Aprendizaje profundo aplicado a la validación de la identidad digital

Fredy Santander Baños[1][0000-0003-0477-4225], Juan Humberto Sossa Azuela[2][0000-0002-0521-4898], y Eduardo Dorantes Sánchez.[3][0009-0004-7995-5682]

[1]Universidad Autónoma del Estado de Hidalgo, Instituto de Ciencias Básicas e Ingeniería, Área Académica de Computación y Electrónica.
[2]Instituto Politécnico Nacional, Centro de Investigación en Computación. [3]Investigador y Desarrollador de Software independiente, México.
fredy_santander@uaeh.edu.mx

Resumen. La digitalización de trámites, servicios financieros y procesos institucionales en México ha incrementado la necesidad de verificar la identidad de las personas de forma remota, segura y confiable. Este proceso enfrenta amenazas como la falsificación de credenciales para votar y la suplantación facial mediante fotografías, videos o imágenes reproducidas ante una cámara. Este capítulo presenta una plataforma de inteligencia artificial desarrollada en México, integrada por dos módulos complementarios: uno orientado a estimar si la imagen de una credencial para votar corresponde a un documento físico auténtico, y otro enfocado en verificar si el rostro capturado pertenece a una persona presente. La solución combina modelos de visión artificial mediante una estrategia de doble opinión adaptativa. Actualmente, la plataforma opera en un entorno productivo y ha mostrado un desempeño cercano al 99% de acierto bajo esquemas de revisión continua. Se describe su diseño, implementación e impacto para fortalecer la confianza en los servicios digitales y promover capacidades nacionales en inteligencia artificial aplicada.

Palabras Clave: Detección de fraude, verificación de identidad digital, inteligencia artificial, antispoofing facial, credencial para votar, ensamble de modelos.

1 Introducción

La credencial para votar emitida por el Instituto Nacional Electoral (INE) es uno de los documentos de identificación oficial de mayor uso en México. Además de permitir el voto, se utiliza como medio de identificación ante instituciones públicas y privadas, incluyendo procesos financieros y trámites ciudadanos [5, 6, 13]. Su amplia cobertura refuerza esta relevancia: al 16 de abril de 2026, el Padrón Electoral registró 101,956,653 ciudadanas y ciudadanos, mientras que la Lista Nominal alcanzó 100,122,170 registros [5].

Con la digitalización de servicios, cada vez más instituciones permiten procesos remotos de registro, contratación o validación de identidad, especialmente en el sector financiero [6]. En estos procesos, la persona usuaria suele capturar con su teléfono móvil una imagen de su credencial para votar y una fotografía de su rostro. Esta

comodidad introduce riesgos: un atacante puede intentar engañar al sistema mediante copias, impresiones, imágenes en pantalla o fotografías usadas para simular la presencia de otra persona. Estos engaños, conocidos como ataques de presentación, son reconocidos por la norma ISO/IEC 30107 como una amenaza para sistemas biométricos y de verificación automatizada [2, 3].

La suplantación de identidad puede generar apertura indebida de cuentas, contratación de créditos, operaciones no reconocidas y reclamaciones ante instituciones financieras. En México, la CONDUSEF ha documentado casos relacionados con posible robo o suplantación de identidad en el sector financiero, así como reportes de instituciones afectadas por el uso indebido de su nombre o datos comerciales [14, 15]. Para las víctimas, esto puede traducirse en deudas no contraídas y procesos prolongados de aclaración; para las instituciones, en pérdida de confianza y mayores costos de verificación. Aunque la revisión humana sigue siendo necesaria en casos ambiguos o de alto riesgo, presenta limitaciones cuando crece el volumen de solicitudes: fatiga, variabilidad entre revisores y dificultad para identificar patrones visuales sutiles. Frente a este escenario, la inteligencia artificial ofrece una alternativa complementaria al analizar imágenes de manera uniforme, detectar señales difíciles de percibir a simple vista y apoyar decisiones en menor tiempo [1, 4, 7].

Este capítulo presenta una plataforma de inteligencia artificial desarrollada en México para fortalecer la validación remota de identidad. La solución integra dos módulos: uno orientado a estimar si la imagen de una credencial para votar corresponde a un documento físico auténtico, y otro enfocado en verificar si el rostro capturado pertenece a una persona físicamente presente. Ambos se encuentran en operación productiva y comparten un principio de diseño: combinar modelos de visión artificial con fortalezas complementarias para tomar decisiones más robustas.

2 Marco de Referencia

La verificación de identidad digital combina elementos documentales, biométricos y computacionales. En un entorno remoto, el sistema no observa directamente a la persona ni al documento, sino imágenes capturadas por una cámara. Por ello, esta sección revisa tres conceptos clave: ataques de presentación, visión por computadora basada en aprendizaje profundo y ensambles de modelos.

2.1 Identidad digital remota y ataques de presentación

En un proceso presencial, un operador puede revisar físicamente a la persona y su documento. En cambio, en un proceso remoto, el sistema evalúa representaciones visuales. En este contexto aparecen los ataques de presentación, definidos por la norma ISO/IEC 30107 como intentos de alterar el funcionamiento de un sistema biométrico mediante la presentación de un artefacto, reproducción o característica falsa [2, 3]. La Fig. 1 ilustra la diferencia entre una captura legítima y un ataque de presentación. En un entorno remoto, el sistema recibe imágenes del documento y del rostro, lo que permite intentos de engaño mediante copias, pantallas, fotografías o máscaras.

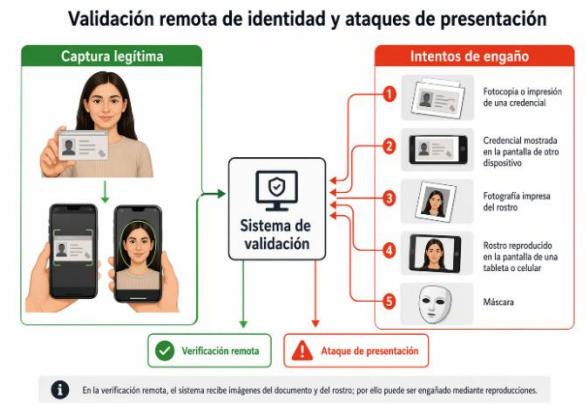

Fig. 1. Validación remota de identidad y ataques de presentación.

2.2 Tipos de ataques contra documentos y rostros

Los ataques de presentación considerados en este capítulo se agrupan en dos categorías: ataques contra documentos y ataques contra rostros. Los primeros buscan que una reproducción sea aceptada como una credencial física auténtica; los segundos intentan simular la presencia de una persona ante la cámara. La Fig. 2 presenta esta clasificación visual.

Fig. 2. Tipos de ataques de presentación contra documentos y rostros.

La Tabla 1 complementa esta clasificación mediante las principales familias de ataques y un ejemplo representativo.

Esta clasificación se centra en ataques de presentación. Otros fraudes, como la alteración de datos en una credencial, pueden requerir mecanismos adicionales: OCR, validación documental, comparación biométrica o consulta con fuentes autorizadas.

Tabla 1. Principales familias de ataques de presentación contra documentos y rostros.

Elemento	Tipo de ataque	Ejemplo
Credencial	Reproducción física del documento	Presentar una fotocopia, impresión o reproducción física de la credencial para votar, ya sea degradada o de alta calidad.
Credencial	Imagen en pantalla	Mostrar la imagen de la credencial en la pantalla de otro teléfono, tableta o computadora.
Credencial	Captura previamente almacenada	Utilizar una fotografía antigua del documento en lugar de capturarlo en el momento del registro.
Rostro	Fotografía impresa	Sostener una fotografía del rostro de otra persona frente a la cámara.
Rostro	Imagen o video en pantalla	Reproducir un rostro en la pantalla de un celular, tableta o monitor.
Rostro	Máscara plana	Utilizar un recorte o impresión del rostro para simular la presencia de una persona.
Rostro	Máscara tridimensional	Emplear una máscara con volumen facial para intentar engañar el sistema.

2.3 Inteligencia artificial para detectar patrones visibles

La visión por computadora permite analizar imágenes y extraer información útil. En particular, los modelos de aprendizaje profundo pueden aprender patrones visuales complejos a partir de ejemplos, sin depender únicamente de reglas manuales [1, 4].

En la verificación documental y facial, estos modelos identifican señales como textura, nitidez, reflejos, patrones de pantalla, iluminación, deformaciones por impresión, bordes inconsistentes o ausencia de profundidad. La Fig. 3 resume cómo estas señales se transforman en un puntaje para estimar si una imagen corresponde a una captura legítima o a una reproducción. El modelo analiza señales como textura, nitidez, reflejos, iluminación y patrones de pantalla para estimar si la imagen corresponde a una captura legítima o a una reproducción.

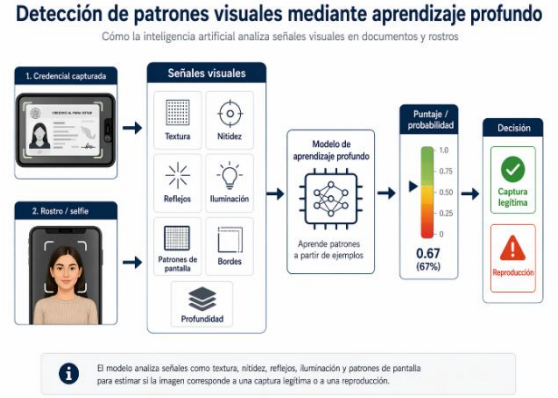

Fig. 3. Detección de patrones visuales mediante aprendizaje profundo.

Esta capacidad resulta útil en escenarios reales, donde las imágenes pueden capturarse con poca luz, inclinación, reflejos o cámaras de distinta calidad.

2.4 Modelos de visión artificial utilizados como base

La plataforma emplea modelos con funciones complementarias: algunos clasifican imágenes completas y otros localizan regiones de interés. Para el análisis documental se utiliza EfficientNet, una familia de modelos diseñada para equilibrar precisión y eficiencia computacional [1].

En la verificación facial, primero se localiza el rostro mediante detectores de la familia YOLO, ampliamente utilizados por su rapidez y precisión; variantes como YOLO5Face han sido propuestas para rostros en condiciones diversas [10]. Después, el sistema evalúa si el rostro corresponde a una persona presente o a una reproducción mediante modelos de antispoofing facial, como MiniFASNet [9]. Uno de los conjuntos de datos más relevantes para esta tarea es CelebA-Spoof, con más de 600,000 imágenes de rostros reales y ataques [8].

2.5 Ensambles de modelos y principio de doble opinión

Un ensamble combina respuestas de varios modelos para obtener una decisión más estable que la de un solo modelo. Esta estrategia se basa en que modelos entrenados de forma distinta pueden cometer errores diferentes, por lo que integrar sus opiniones ayuda a reducir fallos [7].

En este capítulo, el ensamble se interpreta como doble opinión adaptativa: dos modelos analizan el mismo caso y sus respuestas se combinan mediante reglas que ajustan la influencia de cada modelo según su nivel de certeza. La Fig. 4 representa este principio. Dos modelos con fortalezas complementarias analizan la misma imagen; sus puntajes se integran mediante un mecanismo de combinación que ajusta su influencia según la certeza de cada caso.

Este enfoque es relevante porque los errores tienen consecuencias distintas: rechazar a una persona legítima genera fricción, pero aceptar una reproducción puede derivar en fraude. Con base en estos elementos, la siguiente sección describe la plataforma propuesta y su aplicación en los módulos de verificación documental y facial.

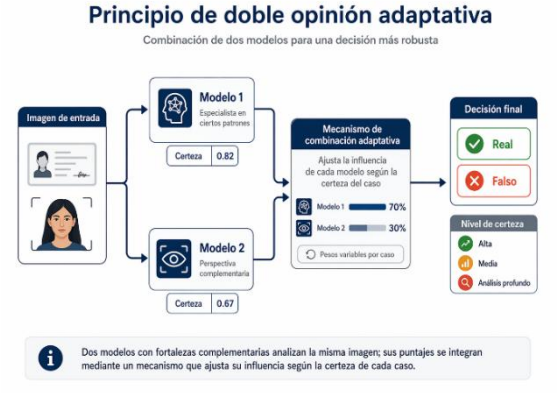

Fig. 4. Principio de doble opinión adaptativa.

3 Descripción de la propuesta de solución

La plataforma propuesta apoya procesos remotos de validación de identidad mediante el análisis automatizado de dos evidencias visuales: una imagen de la credencial para votar y una imagen facial o selfie. La solución se organiza en dos rutas especializadas —verificación documental y verificación facial— que emplean modelos de visión artificial y mecanismos de decisión adaptativos para estimar si las evidencias corresponden a capturas legítimas o a posibles reproducciones.

Esta sección describe la arquitectura general de la plataforma, el funcionamiento de ambas rutas de verificación y su operación en un entorno productivo.

3.1 Arquitectura general de la plataforma

La plataforma funciona como un sistema modular. En un proceso típico, una institución solicitante envía dos evidencias capturadas durante el registro de una persona usuaria: la imagen de la credencial para votar y una selfie. A partir de ellas se activan dos rutas de análisis.

La ruta documental analiza la credencial mediante una etapa de preprocesamiento y dos modelos complementarios, V8 y V3, cuyas salidas se integran mediante una combinación inteligente basada en zonas de confianza. La ruta facial localiza y recorta el rostro antes de evaluarlo mediante un módulo especialista, MiniFASNet, y un módulo generalista, EfficientNet. En este caso, la decisión incorpora una lógica de priorización de fraude. La Fig. 5 resume la arquitectura general: entradas del sistema, rutas de procesamiento, modelos participantes y respuesta final. Esta respuesta incluye clasificación, puntaje de confianza y nivel de certeza, elementos que permiten apoyar decisiones automatizadas o derivar casos ambiguos a revisión humana.

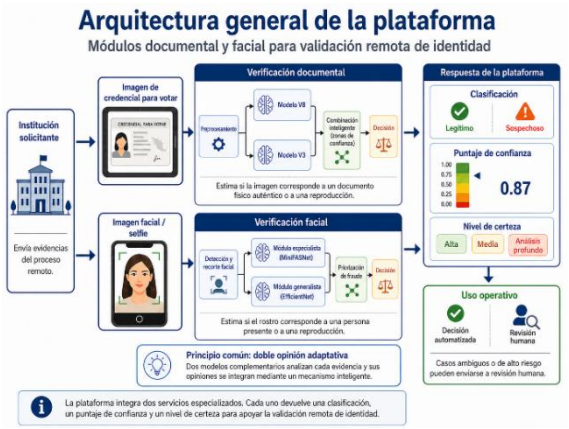

Fig. 5. Arquitectura general de la plataforma de validación de identidad digital.

3.2 **Verificación documental: procesamiento y decisión**

La ruta documental estima si la imagen de la credencial para votar corresponde a un documento físico auténtico o a una reproducción presentada ante la cámara. Como se muestra en la Fig. 5, el proceso inicia con el preprocesamiento de la imagen para reducir variaciones de resolución, iluminación, encuadre o dispositivo de captura. Después, la imagen es evaluada por dos modelos basados en EfficientNet. El Modelo V8 actúa como componente principal de decisión cuando la evidencia visual es clara, mientras que el Modelo V3 funciona como segunda opinión en casos con señales sutiles o zonas de incertidumbre.

La decisión final no se obtiene mediante un promedio simple, sino mediante una combinación basada en zonas de confianza. Cuando V8 muestra certeza muy alta o muy baja, su salida predomina; cuando el caso se ubica en una zona intermedia, V3 adquiere mayor influencia. La Fig. 6 resume esta lógica adaptativa. En ella se observa que el módulo documental no sigue una única ruta de decisión, sino que modifica la influencia de cada modelo según la zona de confianza. De esta manera, los casos evidentes pueden resolverse con rapidez, mientras que los casos ambiguos reciben un análisis más cuidadoso. El sistema combina las salidas de los modelos V8 y V3 mediante zonas de confianza; cuando el caso es ambiguo, el Modelo V3 adquiere mayor influencia como segunda opinión.

La Tabla 2 resume las reglas generales de decisión del módulo documental. En términos operativos, los casos claramente sospechosos pueden rechazarse con alta confianza; los casos donde ambos modelos coinciden positivamente pueden aceptarse con mayor seguridad; y los casos ambiguos o con discrepancia entre modelos pueden recibir un nivel de certeza intermedio o enviarse a revisión humana.

Tabla 2. Reglas de decisión del módulo de verificación documental.

Certeza de V8	¿Qué hace el sistema?	Decisión	Nivel de certeza
Muy baja (< 0.59)	Decide de inmediato sin consultar a V3	Falso	Ultra alta
Baja (0.59 a 0.67)	Consulta a V3; si V3 contradice con fuerza, analiza a fondo	Depende del análisis	Análisis profundo
Baja (0.59 a 0.67)	Si V3 no contradice con fuerza	Falso	Alta
Media-alta (> 0.67)	Si V3 también tiene certeza alta y ambos coinciden	Real	Ultra alta
Media (0.67 a 0.74)	Zona de duda: V3 actúa como árbitro con mayor peso	Depende del promedio	Media
Alta (> 0.74)	V8 domina la decisión, V3 complementa	Depende del promedio	Conservador

Este esquema permite resolver rápidamente casos evidentes y analizar con mayor cuidado aquellos ambiguos. La salida se expresa como clasificación, puntaje de confianza y nivel de certeza.

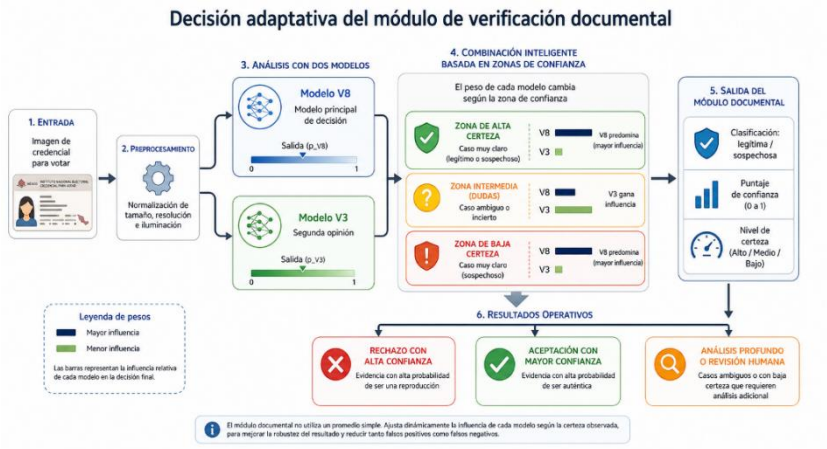

Fig. 6. Decisión adaptativa del módulo de verificación documental.

3.3 **Verificación facial: procesamiento y decisión**

La ruta facial estima si el rostro capturado corresponde a una persona presente o a una reproducción, como una fotografía impresa, una imagen en pantalla o una máscara. A diferencia del módulo documental, primero debe localizar el rostro y después evaluar si la captura es legítima o sospechosa.

Para localizar el rostro se utiliza un detector basado en YOLOv5 [10]. Una vez identificado, el sistema recorta la región facial con un margen ampliado de aproximadamente 50%, lo que permite conservar información contextual útil, como bordes de pantalla, reflejos, textura del fondo o señales de impresión. El análisis se realiza mediante dos componentes: un módulo especialista basado en MiniFASNet [9], apoyado en bases como CelebA-Spoof [8], y un módulo generalista basado en EfficientNet, ajustado a condiciones operativas de la plataforma en México.

La decisión facial incorpora una estrategia de priorización de fraude. Si el módulo especialista detecta suplantación con certeza superior al 95%, la decisión se toma de forma inmediata. Si no existe fraude evidente, se consulta al módulo generalista y se integran ambas salidas. La Fig. 7 resume este funcionamiento.

Cuando el sistema clasifica un rostro como legítimo, ajusta su puntaje de confianza a una escala interpretable para las instituciones usuarias. En esta escala, 0.70 representa el umbral mínimo de aceptación y los valores cercanos a 1.0 indican niveles más altos de confianza. Al igual que en la ruta documental, la salida final se expresa como una clasificación, un puntaje de confianza y un nivel de certeza, lo que permite automatizar casos claros y derivar a revisión humana aquellos con baja certeza o evidencia contradictoria.

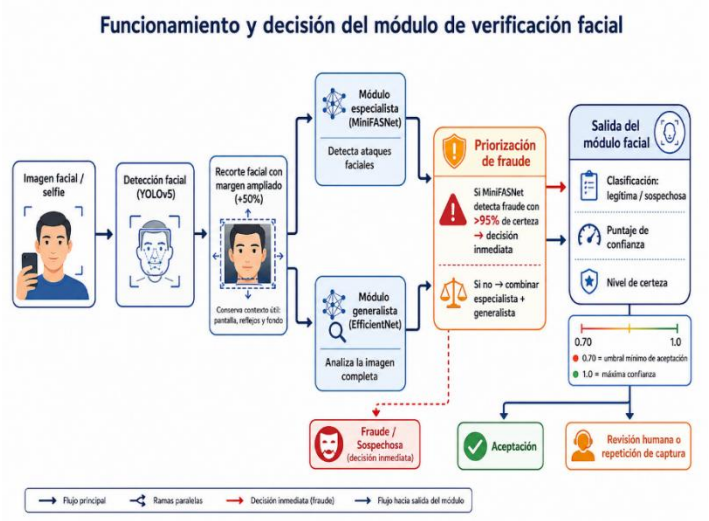

Fig. 7. Funcionamiento y decisión del módulo de verificación facial.

3.4 **Doble opinión adaptativa como patrón común**

Aunque las rutas documental y facial atienden problemas distintos, ambas comparten un principio de diseño: usar dos modelos complementarios y combinar sus salidas de forma adaptativa. En la verificación documental, esto se logra mediante zonas de confianza; en la facial, mediante priorización de fraude.

La Tabla 3 resume las principales coincidencias y diferencias entre ambas rutas, esta comparación permite observar que la plataforma no aplica una misma regla de decisión a todos los casos, sino que ajusta su funcionamiento de acuerdo con el tipo de evidencia analizada y el riesgo asociado.

Tabla 3. Comparación funcional entre las rutas documental y facial.

Característica	Verificación documental	Verificación facial
Evidencia analizada	Imagen de credencial para votar	Imagen facial o selfie
Objetivo principal	Estimar si la credencial corresponde a un documento físico auténtico o a una reproducción	Estimar si el rostro corresponde a una persona presente o a una reproducción
Etapa inicial	Preprocesamiento de la imagen	Detección facial y recorte ampliado
Modelos utilizados	Modelo V8 y Modelo V3	Módulo especialista MiniFASNet y módulo generalista EfficientNet
Estrategia de decisión	Combinación inteligente basada en zonas de confianza	Priorización de fraude ante indicios fuertes de suplantación
Papel del segundo modelo	Segunda opinión en zonas de incertidumbre	Complemento cuando no hay fraude evidente
Salida	Clasificación, puntaje de confianza y nivel de certeza	Clasificación, puntaje de confianza y nivel de certeza

Este patrón permite aprovechar la especialización de cada modelo sin depender de una única salida automática.

3.5 **Despliegue operativo en entorno productivo**

La plataforma opera como servicios disponibles por internet y empaquetados en contenedores, lo que facilita su actualización, escalamiento y despliegue independiente. En producción, la ruta documental opera con 20 réplicas simultáneas y la facial con 5 réplicas, diferencia asociada con la complejidad adicional de localizar y recortar el rostro.

Ambos módulos responden en fracciones de segundo y fueron optimizados para ejecutarse en servidores convencionales, sin depender de hardware especializado. Sus modelos ocupan entre 1.9 y 4.5 MB, lo que reduce costos operativos y favorece su implementación en infraestructura local, aspecto relevante cuando se procesan documentos de identidad y rostros.

En conjunto, este esquema de despliegue busca equilibrar tres necesidades: rapidez de respuesta, escalabilidad operativa y control sobre los datos procesados. Esto resulta especialmente relevante en aplicaciones de validación de identidad digital, donde la eficiencia técnica debe acompañarse de criterios de seguridad, privacidad y continuidad del servicio.

4 **Resultados y Discusión**

Esta sección resume los datos utilizados, el desempeño observado en producción y la utilidad de los niveles de certeza. Los resultados se presentan como evidencia operativa en condiciones reales de uso, no como una evaluación formal bajo protocolo de laboratorio.

4.1 **Datos utilizados para entrenamiento y ajuste**

El módulo documental fue entrenado con aproximadamente 20,000 imágenes de credenciales para votar: cerca de 10,000 auténticas y 10,000 no legítimas o asociadas con reproducciones. Las imágenes incluyeron variaciones de iluminación, ángulo, resolución y tipo de cámara.

Para la verificación facial, el módulo especialista se apoyó en CelebA-Spoof [8], con más de 600,000 imágenes de rostros reales y ataques. De forma complementaria, el módulo generalista fue ajustado con datos representativos de las condiciones operativas en México.

La Fig. 8 ilustra la separación conceptual entre puntajes de capturas legítimas y reproducciones, útil para definir umbrales, zonas de confianza y reglas de decisión.

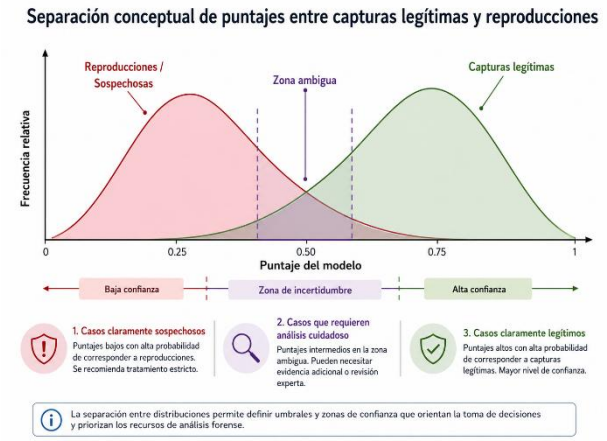

Fig. 8. Separación conceptual de puntajes entre capturas legítimas y reproducciones.

4.2 Desempeño observado en operación productiva

En operación productiva, la plataforma ha mostrado un desempeño cercano al 99% de acierto bajo un esquema de muestreo y revisión humana continua. Este valor debe entenderse como un indicador operativo observado en condiciones reales, no como una evaluación formal estandarizada.

La Tabla 4 presenta ejemplos representativos del módulo documental. Los valores de V8 y V3 indican confianza en una escala de 0 a 1, donde valores cercanos a 1 favorecen una captura legítima y valores cercanos a 0 sugieren una reproducción.

Tabla 4. Ejemplos representativos de clasificación del módulo de verificación documental.

Escenario	Certeza V8	Certeza V3	Decisión	Nivel de certeza
Credencial auténtica con buena iluminación	0.92	0.88	Legítima	Conservador
Credencial auténtica con captura oscura	0.71	0.83	Legítima	Verificado
Fotocopia o impresión a color	0.31	0.22	Sospechosa	Ultra alta
Imagen de credencial mostrada en pantalla	0.45	0.39	Sospechosa	Ultra alta
Credencial auténtica con reflejos o ángulo pronunciado	0.63	0.78	Legítima	Análisis profundo
Reproducción física de alta calidad	0.55	0.48	Sospechosa	Alta

Estos ejemplos muestran que el sistema distingue casos evidentes y también identifica situaciones intermedias. Para fortalecer la validación futura, será conveniente complementar la medición productiva con métricas estandarizadas bajo ISO/IEC 30107-3.

4.3 Niveles de certeza y apoyo a la revisión humana

Además de la clasificación final, la plataforma entrega un nivel de certeza que facilita la interpretación operativa. Este nivel permite diferenciar casos claros de casos ambiguos y definir cuándo conviene automatizar una decisión o derivarla a revisión humana. La Tabla 5 resume el significado operativo de los principales niveles de certeza utilizados por el módulo documental.

Tabla 5. Niveles de certeza y significado operativo en la verificación documental.

Nivel de certeza	Significado operativo
Ultra alta	El sistema identifica un caso claro, generalmente asociado con una reproducción evidente. Puede procesarse automáticamente.
Alta	Existe alta confianza en la decisión. Se recomienda acción automática o revisión mínima según la política de la institución.
Verificado	Los modelos coinciden de forma favorable después del cruce de opiniones. Indica alta confiabilidad.
Análisis profundo	Los modelos presentan diferencias relevantes o el caso se ubica en una zona ambigua. Se recomienda revisión humana.
Media	El resultado no es concluyente. Conviene considerar evidencia adicional o revisión operativa.
Conservador	El sistema toma una decisión positiva, pero mantiene cautela por las condiciones de captura o el nivel de confianza observado.

Esta salida graduada evita respuestas puramente binarias y permite concentrar la revisión humana en casos de mayor incertidumbre o riesgo.

4.4 Discusión: valor del ensamble y eficiencia operativa

Los resultados sugieren que la doble opinión adaptativa aporta valor frente al uso de modelos individuales. En la ruta documental, V8 y V3 ajustan la decisión según zonas de confianza; en la ruta facial, el módulo especialista prioriza fraude y el generalista complementa cuando no hay indicios fuertes de suplantación. La Fig. 9 ilustra esta diferencia entre modelos individuales y ensamble. El uso de ensambles no elimina por completo los errores, pero mejora la robustez ante imágenes capturadas en condiciones variables. Además, los niveles de certeza ayudan a equilibrar dos riesgos: rechazar a una persona legítima o aceptar una reproducción. En conjunto, el valor de la plataforma no depende solo de la precisión de los modelos, sino de la integración entre desempeño técnico, interpretación operativa, revisión humana focalizada y viabilidad de despliegue.

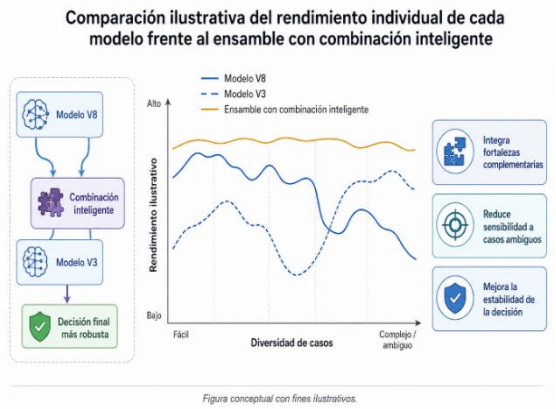

Fig. 9. Comparación ilustrativa del rendimiento individual de cada modelo frente al ensamble con combinación inteligente.

5 Conclusiones y trabajo a futuro

Esta sección sintetiza las aportaciones de la plataforma y plantea líneas de continuidad para fortalecer su validación, ampliar su alcance y responder a nuevas amenazas en identidad digital.

5.1 Conclusiones

Este capítulo presentó una plataforma de inteligencia artificial desarrollada en México para apoyar la validación remota de identidad mediante dos rutas complementarias: verificación documental de la credencial para votar y verificación facial contra ataques de presentación. La solución atiende un problema relevante en el contexto nacional, donde la digitalización de servicios exige mecanismos confiables para reducir riesgos de suplantación y fraude.

Su principal aportación es el uso de modelos de visión artificial combinados mediante estrategias adaptativas de decisión. En la ruta documental, los modelos V8 y V3 analizan la credencial desde perspectivas complementarias; en la ruta facial, MiniFASNet prioriza la detección de fraude y EfficientNet aporta una valoración adicional cuando no existen indicios fuertes de suplantación.

En operación productiva, la plataforma ha mostrado un desempeño cercano al 99% de acierto bajo esquemas de revisión continua. Además, sus niveles de certeza permiten automatizar casos claros y derivar a revisión humana aquellos con mayor incertidumbre. En conjunto, la solución demuestra el potencial de desarrollar en México aplicaciones de inteligencia artificial orientadas a problemas reales de alto impacto, con operación productiva, eficiencia computacional y utilidad social.

5.2 **Trabajo a futuro**

Como trabajo a futuro, se plantea realizar una evaluación formal bajo métricas estandarizadas de detección de ataques de presentación, particularmente conforme a la norma ISO/IEC 30107-3. Esto permitiría complementar la evidencia operativa actual con tasas de falsos positivos, falsos negativos y desempeño por tipo de ataque.

También se considera ampliar la plataforma hacia otros documentos de identidad, como pasaportes, licencias de conducir o cédulas profesionales, así como incorporar mecanismos de detección activa, por ejemplo, solicitar al usuario inclinar el documento o mover el rostro durante la captura.

Otra evolución relevante consiste en integrar ambos módulos de forma más estrecha, comparando el rostro de la selfie con la fotografía contenida en la credencial para votar. Finalmente, será necesario fortalecer la detección de amenazas emergentes, como deepfakes, rostros sintéticos y ataques generados mediante inteligencia artificial, para mantener la plataforma vigente ante nuevos escenarios de fraude digital.

Declaración de intereses. Los autores declaran no tener intereses en competencia que sean relevantes para el contenido de este capítulo.

Referencias

1. Tan, M., Le, Q.V.: EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks. In: Proceedings of the 36th International Conference on Machine Learning (ICML), pp. 6105–6114. PMLR (2019).
2. ISO/IEC: ISO/IEC 30107-1:2023. Information technology — Biometric presentation attack detection — Part 1: Framework. International Organization for Standardization, Geneva (2023).
3. ISO/IEC: ISO/IEC 30107-3:2023. Information technology — Biometric presentation attack detection — Part 3: Testing and reporting. International Organization for Standardization, Geneva (2023).
4. Galbally, J., Marcel, S., Fierrez, J.: Biometric Antispoofing Methods: A Survey in Face Recognition. IEEE Access 2, 1530–1552 (2014).
5. Instituto Nacional Electoral: Estadísticas Lista Nominal y Padrón Electoral. Instituto Nacional Electoral, México. Disponible en: https://ine.mx/credencial/estadisticas-lista-nominal-padron-electoral/. Consultado el 26 de abril de 2026.
6. Secretaría de Hacienda y Crédito Público; Comisión Nacional Bancaria y de Valores: Resolución que modifica las Disposiciones de carácter general aplicables a las instituciones de crédito. Diario Oficial de la Federación, México, 21 de mayo de 2021.
7. Dietterich, T.G.: Ensemble Methods in Machine Learning. In: Kittler, J., Roli, F. (eds.) Multiple Classifier Systems. MCS 2000. Lecture Notes in Computer Science, vol. 1857, pp. 1–15. Springer, Berlin, Heidelberg (2000).
8. Zhang, Y., Yin, Z., Li, Y., Yin, G., Yan, J., Shao, J., Liu, Z.: CelebA-Spoof: Large-Scale Face Anti-Spoofing Dataset with Rich Annotations. In: Vedaldi, A., Bischof, H., Brox, T., Frahm, J.M. (eds.) Computer Vision – ECCV 2020. Lecture Notes in Computer Science, vol. 12357, pp. 70–85. Springer, Cham (2020).
9. Yu, Z., Zhao, C., Wang, Z., Qin, Y., Su, Z., Li, X., Zhou, F., Zhao, G.: Searching Central Difference Convolutional Networks for Face Anti-Spoofing. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pp. 5295–5305 (2020).
10. Qi, D., Tan, W., Yao, Q., Liu, J.: YOLO5Face: Why Reinventing a Face Detector. arXiv:2105.12931 (2021).

11. González-Soler, L.J., Patino, J., Busch, C.: Face Morphing Attack Detection Using Deep Learning. In: Marcel, S., Nixon, M.S., Fierrez, J., Evans, N. (eds.) Handbook of Biometric Anti-Spoofing, pp. 383–410. Springer, Cham (2023).
12. Howard, A.G., Zhu, M., Chen, B., Kalenichenko, D., Wang, W., Weyand, T., Andreetto, M., Adam, H.: MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications. arXiv:1704.04861 (2017).
13. Secretaría de Relaciones Exteriores: Credencial para votar (INE). Consulado General de México en Boston, Secretaría de Relaciones Exteriores, México. Disponible en: https://consulmex.sre.gob.mx/boston/index.php/documentos-de-identidad/credencial-para-votar-ine. Consultado el 26 de abril de 2026.
14. Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros: Reclamaciones imputables a un posible robo de identidad entre las reclamaciones imputables a un posible fraude. CONDUSEF, México. Disponible en: https://www.condusef.gob.mx/documentos/com71_reclamaciones-robo-identidad.pdf. Consultado el 26 de abril de 2026.
15. Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros: CONDUSEF informa que durante enero de 2026 siete instituciones financieras informaron suplantación de identidad. CONDUSEF, México, 3 de marzo de 2026. Disponible en: https://www.gob.mx/condusef/prensa/condusef-informa-que-durante-enero-de-2026-siete-instituciones-financieras-informaron-suplantacion-de-identidad. Consultado el 26 de abril de 2026.