Regula

19 JUN 2025 11 MIN PARA LEER EN FRAUDE DE IDENTIDAD

Dos caras de la IA en la verificación de identidad y prevención del fraude

Nikita Dunets
Subdirector, Verificación de Identidad Digital, Regula

CONTENIDO

Suscribirse

COMPARTE ESTE ARTÍCULO

No hay duda de que la inteligencia artificial (IA) está transformando la verificación de identidad, al igual que está revolucionando muchos otros aspectos del mundo. Cada vez más, gobiernos y empresas de todo el mundo integran IA en sus sistemas de verificación de identidad, no solo para ganar en eficiencia, sino también en eficacia. Mientras tanto, los delincuentes no se quedan atrás: aprovechan la IA para crear sofisticados deepfakes y generar identidades falsas cada vez más difíciles de detectar.

En este artículo, exploraremos ambas caras de la IA en el ámbito de la verificación de identidad: cómo esta tecnología ayuda a verificar a las personas (a través de biometría, prueba de vida y análisis antifraude), y cómo también puede obstaculizar el proceso (con fraudes basados en deepfakes e identidades sintéticas). Compartiremos, además, nuestra visión sobre el futuro de la industria y las claves para impulsar un desarrollo positivo.

El lado positivo: cómo la IA impulsa la verificación de identidad

En los últimos años, hemos visto cómo las tecnologías de IA han mejorado de forma notable la seguridad, precisión y eficiencia de los procesos de verificación de identidad. Siempre que no utilice ChatGPT para autenticar documentos de identidad importantes, podrá aprovechar la inteligencia artificial de muchas otras formas.

Comparación biométrica

Hoy en día, la verificación de identidad depende en gran medida de la biometría, como el reconocimiento facial, de huellas dactilares y de voz. Justamente en estas áreas, la inteligencia artificial ha mejorado significativamente la precisión, gracias a su capacidad para mapear los rasgos faciales de una persona y compararlos con documentos de identidad o plantillas previamente almacenadas.

El Departamento de Seguridad Nacional de los Estados Unidos destaca que el reconocimiento y la captura facial son "tecnologías de IA sumamente potentes", que ellos mismos utilizan con gran éxito: cuentan con 14 casos de uso distintos y una tasa de acierto mínima del 97 %.

Mientras tanto, en Europa, la Ley de IA de la UE entró en vigor el 1 de agosto de 2024, con el objetivo principal de proteger a las empresas y a los consumidores europeos frente al uso indebido de la inteligencia artificial. Su aplicación general será obligatoria en agosto de 2026, aunque ya contempla etapas intermedias que brindan a las empresas directrices adicionales para preparar sus sistemas y lograr una total conformidad para agosto de 2027. Según esta legislación, muchas

aplicaciones relacionadas con la verificación de identidad — como el software de clasificación de CV o los sistemas de gestión de control fronterizo — se consideran de alto riesgo.

Para cumplir con estos requisitos, las organizaciones deben:

- Implementar un marco de evaluación de riesgos y seguridad, que incluya el registro completo de las actividades del sistema y la preparación de documentación detallada para su revisión por parte de los organismos reguladores.
- Utilizar conjuntos de datos de alta calidad para entrenar redes neuronales y minimizar posibles sesgos en los resultados.
- Garantizar la supervisión humana de los sistemas de verificación de identidad basados en IA.

Prueba de vida

Uno de los métodos más comunes para intentar engañar a un sistema de comparación facial es utilizar una fotografía o un video de otra persona. Podría ser una técnica muy poderosa, si no fuera por la prueba de vida.

La prueba de vida garantiza que haya una persona real y viva durante el proceso de verificación biométrica, analizando señales sutiles como el parpadeo, la textura facial, la profundidad en 3D o el movimiento. Estos indicadores físicos son extremadamente difíciles de falsificar mediante fotografías o videos pregrabados. Hoy en día, muchos servicios de verificación de identidad en línea ya integran este tipo de pruebas en sus flujos de registro, por ejemplo, solicitando al usuario que gire la cabeza.

Verificación automatizada de documentos

A diferencia de las revisiones manuales, que suelen ser más lentas y propensas a errores, las redes neuronales y los sistemas de visión basados en IA permiten inspeccionar automáticamente una amplia variedad de documentos de identidad, como pasaportes, cédulas nacionales y licencias de conducir, entre otros.

Estos modelos están entrenados para detectar numerosos elementos de seguridad (tinta OVI, hologramas, entre otros) y para extraer texto de los documentos mediante reconocimiento óptico de caracteres (OCR), con el fin de realizar comprobaciones cruzadas posteriores. Cualquier anomalía detectada se compara con una base de datos que puede contener miles de plantillas de documentos de identidad, lo que permite identificar incluso los indicios más sutiles de manipulación o falsificación.

El lado oscuro: cómo la IA puede obstaculizar la verificación de identidad

Al mismo tiempo, existe otra cara en la historia de la inteligencia artificial. Aunque ha contribuido a reforzar las medidas de seguridad, también ha facilitado a los estafadores nuevas formas de atacarlas. Los actores malintencionados están utilizando algoritmos de IA para suplantar identidades, crear identidades falsas o engañar los controles biométricos, a veces con un nivel de éxito alarmante.

Fraude de identidad con deepfakes

Quizás la amenaza más disruptiva sea el auge de los deepfakes: videos, imágenes o audios falsos generados por IA que imitan a personas reales. En algunos casos, estos materiales pueden ser lo suficientemente sofisticados como para superar verificaciones de identidad en tiempo real. Los impostores pueden utilizar marionetas digitales para simular el rostro de la víctima o utilizar voces clonadas mediante IA para cometer fraudes de identidad. Esto ya ha sido demostrado por diversos informes del sector en 2024; uno de ellos señala que “los sistemas de autenticación biométrica que utilizan reconocimiento facial o de voz ya han sido comprometidos por la tecnología de deepfakes en varios casos críticos”.

Un caso particularmente impactante ocurrió a principios de 2024: un grupo de delincuentes crearon un deepfake del director financiero (CFO) de una empresa y de otros empleados para engañar a un responsable del área financiera. Durante una videoconferencia, este empleado vio lo que parecía ser el rostro auténtico de su CFO dándole instrucciones. Convencido de que la interacción era genuina, transfirió posteriormente 25 millones de dólares a las cuentas de los atacantes, antes de que se descubriera el fraude.

Fraude de identidad sintética

Otra forma de delito financiero que está creciendo rápidamente es el fraude de identidad sintética, en el cual los delincuentes crean una persona completamente falsa combinando datos reales (por ejemplo, un número de seguridad social válido) con información inventada. Históricamente, este tipo de fraude era difícil de detectar porque no corresponde a una víctima real (por lo tanto, nadie lo reporta) y permite a los estafadores desarrollar un perfil crediticio falso de manera gradual para evitar ser detectados.

Hoy en día, la inteligencia artificial facilita aún más este tipo de fraude: los estafadores pueden generar fotos de perfil únicas para sus identidades sintéticas, de modo que una búsqueda inversa de imágenes no detecte ninguna foto de archivo. Además, pueden utilizar IA para crear documentos de respaldo falsos.

En una encuesta reciente realizada por nuestro equipo, descubrimos que aproximadamente el 49 % de las empresas en EE. UU. y el 51 % de las empresas en los Emiratos Árabes Unidos ya enfrentan dificultades con identidades sintéticas que se utilizan para solicitar sus servicios. Aún más preocupante, periodistas de investigación han demostrado lo sencillo (y económico) que resulta hoy en día obtener credenciales falsas de alta calidad. En una prueba realizada en 2024, un investigador generó una licencia de conducir ficticia a través de un servicio clandestino de IA utilizando su propia foto y datos personales falsos por tan solo 15 dólares. El sistema produjo una imagen de documento hiperrealista, con firma y datos coherentes, que el investigador presentó en el proceso de verificación KYC de una plataforma de criptomonedas... y la revisión automatizada lo aprobó, permitiéndole abrir una cuenta.

Falsos negativos

Este caso no corresponde a un intento malicioso de fraude, sino a una consecuencia no deseada de sistemas que no son perfectos: los falsos negativos, donde usuarios legítimos son marcados erróneamente como fraude. Esto puede deberse a cambios en la iluminación, al envejecimiento de la fotografía en el documento de identidad, o incluso a patrones extraños detectados por el algoritmo. Cada rechazo erróneo genera, comprensiblemente, frustración en los usuarios, lo que obliga a las empresas a recurrir nuevamente a supervisión humana para no depender en exceso de la automatización.

Además, las redes neuronales pueden fallar de maneras que incluso resulten sesgadas. Si un modelo no ha sido entrenado con un conjunto de datos diverso, puede tener dificultades para reconocer rostros de ciertos grupos demográficos, lo que provoca tasas de rechazo más altas para esas poblaciones. Por ejemplo, en el Reino Unido, un repartidor de UberEats fue despedido injustamente luego de que la IA fallara repetidamente al verificar su rostro. Se le informó que existían "desajustes continuos" con sus selfies, y fue eliminado de la plataforma, lo que

derivó en una demanda por discriminación que finalmente terminó en una compensación económica.

¿Qué lado está ganando?

En nuestra opinión, hoy en día la mayoría de los deepfakes todavía son detectables, ya sea por profesionales atentos o mediante soluciones de verificación de identidad basadas en IA que llevan tiempo en el mercado. Dicho esto, las amenazas basadas en deepfakes evolucionan rápidamente, y ya estamos cerca de ver ejemplos altamente convincentes que apenas generan sospechas.

Por ello, la prioridad debe ser "entrenar mejor a la buena IA", reforzándola continuamente con más datos sobre fraudes. Los equipos deben estar atentos a cualquier detalle sospechoso o inconsistente durante las comprobaciones de liveness, capturar nuevos ejemplos de datos y alimentar esos aprendizajes al sistema.

Afortunadamente, el fraude de identidad generado por IA todavía presenta ciertas limitaciones. Por ejemplo, muchos deepfakes no reproducen correctamente las sombras o presentan fondos poco naturales. Los documentos falsos también suelen carecer de elementos de seguridad dinámicos y no proyectan imágenes específicas cuando se ven desde ciertos ángulos. Otro desafío clave que enfrentan los delincuentes es que muchos modelos de IA han sido entrenados principalmente con imágenes faciales estáticas, ya que son las más accesibles en línea. Por lo tanto, estos modelos tienen dificultades para generar realismo en sesiones de video en 3D con prueba de vida, donde se solicita a la persona que mueva la cabeza.

Además, los documentos de identidad modernos suelen incluir características de seguridad dinámicas visibles únicamente cuando el documento está en movimiento. La industria sigue innovando constantemente en este ámbito, lo que hace prácticamente imposible crear documentos falsos convincentes que superen una sesión de captura con validación de liveness, en la cual el documento debe girarse en diferentes ángulos. Por ello, requerir documentos físicos para las pruebas de liveness puede incrementar notablemente la seguridad de su organización.

Las empresas también pueden combatir los deepfakes controlando por completo la fuente de señal. Algunas plataformas móviles nativas no permiten la manipulación del flujo de video, lo cual supone una gran ventaja. Y siempre se puede emplear la autenticación multifactor: la identidad de una persona no solo puede verificarse mediante su documento o biometría, sino también a través de otros elementos, como su dirección, número telefónico, verificaciones en bases de datos o información personal adicional.

En definitiva, esta es una constante lucha de gato y ratón con los estafadores, y los resultados suelen ser imprevisibles. Pero, por ahora, parece que el lado positivo todavía mantiene la ventaja.

Cómo lograr una verificación de identidad segura

Su proceso de verificación de identidad puede beneficiarse enormemente de soluciones de software robustas que lo hagan no solo seguro, sino también ágil, intuitivo y conforme a la normativa vigente. Por ejemplo, la verificación de identidad y la biometría facial con prueba de vida pueden realizarse con soluciones como Regula Document Reader SDK y Regula Face SDK.

Document Reader SDK procesa imágenes de documentos y verifica tanto su autenticidad como su presencia física (liveness), superando la gran mayoría de intentos fraudulentos impulsados por IA. El software identifica el tipo de documento, extrae toda la información necesaria y confirma si se trata de un documento genuino.

Por su parte, Regula Face SDK realiza reconocimiento facial instantáneo y previene ataques de presentación basados en IA gracias a su avanzada prueba de vida y evaluación de atributos faciales.

Reserva tu consulta gratuita

Descubra cómo optimizar su verificación de identidad: sin complicaciones, más eficiente y todo desde un solo lugar.

Contáctenos

También te puede interesar

VERIFICACIÓN DE DOCUMENTOS

Escáneres de documentos de identidad: Cómo funcionan, tipos y cómo elegir el adecuado

CASOS DE USO EMPRESARIALES

eKYC explicado: Por qué el futuro es digital

VERIFICACIÓN DE DOCUMENTOS

Control de pasaportes: Fases de inspección primaria y secundaria

FRAUDE DE IDENTIDAD

Deepfakes en verificación de identidad: Lo que las empresas deben saber

Ayuda a las organizaciones a simplificar y agilizar el proceso de autenticación de documentos y la verificación de identidad.

Manténgase en contacto con Regula.

Suscribirse

PRODUCTOS

Software de Verificación de Identidad

Dispositivos de Lectura de Documentos

Lectores de Documentos
Comparadores Espectrales de Vídeo
Microscopios y Lupas
Dispositivos de Control Manual
Dispositivos Magneto-Ópticos
Sistema de Información y Referencia
Inspección de Vehículos y Armas
Examinación Remota

CASOS DE USO

Automatización KYC
Incorporación de clientes
Automatización de ingreso de datos
Prevención del fraude
Automatización del check-in
Verificación de la edad
Comprobación no destructiva del VIN
Examen remoto de documentos
Control fronterizo de primera línea

ARTÍCULOS

Verificación de identidad de la A a la Z
¿Cómo funcionan los escáneres de DNI?

INDUSTRIAS

Control fronterizo
Gobierno
Tecnología financiera y criptomoneda
Bancos
Viajes y hostelería
Asistencia sanitaria
Apuestas
Educación

Telecomunicaciones

Seguros

Laboratorios forenses

EXPLORAR

Historias de Éxito de Clientes

Blog

Centro de Recursos

Tecnologías

Eventos y Seminarios Web

Sala de Prensa

Regula para Desarrolladores

PROBAR EN LÍNEA

Verificación de Documentos

Verificación Biométrica

App Store

Google Play

REGULA PARA EXPERTOS FORENSES

Sistema de Información y Referencia

Capacitación Especializada

Glosario de Documentos

Glosario de Billetes de Banco

CENTRO DE AYUDA

COMPAÑÍA

Acerca de Regula

Certificados