANTE PAPEL DE LA DETECCIÓN DE VIDA EN LA AUTENTICACIÓN BIOMÉTRICA FACIAL

Y CÓMO ELEGIR LA OPCIÓN CORRECTA PARA SU CASO DE USO

IDR&D

Para que la biometría facial pueda realmente ser adoptada por la mayoría como el mejor modo de autenticación, es esencial distinguir entre un rostro vivo genuino y un intento de falsificar el sistema con la representación artificial de un rostro. La detección automatizada de ataques de presentación, y en particular la detección de vida, se ha convertido en un componente necesario de cualquier sistema de autenticación que se base en tecnología biométrica facial en la que un ser humano no supervisa el intento de autenticación.

En el presente documento se discute la necesidad de una tecnología de detección de vida, su funcionamiento y sus enfoques.

INTRODUCCIÓN

La biometría facial está siendo rápidamente aceptada tanto entre los consumidores como entre las empresas como un método conveniente y seguro de verificación de la identidad. La tecnología cierra las brechas de seguridad que a menudo se explotan en soluciones que se basan en algo que puede perderse o robarse, como una contraseña o la respuesta a una pregunta "secreta", así como nuevos hackeos como el fraude de la tarjeta SIM. El simple hecho de mostrar el rostro en una selfie también es mucho menos frustrante para los usuarios.

La tecnología de reconocimiento facial ha avanzado espectacularmente en los últimos años gracias a los avances en la inteligencia artificial, la amplia disponibilidad de cámaras de alta calidad, pero baratas, y la posterior creación de una enorme cantidad de datos disponibles públicamente para entrenar algoritmos de reconocimiento facial. Las continuas mejoras en la potencia de cálculo, incluyendo las unidades de procesamiento gráfico (GPU) y su disponibilidad, han hecho posible aplicar a estos sistemas sofisticados algoritmos de machine learning como las Redes Neurales Convolucionales y Redes Neurales Profundas y ejecutarlos en dispositivos cotidianos. Además de ser altamente precisos, los algoritmos actuales son lo suficientemente rápidos como para ser implementados en grandes sistemas de autenticación comercial, incluso en aquellos con varios millones de usuarios.

OFRECIENDO LA CAPACIDAD DE FORTALECER LA SEGURIDAD Y MEJORAR LA EXPERIENCIA DEL USUARIO, LA BIOMETRÍA FACIAL HA SIDO APLICADA EN CASOS DE USO COMO EL DESBLOQUEO DE DISPOSITIVOS MÓVILES, LA SEGURIDAD DE TRANSACCIONES FINANCIERAS Y REGISTROS DE SALUD Y LA MEJORA EN LOS PROCESOS DE INCORPORACIÓN DIGITAL.

Las aplicaciones en la vida real de la biometría facial para la autenticación plantean la cuestión de la seguridad. Si un posible estafador puede acceder fácilmente a la representación del rostro de una persona y presentarla como propia, ¿es posible confiar en ese método de autenticación?

Para que la biometría facial pueda realmente ser adoptada por la mayoría como el mejor modo de autenticación, es esencial distinguir entre un rostro vivo genuino (de buena fe) y un intento de falsificar el sistema con la representación artificial de un rostro. Por lo tanto, la detección automatizada de ataques de presentación, y en particular la detección de vida, se ha convertido en un componente necesario de cualquier sistema de autenticación que se base en tecnología biométrica facial en la que un ser humano no supervisa el intento de autenticación.

También aborda el temor de que nuestros datos biométricos puedan verse comprometidos, y a diferencia de una contraseña, nuestra biometría no puede ser "restablecida." Las plantillas biométricas codificadas por naturaleza tienen poca o ninguna utilidad si son robadas, y la mejor práctica es almacenar estas plantillas por separado de cualquier Información de Identificación Personal (PII). Pero la realidad es que nuestros datos biométricos ya están ahí para ser tomados. Incluso si no tiene un perfil en Facebook ni publica alguna foto suya, lo más probable es que aún pueda encontrar su imagen online. Esta es otra razón por la que la detección de vida es fundamental. Al integrar la detección de vida con el reconocimiento facial, podemos hacer que nuestra biometría sea inútil para los impostores.

EN ESTE ARTÍCULO EXPLORAMOS LA IMPORTANCIA DE ESTA TECNOLOGÍA AL IMPLEMENTAR LA BIOMETRÍA FACIAL PARA LA AUTENTICACIÓN, INCLUYENDO LAS MEJORES PRÁCTICAS Y CASOS DE USO ESPECÍFICOS.

CÓMO LA TECNOLOGÍA DE DETECCIÓN DE VIDA PERMITE UNA AUTENTICACIÓN BIOMÉTRICA FACIAL DE CONFIANZA

Cuando se trata de utilizar la biometría facial para la autenticación, la precisión y el desempeño ya no son una preocupación. Sin embargo, la amenaza de falsificación de identidades ha evolucionado de artículos teóricos y experimentos de laboratorio a ataques en la vida real que afectan a las empresas, los clientes y su dinero. Detectar las falsificaciones es esencial para que la coincidencia biométrica facial sea confiable.

Mientras que el reconocimiento facial para la autenticación puede responder con precisión a la pregunta, "¿Es esta la persona correcta?", no responde a la pregunta, "¿Es esta una persona viva?" Este es el papel de la detección de vida.

LA AUTENTICACIÓN BIOMÉTRICA INTEGRAL DEBE RESPONDER A DOS PREGUNTAS:

1. ¿ES ESTA LA PERSONA CORRECTA? **(COINCIDENCIA BIOMÉTRICA)**

2. ¿ES ESTA UNA PERSONA VIVA? **(DETECCIÓN DE VIDA)**

EXPLICACIÓN SOBRE LA DETECCIÓN DE VIDA

El reconocimiento facial funciona comparando las características mapeadas de un usuario inscrito, como la distancia entre sus ojos o la longitud de la línea de la mandíbula, con una plantilla biométrica para verificar su identidad. Examina la imagen que ve y realiza mediciones. Lo que no hace es reconocer la presencia física de un usuario frente a una impresión de calidad o a una representación digital. ***¡Una fotografía o imagen en una pantalla funciona tan bien como la persona real!***

Cuando se utiliza la biometría facial para la autenticación, un intruso es capaz de explorar esa limitación para engañar al sistema y hacerle creer que ve al usuario autorizado. A esto le llamamos un ataque de presentación y estos ataques se han vuelto más fáciles para los estafadores debido al fácil acceso online a fotos de alta definición, imágenes de pantalla, máscaras y videos que pueden ser utilizados para falsificar un sistema de reconocimiento facial.

La detección de vida trabaja con un sistema biométrico para medir y analizar las características físicas y las reacciones con el fin de determinar si se está capturando la muestra biométrica de un sujeto vivo que está presente en el punto de captura. La tecnología no realiza ninguna función de comparación, sino que detecta ataques de presentación. Entre ellos se incluyen:

ATAQUE A FOTOS O VIDEOS

Los estafadores obtienen acceso a una foto o video de los usuarios autorizados. Esto puede ser tan fácil como realizar una simple búsqueda en Google o visitar la cuenta de redes sociales de un individuo. El estafador puede utilizar la imagen impresa para crear una máscara 2D.

VIDEO SINTÉTICO O DEEPFAKE

Los estafadores toman una foto o un video y, mediante la edición con un software de animación, crean una versión realista del individuo hablando y asintiendo con la cabeza.

MODELO O MÁSCARA 3D

Los estafadores invierten en máscaras tridimensionales o modelos personalizados que imitan la semejanza física de un individuo.

ENFOQUES PARA LA DETECCIÓN DE VIDA - PASIVA VS. ACTIVA

Existen una variedad de enfoques para detectar la vida. A un alto nivel, estas pueden clasificarse como activas o pasivas:

La detección de vida activa **requiere que los usuarios participen en una verificación respondiendo a un desafío. Entre los ejemplos de sistemas implementados hoy en día se encuentran los siguientes:**

- **Asentir o girar la cabeza de lado a lado**
- **Parpadear**
- **Seguir un punto en una pantalla**
- **Sonreír**
- **Hablar una serie de palabras o números**
- **Mover la cámara hacia la cara o inclinarse hacia la cámara**
- **Grabar un breve video**

La detección de vida pasiva **no requiere ninguna acción por parte del usuario. La detección de vida se produce cuando el usuario se toma una selfie. Existen varias técnicas posibles para la vida pasiva, que van desde el análisis de una imagen de selfie hasta la captura de un video y la proyección de diferentes luces sobre el sujeto. Cada enfoque de la vida pasiva tiene un impacto diferente en la experiencia del usuario y en los requisitos de procesamiento.**

PASIVA O ACTIVA: ¿CUÁL ES LA MEJOR?

Para comprender el tipo correcto de vida, la siguiente sección examina la vida activa en comparación con la vida pasiva, seguida de una explicación de los diferentes tipos de vida pasiva.

	DETECCION DE VIDA PASIVA	DETECCION DE VIDA ACTIVA
EXPERIENCIA DEL USUARIO	No requiere ninguna acción por parte del usuario, lo que se traduce en un menor abandono y, por lo general, en menos tiempo y esfuerzo.	Requiere que los usuarios respondan a "desafíos" que añaden tiempo y esfuerzo al proceso, y que son poco prácticos para casos de uso con frecuente coincidencia biométrica facial, como el inicio de sesión. Las empresas informan de tasas de abandono de hasta el 50% en el caso de vida activa.
REQUISITOS DE SOFTWARE	Algunos métodos requieren la instalación previa de un componente de software en un dispositivo; otros no.	Por lo general, se requiere la instalación de un software en el dispositivo, un problema para casos de uso como la incorporación remota de nuevos clientes antes de descargar una aplicación móvil nativa.
ANÁLISIS DE IMÁGENES	Esto varía dependiendo del enfoque. Puede basarse en una sola imagen con procesamiento casi en tiempo real.	Requiere el análisis de múltiples fotogramas de video para detectar el movimiento solicitado.
REQUISITOS DE ANCHO DE BANDA	Bajo en función del uso de una sola imagen o análisis. Puede utilizar la misma imagen tomada para reconocimiento facial, lo que resulta en que no haya tráfico incremental hacia el servidor.	Puede requerir que se intercambien más datos entre el dispositivo del usuario y la solución basada en el servidor, lo que suele ser un problema en áreas con velocidades de Internet lentas.
VELOCIDAD	La velocidad con la que se realiza una verificación de vida pasiva varía dependiendo del método.	La vida activa siempre aumenta el esfuerzo del usuario, lo que resulta en una verificación más larga.
ROBUSTEZ ANTE LA FALSIFICACIÓN	Los métodos pasivos suelen ser más inmunes a la falsificación, ya que ofrecen "seguridad a través de la oscuridad" por lo que el estafador no tiene pistas sobre cómo engañar la verificación de vida.	Los sistemas activos proporcionan a estos estafadores información sobre cómo atacar y derrotar dicha verificación. Casi todos aplican técnicas conocidas para atacar, como el uso de una simple máscara 2D con ojos recortados y un software de animación que imita los movimientos de la cabeza, la sonrisa y el parpadeo.
CUMPLE CON LA NORMA ISO 30107-3 **DE ROBUSTEZ**	Dos soluciones cumplen con esta norma	Dos soluciones están certificadas como conformes

Desde casi todos los puntos de vista, es preferible una solución pasiva con una robustez comprobada y mensurable a una solución activa. ¿Por qué dar pistas a los estafadores, por qué sufrir de abandono y por qué obligar a un usuario a pasar más tiempo y esfuerzo cuando una solución pasiva ofrece seguridad y una experiencia simplificada?

PASIVA VS. PASIVA: ¿CUÁL ES LA DIFERENCIA?

No todas las soluciones pasivas son las mismas. A continuación se presentan cuatro variaciones conocidas:

- **Brilla con diferentes luces sobre la persona para crear diferentes exposiciones y garantizar que se trate de un rostro vivo**
- **Captura videos cortos que detectan micro-movimientos**
- **Examina la misma imagen de selfie que la imagen utilizada en la comparación facial**
- **Enfoque asistido por hardware (por ejemplo, medición de profundidad)**

ENFOQUE PASIVO	PROS	CONTRAS
BRILLAN LUCES VARIADAS	• Pasivo porque el usuario no necesita moverse	• El usuario debe mantener el dispositivo firme • El proceso requiere cierto período de tiempo • El enfoque falla en locales externos con luz solar brillante • Los usuarios pueden admitir que el parpadeo de luz es molesto
CAPTURA DE UN VIDEO CORTO	• Pasivo porque el usuario no necesita moverse	• El video tarda en capturarse • El video puede requerir la descarga previa de un software al dispositivo o el envío de grandes cantidades de datos a un servidor • La observación pasiva se basa en micro-imágenes y pequeños movimientos, que pueden ser difíciles de capturar
EXAMINA UNA SOLA IMAGEN DE SELFIE	• No requiere absolutamente ningún esfuerzo adicional • Tamaño mínimo de datos porque solo se necesita una imagen, no una transmisión de video • Rápida velocidad de procesamiento	• Requiere un componente del lado del servidor
ENFOQUE ASISTIDO POR HARDWARE (POR EJEMPLO, MEDICIÓN DE PROFUNDIDAD)	• No requiere absolutamente ningún esfuerzo adicional • El tamaño de los datos es aceptable porque solo se requieren unas pocas imágenes • Rápida velocidad de procesamiento	• Requiere un hardware costoso y específico del lado del cliente (por ejemplo una cámara con sensor de infrarrojos y/o de profundidad) • Requiere un componente del lado del servidor • Utiliza más potencia de CPU para el procesamiento

¿CUÁL ES EL MEJOR ENFOQUE?

La detección de vida pasiva es claramente la preferida ante la activa. El enfoque cierra las brechas de seguridad en la biometría facial sin añadirle fricción al proceso de autenticación y no requiere que los usuarios reciban capacitación sobre el mismo.

De los posibles enfoques pasivos, es preferible una sola imagen de selfie a las demás opciones.
Sin embargo, en cualquier caso, elija un enfoque pasivo que también cumpla con la norma ISO 30107-3.

CASOS DE USO PARA LA DETECCIÓN DE VIDA

La detección de vida facial combinada con la biometría facial proporciona una potente verificación y autenticación de la identidad cada vez que una aplicación necesite verificar la identidad de una persona sin que un humano de confianza supervise el proceso de coincidencia facial. Los casos de uso incluyen:

INCORPORACIÓN DIGITAL PARA NUEVOS CLIENTES Y CUENTAS

Permitir que nuevos clientes se registren en una cuenta de forma remota en un dispositivo móvil o una computadora en lugar de ir a un local físico aumenta en gran medida la oportunidad de que las empresas adquieran clientes. Un paso importante es "la verificación de la identidad." La verificación de la identidad es el proceso de comprobar la identidad de una persona antes de configurar una cuenta. Normalmente requiere que una persona tome una foto de un documento de identificación válido, como un pasaporte, se tome una selfie y luego envíe los dos elementos a un sistema que compruebe la validez del documento y haga coincidir el documento de identificación con la imagen de la selfie. La tecnología de detección de vida es fundamental para garantizar que la persona en la selfie es real y no una identidad fabricada. En la actualidad, las entidades gubernamentales en la mayor parte del mundo regulan la verificación de la identidad como algo necesario para el proceso "Conozca a su cliente" (KYC).

PROTECCIÓN DEL CLIENTE DIGITAL

Cada vez que un canal digital, como una aplicación móvil, un chatbot o un asistente virtual, utiliza la biometría facial para autenticar a un usuario, es fundamental verificar la detección de vida. La vida pasiva es fundamental para eliminar inconvenientes en la experiencia del usuario de modo que la autenticación sea rápida, sencilla y segura.

AUTENTICACIÓN MULTIFACTORIAL Y "ESCALONADA" DE LOS PAGOS

Los pagos se realizan habitualmente fuera de los locales comerciales, y esta tendencia aumentará para permitir condiciones crediticias más fáciles y menos inconvenientes en el proceso de compra. El riesgo de fraude aumenta a su vez. El reconocimiento facial con vida pasiva proporciona el segundo o tercer factor perfecto para transacciones de pago de mayor riesgo, apuntalando las vulnerabilidades que pueden ocurrir a través de la falsificación de SMS, los intercambios de tarjetas SIM, la falsificación y otros ataques de fraude que comprometen la posesión del dispositivo móvil como un factor.

ACCESO SIN TARJETA

Los quioscos de autoservicio, las terminales, los cajeros automáticos y los sistemas de entrada suelen depender de tarjetas o tokens, a veces combinados con códigos PIN, como medio para acceder a un sistema. Estos sistemas se ven fácilmente comprometidos por el robo de la tarjeta y el conocimiento del código PIN. Un factor adicional es el reconocimiento facial, pero debido a que no hay ningún humano de confianza para supervisar, la detección de vida es fundamental. La detección de vida pasiva proporciona una solución superior, ya que un estafador no tiene idea de que se está llevando a cabo la verificación. Y los usuarios ya no necesitan llevar fichas o tarjetas. Un rostro, una verificación de vida y, opcionalmente, un PIN es todo lo que se necesita para la autenticación.

¿CUÁL ES SOLUCIÓN DE DETECCIÓN DE VIDA ADECUADA PARA USTED?

Ya hemos abordado las diferencias entre la detección de vida facial pasiva y activa y por qué el equipo de ID R&D cree que una solución pasiva es superior por razones que incluyen la capacidad de ofrecer seguridad y una mejor experiencia al usuario. A continuación se presenta un resumen de las consideraciones a la hora de evaluar las tecnologías::

SIMPLICIDAD

Ya hemos abordado las diferencias entre la detección de vida facial pasiva y activa y por qué el equipo de ID R&D cree que una solución pasiva es superior para equilibrar el desempeño y la experiencia del usuario. Encontrar una solución que proporcione alta seguridad sin causar la frustración del usuario, lo que lleva al abandono y a la pérdida de clientes.

FACTORES AMBIENTALES

En general, la detección de vida funciona en las mismas condiciones que un sistema de reconocimiento facial. Los algoritmos de vida actuales admiten diversas condiciones de iluminación, desde la luz diurna y del crepúsculo hasta entornos interiores y exteriores. Las funciones de control de calidad deben estar en funcionamiento para restringir la detección de vida cuando no hay iluminación o cuando la imagen está demasiado borrosa. En el caso de los accesos de alto riesgo, las empresas pueden considerar la posibilidad de aumentar la seguridad utilizando otra modalidad biométrica o un factor de autenticación cuando las condiciones de reconocimiento facial/ detección de vida sean deficientes.

COMPATIBILIDAD ENTRE CANALES

¿La solución es compatible con todos los dispositivos móviles y aplicaciones de escritorio, ya sea en el dispositivo, en la nube o en el servidor?

Cuando los clientes utilicen una solución con una variedad de dispositivos, es importante que la tecnología de detección de vida funcione universalmente en todos los canales y sea agnóstica a la marca/modelo del dispositivo siempre que cumpla con los criterios mínimos. La tecnología debe ser compatible con cualquier

dispositivo con una cámara HD que sea capaz de tomar una selfie a una resolución de al menos 720 megapíxeles. Por ejemplo, el iPhone5, lanzado en 2012, cumplía con este criterio y las cámaras actuales están en el rango de megapíxeles.

FACILIDAD DE INTEGRACIÓN E IMPLEMENTACIÓN

Evite el bloqueo eligiendo una solución de detección de vida que se pueda integrar con cualquier solución biométrica facial de terceros. También comprenda las opciones de implementación, que pueden variar desde aquellas basadas solamente en la nube hasta las de nube local o privada. Asegúrese de que las opciones de un proveedor cumplan con los requisitos de su empresa para el acceso y almacenamiento de datos.

PRUEBAS DE TERCEROS

iBeta Quality Assurance es el líder de la industria en pruebas de biometría y es el único laboratorio de pruebas biométricas acreditado por el Instituto Nacional de Estándares y Tecnología (NIST) bajo el Programa Nacional de Acreditación Voluntaria de Laboratorio (NVLAP). iBeta proporciona pruebas de Detección de Ataques de Presentación (PAD) realizadas de acuerdo con la norma ISO/IEC 30107-3.

Durante las pruebas, los sistemas sufren miles de ataques de presentación. Una solución compatible (anteriormente denominada “Certificada”) debe detectar el 100% de los ataques.

IDLive ha aprobado las pruebas de conformidad de Detección de Ataques de Presentación (PAD) de Nivel 1 y Nivel 2 de iBeta con una puntuación perfecta. ID R&D es el único proveedor que alcanza el Nivel 2 utilizando un enfoque de captura pasiva de una sola imagen.

Las pruebas de terceros son una consideración importante para validar las reclamaciones de un proveedor, pero no deben reemplazar las pruebas internas y la debida diligencia.

RESUMEN

La tecnología biométrica facial ofrece la posibilidad de autentificar a los clientes de una manera fácil de usar y, al mismo tiempo, reforzar la seguridad. Pero incluso las soluciones más difíciles son susceptibles a ataques de falsificación utilizando imágenes de alta resolución, videos, máscaras y falsificaciones. La superación de estos desafíos ha presentado ciertos obstáculos a los clientes, lo que es frustrante y un factor disuasorio para una adopción biométrica exitosa.

La detección de vida pasiva cierra las brechas de seguridad en la biometría facial sin volver a presentar inconvenientes en el proceso de autenticación. Esta tecnología funciona rápidamente en segundo plano y no requiere que los usuarios reciban capacitación sobre el proceso.

Reducir el esfuerzo de los clientes es una prioridad para la mayoría de las empresas. Al implementarla como parte de un sistema biométrico facial, es importante considerar cómo la solución impacta en la experiencia del usuario. ¿Reducirá la velocidad de los usuarios, causará confusión o aumentará las tasas de abandono?

Además de la experiencia del usuario, hay otros elementos a tener en cuenta como los requisitos de software, el impacto en la velocidad, la complejidad de la integración, las opciones de implementación, la robustez de la solución y, por supuesto, su caso de uso específico.

SIENDO LA BIOMETRÍA FACIAL UN ELEMENTO CADA VEZ MÁS COMÚN PARA AUTENTIFICAR A LOS USUARIOS ONLINE Y REMOTOS, LA DETECCIÓN DE VIDA ESTÁ EMERGIENDO COMO LA PIEZA CRÍTICA DE UNA SOLUCIÓN INTEGRAL.

Acerca de IDLive™ Face por ID R&D

ID R&D proporciona IDLive Face, el primer producto de detección de vida facial verdaderamente pasivo del mundo. IDLive face funciona con cualquier software de reconocimiento facial de terceros y no requiere ninguna acción adicional por parte del usuario. La tecnología utiliza un análisis de un solo disparo y no requiere ningún software especial de captura. También funciona en dispositivos móviles, web y dispositivos independientes.

IDLive ha aprobado las pruebas de conformidad de Detección de Ataques de Presentación (PAD) de Nivel 1 de iBeta con una puntuación perfecta y cumple con la norma ISO/IEC 30107-3.

Vea una demostración en www.idrnd.ai.

1441 Broadway, Suite 6019
New York, New York 10018 USA
info@idrnd.net