CASO DE USO

VIDEO IDENTIFICACIÓN AUTOMATIZADA

Alexandra OANE

27 de noviembre de 2022

ÍNDICE

Descripción del caso de uso

En el siguiente caso de uso tratará de ayudar a aquellas personas y empresas a agilizar trámites de transacciones financieras. Las empresas dispondrán de un proceso de identificación y contratación para evitar que las personas se deban desplazar hasta las oficinas físicas.

Nos enfocaremos en un software que nos permite identificar a personas a través de una video identificación.

Este tipo de casos se ofrecería a clientes como bancos, concesionarios de automóviles o grandes superficies comerciales.

El proceso constaría en que si un usuario o destinatario final quiere realizar la compra de un vehículo, solicitar un préstamo o financiar sus compras, nuestro cliente dispondrá de nuestro software por el cual se podrá identificar y realizar la firma de un contrato a distancia, sin la necesidad de que sus clientes se deban de desplazar.

Para verificar que nuestros procedimientos son totalmente válidos y dentro del marco legal, se dará un certificado con un sello que verificará la veracidad del mismo. Se necesitará de colaboración notarial o disponer de la misma autoridad.

Aunque nuestros clientes solamente soliciten solo la primera parte del proceso, se entregará de la misma manera un certificado haciendo que sea válida la identificación de aquellas personas que usen estos servicios.

El proceso de identificación se llamará video identificación, actualmente existen dos tipos de video identificación:

- Video identificación atendida
- Video identificación desentendida

Enfocando el caso de uso en la video identificación desatendida.

Los usuarios acceden a un enlace que será enviado por la empresa, con la que estén realizando una operación, al correo electrónico personal.

Al pulsar el enlace se debe introducir el número de documento de identidad, de la persona que se va a identificar. Primero se realizarán unas capturas del documento, por el anverso y el reverso (en los casos de DNI o NIE) y solo anverso en caso de ser un Pasaporte.

Tras realizar las capturas deberán realizar una pequeña sesión de grabación en la que se debe ver en todo momento a la persona que se identifica, sin gafas de sol, gorras o mascarillas. Debe decir su nombre y apellidos y volver a mostrar el documento de identidad.

Con este proceso si todos los valores del resultado salen correctamente, se dará por válido y se podrá continuar con el proceso de compra o financiación.

¿Cuál es el problema?

Los inconvenientes que presenta este caso de uso, es que se pueda engañar al programa y que se valide y autorice la continuación de la operación.

En el caso de que una persona quiere comprar un vehículo pero dispone de un documento robado o extraviado, y se “disfraza” para poder parecerse a la fotografía que el documento contiene, se pueden dar el caso de que los parámetros nos indiquen que todo es correcto, si la persona es parecida a la de la fotografía. Dicha persona estaría cometiendo un fraude, por ello a día de hoy obliga a que haya agentes que validan o rechacen este tipo de video identificaciones.

Los parámetros a tener en cuenta para los procesos de video identificación son los siguientes:

1. Veracidad del documento de identidad: debe ser un documento original siempre y físico.

2. La comparación de biometría facial: se realizará una comparación con la fotografía del documento de identidad y la persona que se está identificando.
3. Prueba de vida: el usuario debe decir su nombre completo y mostrar el documento como prueba de vida.

Estos tres parámetros principales se regirán por los siguientes valores:

80% o superior: se considerará válida.

Entre 50% y 80%: se considerará pendiente de revisión/dudosa.

Inferior al 50%: se considerará no válida/rechazada.

El software de video identificación, deberá poder extraer todos los datos del documento de identidad, los campos a extraer:

1. Nombre y apellidos.
2. Número de identificación personal.
3. Número del documento.
4. Fecha de nacimiento.
5. Fecha de emisión del documento.
6. Fecha de validez del documento.
7. Nacionalidad.
8. Sexo.
9. Domicilio.
10. Lugar de nacimiento.
11. Nombre de los progenitores.

Además de la lectura de las líneas MRZ de los documentos.

También se debe contar con un sistema de bases de datos de los documentos de identidad a nivel mundial, para que nuestro software sea capaz de identificar el tipo de documento, teniendo en cuenta las versiones que se vayan realizando para cada uno de ellos.

El programa además debe contener una detección de documentos manipulados o falsos (incluso siendo fotocopias o imágenes del documento en otro dispositivo).

El número de clientes a los que afecta el problema es elevado, teniendo en cuenta que serían entidades financieras, bancos o concesionarios de automóviles.

Los números de video identificaciones anuales por un solo cliente, en este caso se toma como referencia una entidad financiera , una cifra aproximádamente de 140.000/cada año, teniendo en cuenta que los fines de semana no se realizarán validaciones, serían 140.000/261 días = 537 video identificaciones diarias.

Este número elevado podría ser asumible por 7 agentes, teniendo en cuenta sus jornadas laborales de lunes a viernes, cada uno debería de atender 76 video identificaciones, pudiendo cometer errores.

Por ello se debe considerar en que el software pueda validar o rechazar de manera automática. Sin embargo, en los casos en que las video identificaciones sean dudosas, los parámetros anteriormente mencionados 1, 2 o los 3 nos hayan devuelto un porcentaje que se halla entre el 50% y el 80%, quedarían pendiente de revisión por una persona.

Así de esta manera solamente se tendrán en cuenta para el proceso de revisión a 2 personas.

El coste de que un usuario final se identifique a través de nuestra plataforma es mucho menor que si el cliente realizará todo el proceso presentándose en una oficina de manera física. Se ahorrará en gastos de notario, económicos, de papel, siendo más respetuosos con el medio ambiente y de tiempo. Se agilizan los procesos y se pueden realizar video identificaciones y firmas el mismo día.

El precio que se debería poner por video identificación desatendida sería de 4€.

Teniendo en cuenta que sólo se ha empleado el ejemplo de uno de los posibles clientes que es donde se considera que puede haber mayor número de posibles usuarios.

Los ingresos que se generarían con un un solo cliente siendo una entidad financiera sería de 560.000€ anuales.

Los beneficios son mayores, con menor coste y más seguridad para nuestros clientes ya que de esta manera se evitarán casos de fraude.

¿Cómo se está afrontando ahora?

Actualmente para este tipo de procesos se están empleando agentes para evitar validar una video identificación que sea un fraude. El factor humano sigue siendo necesario, ya que si se realizaran pruebas desde distintos dispositivos con los diferentes tipos de documentos identificativos, tendríamos ciertos casos en que daría error, y podría dar por válida una video identificación en la que el usuario ha mostrado una fotocopia plastificada.

En este tipo de casos un agente puede verificar más detenidamente si el documento es real, analizando el video. Sin embargo, si se presentara un documento falso, reproduciendo un documento auténtico, sería mucho más complicado detectar incluso en un proceso físico y manual debido a técnicas muy avanzadas que se emplean para crear documentación falsa.

¿Acción que buscamos poder hacer para solucionar el problema?

Para solucionar el problema de posibles fraudes se debe establecer los parámetros que deben indicar si se puede dar por válida o debe ser rechazada.

- Ataque de impresión (print attack): fotocopia simple de documento
- Ataque de repetición (replay attack): foto o escaneo del documento en otro dispositivo.
- Manipulación de los datos impresos en el documento.
- Manipulación de los códigos QR o bidi.
- Sustitución de fotografías.

KPIs - Indicadores de negocio

Las soluciones que se implementan durante el proceso de identificación es necesario para garantizar la seguridad de la operación para nuestro cliente. Por

ello, aunque se automatice el 98% del sistema siempre tendremos revisando a un agente para el 2% de aquellas video identificaciones que sean dudosas.

¿Cuáles son los mínimos que se esperan de este caso de uso?

En los casos de posibles fraudes se esperan que haya un número de personas que trate de identificarse con un documento falso, un documento robado, una fotocopia o mostrar un documento en otro dispositivo. Este número no es elevado, con el proceso de video identificación se puede detectar, no el 100% de los casos pero sí el 99%, en este caso contamos con la posibilidad de que el usuario haya presentado un documento falso.

Incluso en este tipo de casos, como se ha mencionado anteriormente, si el usuario se presentará en una oficina de manera física y mostrará el documento de identidad, el trabajador no tendría todos los medios necesarios para detectar si se trata de un documento real o creado de manera ilegal.

Validación: ¿Qué criterio se va a usar para decidir si la solución es aceptable?

Los tipos de situaciones en los que se daría mayor fraude serían temporadas altas de ventas. Se debe analizar con cada de nuestros clientes sus fechas de mayor solicitudes de crédito, en el caso de las entidades financieras.

Consideramos que en los meses de noviembre, diciembre, junio y julio. Hay mayor volúmen de solicitud de préstamos en este tipo de épocas del año.

Dentro de nuestras predicciones consideramos que un mínimo de 2 personas al año podrían engañar a nuestros sistemas y llevar a cabo una operación con una falsa identidad.

Los casos imposibles de detectar son aquellos, en los que una persona puede manipular y obligar a una persona mayor a solicitar un préstamo. Es decir, cometería un delito de cohesión y manipulación, es ilegal obligar a una tercera persona a realizar una operación en su nombre sin su consentimiento o bajo amenaza.

Por ello las personas de la tercera edad son más vulnerables a este tipo de situaciones.

También tenemos en cuenta los posibles casos de que un hacker tratara de acceder al enlace enviado a un usuario de nuestro cliente. Sin embargo existen medidas para ello como por ejemplo, poner un tiempo determinado de duración desde que se envía el proceso de video identificación, un máximo de 3 ó 4 días hasta que dicho enlace se cierra por tiempo expirado, aunque el usuario haya accedido al proceso pero no ha finalizado, si tratara de acceder después del tiempo establecido de vida del enlace, no podría acceder dando un error de acceso denegado.

Se ha implementado también el tiempo de vida total de la video identificación desde que el usuario inicia el proceso, un máximo de 20 min, para que nadie tenga tiempo de acceder al mismo tiempo durante la sesión.

Se cuenta también con la verificación de un código PIN enviado a través de SMS al número del usuario, asegurando de esta manera una barrera más de seguridad para evitar que un tercero se “cuele” en el proceso, pudiendo extraer datos de los usuarios que se están identificando.

Experimentación: ¿Cómo vamos a corroborar el funcionamiento?

- Una vez hayamos recibido la video identificación en nuestros sistemas, con los resultados devueltos tras el análisis, se validará, rechazará o pasará a una de las pestañas donde se depositarán todas aquellas con resultados inferiores al 80% y superiores al 50%.

Estas últimas video identificaciones, considero que se deberían de rechazar, ya que como empresa especializada en identificación a distancia, se debe entregar un certificado con los porcentajes máximos posibles, para que no se pueda presentar dudas acerca de nuestro proceso. Y se deberían volver a lanzar de nuevo, para asegurarnos de que todo sale correctamente.

- Este tipo de revisiones se harán diariamente y semanalmente. Para evitar demoras en tiempo y tener un seguimiento continuo.
- El tiempo del que se dispondrá para poder verificarlo sería dependiendo de la cantidad de pruebas satisfactorias que se den.

Productivización: ¿Qué salida debe tener la solución que se desarrolle?

Se extraerán todos los datos de las video identificaciones: datos de nuestro cliente y datos del usuario, desde que el proceso sale de nuestros sistemas, todas las trazas y los nodos de tiempo, el documento con el que ha realizado la identificación, el dispositivo, fecha y hora, sistema operativo del dispositivo, marca y modelo y todas las acciones que se realizaron durante dicho proceso, quedará registrado en nuestros sistemas.

Antes de que nuestros clientes se integren o empleen nuestro proceso de video identificación, se realizarán las pruebas necesarias en un entorno Demo, para evitar errores en los entornos de producción.

Al realizar todas estas pruebas con distintos ejemplos que nuestro cliente quiera emplear, se obtendrán resultados para cada una de las pruebas.

EQUIPO DE TRABAJO

Identificación de personas colaboradoras

Las personas que sean encargadas de esta parte del proceso, deberán estar formados y mantener un contacto constante con el departamento correspondiente

de nuestros clientes. Es muy importante mantener la comunicación ya que se puede detectar antes un caso de posible fraude.

Un agente con una formación básica y necesaria no podría detectar a simple vista si la video identificación ha sido manipulada, para ello se debe añadir un equipo de soporte técnico, que puedan verificar que el proceso ha tenido un flujo adecuado y ha finalizado correctamente.

DETALLE DEL CASO DE USO

Detalle funcional

El producto principal que se quiere destacar de nuestros procesos, es la video identificación. El cliente puede elegir que el usuario solamente se identifique a través de nuestros sistemas y realizar la firma de manera física o con otra empresa, o puede elegir el proceso completo, los usuarios primero se identifican y luego firman el documento, a través de un código PIN para verificar al destinatario final.

Esta facilidad que podemos ofrecer a nuestros clientes, supone un mayor beneficio para ellos en costes a la hora de facilitar este avance a sus clientes.

Los usuarios pueden realizar la operación que deseen en cualquier momento del día y desde otro país, sin la necesidad de realizar todos los trámites que anteriormente se realizaban y la cantidad de tiempo que podían llegar a emplear para este tipo de operaciones.

Además se ofrece una mayor seguridad, ya que nuestros sistemas son capaces de detectar el mayor número de fraudes, evitamos que terceros se agreguen al proceso y puedan realizar la sustracción de datos.

Para la video identificación nos debemos regir por la Ley 10 del 2010 de prevención de blanqueo de capitales, el cliente si elige la video identificación desatendida estará obligado a seguir todas las indicaciones de dicha ley.

Identificación de orígenes de datos

Para este tipo de operaciones, anteriormente mencionado, se debe hacer un análisis inicial con el cliente, ya que en función de sus números de años anteriores podremos proporcionarle una respuesta.

Nuestro sistema es capaz de recibir más de 500 video identificaciones diarias y poder ofrecer un informe diario o semanal completo de las transacciones realizadas.

También se debe establecer un tiempo de custodia de las transacciones en nuestros sistemas, ya que al cumplir el tiempo máximo establecido, para consultar operaciones antiguas se deberán tener unos permisos para poder acceder a la información. Es información muy sensible y queremos garantizar la mayor seguridad a nuestros clientes y cumplir con la ley en protección de datos.

DESARROLLO DEL CASO DE USO

Puntos intermedios o seguimiento

En este punto se puede dar la posibilidad de que un usuario pueda tener dificultades para realizar la video identificación. Como por ejemplo:

- El dispositivo móvil no está actualizado y da error en la versión del navegador.
- El usuario trata de acceder a la video identificación pero no puede recibir el código PIN porque tiene mala cobertura de red.

- El usuario trata de identificarse con un documento que no está establecido por el emisor.
- El usuario trata de identificarse con un documento que no contiene fotografía
- El usuario trata de identificarse con un documento deteriorado, en mal estado o todo.
- El usuario trata de identificarse con un documento caducado (por la ley que nos regimos no está admitido identificarse con el documento de identidad caducado aunque el usuario presente una denuncia del documento extraviado o que se está a punto de renovar).
- El usuario trata de identificarse con un documento sin chip, en casos de DNI/NIE. Por la ley que nos regimos tampoco es válido presentar un documento sin chip.
- El usuario está tratando de identificarse en un ambiente con poca iluminación y mal enfoque y no consigue finalizar correctamente.

Todos estos casos son posibles pérdidas de clientes para nuestro cliente. Ya que si una persona no dispone de un documento de manera física, ya que en algunas oficinas se pueden presentar fotocopias y son válidas o identificarse con un documento de identidad caducado y te permitirán continuar con la operación, luego el cliente en general toma las medidas necesarias. Como ejemplo, solicitar un préstamo con el DNI caducado, se concede y luego se bloqueará la cuenta bancaria del usuario hasta presentar el documento en vigencia.

Con nuestros procesos se tratará de evitar este tipo de situaciones consideradas como ilícitas.

Se tendrán en cuenta aquellos casos, en los que los usuarios nos comuniquen que no pueden acceder a la video identificación o que están teniendo problemas para finalizar, y nuestro cliente lance varias transacciones para un mismo cliente. Si el

usuario no consigue realizarla puede comunicar que no quiere continuar con la operación que presenta muchas dificultades con la tecnología.

Para este punto también se ofrecerá un tipo de soporte técnico, en casos de mayor necesidad, ya que sería imposible asistir a todos los usuarios.

Hasta el momento nada está automatizado, ya que en el sector público se halla la video identificación atendida, sin embargo, desde mi punto de vista de varios casos no garantiza seguridad alguna. También otras empresas la tienen implementada y tienen casos que demuestra que no es segura.

La video identificación se puede automatizar, pero no al 100%, sigue presentando errores y por ello debe intervenir el factor humano para aquellos casos en los que no nos devuelva los parámetros esperados.

Para estas mejoras que se han propuesto se deben realizar más pruebas y mejoras necesarias al software. Que este sea capaz de detectar y cerrar automáticamente en caso de estar sufriendo un posible ataque al proceso.

Aporte esperado por Big Data

Considerar que la video identificación desatendida se automatice se trata de resolver y mejorar con la propuesta anteriormente expuesta.

El aporte por parte del equipo de Big Data, será la extracción y clasificación adecuada de los datos obtenidos.

Se deberá recoger adecuadamente dichos datos ya que sería necesario comprobar con otras bases de datos.

En los casos de un documento de identidad robado, una persona trata de identificarse con dicho documento, se debería poder comprobar y comparar que el documento no se halle en una situación similar.