

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 374 221**

51 Int. Cl.:
B60R 25/00 (2006.01)
B60R 25/10 (2006.01)
B60R 25/04 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **06758051 .4**
96 Fecha de presentación: **11.07.2006**
97 Número de publicación de la solicitud: **1904347**
97 Fecha de publicación de la solicitud: **02.04.2008**

54 Título: **MÉTODOS Y DISPOSITIVO PARA LLEVAR A CABO LA VERIFICACIÓN DE IDENTIDAD DE UN CONDUCTOR.**

30 Prioridad:
11.07.2005 US 697564 P

45 Fecha de publicación de la mención BOPI:
14.02.2012

45 Fecha de la publicación del folleto de la patente:
14.02.2012

73 Titular/es:
VOLVO TECHNOLOGY CORPORATION
S-405 08 Göteborg, SE

72 Inventor/es:
LARSSON, Petter;
HAGERMANN, Andreas y
BJÖRK, Hanna

74 Agente: **Isern Jara, Jorge**

ES 2 374 221 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Métodos y dispositivo para llevar a cabo la verificación de identidad de un conductor

5 SECTOR DE LA INVENCION

La invención se refiere a métodos y a un dispositivo para llevar a cabo la verificación de la identidad de un conductor.

10 ANTECEDENTES DE LA INVENCION

15 La industria del transporte sufre problemas de hurtos y robos de artículos valiosos. Diferentes temas de seguridad han pasado a ser un asunto de máxima importancia en todo el mundo, especialmente dado que las amenazas del terrorismo parecen intensificarse. Una forma de incrementar el nivel de seguridad podría ser, disponer de un sistema de verificación montado en vehículos comerciales para asegurar que el conductor es el adecuado.

20 El documento DE 43 26 514 A1 da a conocer un dispositivo electrónico anti-robo para vehículos que, gradualmente, deja inactivo un vehículo a motor si tiene lugar un robo, hurto o ataque, si el conductor no puede demostrar su autorización al introducir un número de identificación personal (PIN). La investigación controlada por el sistema de seguridad electrónico para demostrar la identificación tiene lugar a intervalos determinados durante el desplazamiento o a lo largo de la ruta mientras el vehículo está siendo utilizado. Si el conductor no puede demostrar su identidad dentro de un periodo determinado de tiempo de respuesta, la velocidad del vehículo disminuye por etapas hasta llegar al paro, sin poner en peligro el tráfico, al actuar en el control electrónico del motor, y entonces, al llegar a encontrarse el vehículo estacionario queda bloqueado, de manera que no puede circular nuevamente ni ser remolcado al actuar en el sistema de freno, actuando también en otros sistemas electrónicos del conjunto motriz, si existen.

30 El documento DE 10156 731 A1 da a conocer un método y un aparato para la verificación de conductores autorizados de un vehículo. Los datos biométricos del conductor a verificar son determinados antes y/o durante la conducción del vehículo, y son comparados con datos de referencia. Si no hay correspondencia entre los datos biométricos medidos y los datos de referencia, un sistema de control de funcionamiento autónomo toma el control del vehículo.

35 El documento US 2004078118 A1 da a conocer un dispositivo para el control de un mecanismo que coopera con un operador humano, en el que el mecanismo comprende un dispositivo de seguridad adyacente al mecanismo, que puede interactuar con un elemento activador dotado de medios de memoria y asociado con un operador humano específico, autorizado, pudiendo funcionar el mecanismo solamente después de la interacción con el elemento activador.

40 El documento US 2002/0048391 A1 da a conocer un sistema de identificación de huellas dactilares para un vehículo a motor, que comprende una unidad de ajuste de la modalidad de ignición, un panel de correspondencia y una unidad de control del motor. La unidad de ajuste de la modalidad de ignición identifica una modalidad de ignición, escanea y lee una huella dactilar como dato de entrada, y ajusta y borra una huella dactilar registrada. El panel de correspondencia almacena la huella dactilar registrada y compara la huella dactilar de entrada con la huella dactilar registrada para emitir una señal de salida. La unidad de control del motor recibe la señal de salida para emitir una señal de control para controlar un mecanismo de bloqueo/liberación de la llave y un mecanismo de bloqueo/liberación del volante.

50 En una aplicación, los eventos a controlar pueden ser almacenados en medios de memoria del elemento de activación, por ejemplo, para controlar vehículos a motor con respecto a tiempos de conducción, inaceptablemente largos, de un conductor determinado. En otra aplicación, los medios de control de un avión son supervisados para asegurar que el avión puede volar solamente por medio de un piloto autorizado. Las características corporales invariables del conductor o piloto o, por ejemplo, las huellas dactilares, son almacenadas en el elemento activador. Las características reales del cuerpo son detectadas por sensores y son comparadas con las almacenadas. El vehículo o avión puede ser utilizado solamente si las características detectadas y las características almacenadas del cuerpo son idénticas.

60 El documento US 5.686.765 A da a conocer un sistema a utilizar en un vehículo automóvil que tiene un sistema de ignición normalmente desactivado. El sistema comprende un dispositivo lector, tal como un lector de huellas dactilares o un lector de retina para identificar al conductor. La señal de salida del lector es comparada con datos fisiológicos correspondientes, almacenados en la memoria para determinar si el conductor está autorizado para controlar el vehículo. De manera opcional, un temporizador es utilizado para permitir el funcionamiento del vehículo solamente durante periodos de tiempo prescritos que se hayan predeterminado.

Un objetivo de la invención consiste en proporcionar métodos y sistemas flexibles, fáciles de utilizar, no intrusivos, seguros contra falsificaciones, para la verificación de conductores de camiones. Otro objetivo consiste en dar a conocer métodos y sistemas de verificación y/o identificación similares.

5 El objetivo es conseguido mediante las características de las reivindicaciones independientes.

La aplicación tiene dos objetivos. Uno consiste en encontrar métodos apropiados para la verificación del conductor y para constituir un prototipo de sistema de verificación que puede ser utilizado para la comprobación y el desarrollo posterior. El otro consiste en estudiar de qué forma los conductores de camión perciben dichos sistemas y de qué forma su constitución se corresponde con la demanda creciente de mayor seguridad. La aplicación está dirigida a la industria del transporte.

Se estudiaron once métodos de verificación disponibles. Para posibilitar una selección bien fundamentada en métodos para implementar un prototipo, encuestas y entrevistas con conductores de camiones y contratistas de transporte fueron llevadas a cabo para complementar el estudio teórico.

Se escogieron para una prueba, un método de verificación normal y tres métodos de verificación biométrica; verificación de huellas dactilares, reconocimiento fácil, reconocimiento de voz, y código PIN. Estos métodos fueron reunidos en un sistema que fue implementado en un simulador de conducción de camiones. Un interfaz de usuario gráfico fue desarrollado para hacer el sistema más aceptable por el usuario. 18 conductores de camión probaron el sistema de verificación. Fueron entrevistados de modo completo antes y después de la prueba a efectos de captar sus antecedentes, expectativas y opiniones.

La mayor parte de los participantes de la prueba tuvieron una actitud positiva frente al sistema. Aunque no sintieron que fuera necesario en aquel momento, creyeron que "era el futuro". No obstante, algunos participantes se encontraron incómodos con el sistema puesto que se sintieron controlados por el mismo. Quedó evidente lo importante que es tener un sistema que respeta la intimidad del usuario, y asegurar que los usuarios están bien informados con respecto a la forma en que se utiliza el sistema. Una parte de la tecnología utilizada para el sistema de verificación requiere más desarrollo para encajar en el contexto de la automoción, pero se considera que es posible conseguir un sistema consistente y seguro.

RESUMEN DE LA INVENCION

Tal como se describirá en mayor detalle a continuación, se han realizado una serie de invenciones en el curso de la investigación descrita y análisis de sistemas de verificación del conductor.

En, como mínimo, una realización, la invención adopta la forma de un método para asegurar que el conductor de un vehículo es el conductor autorizado. Este método se logra por la utilización de un sistema multimodal de identificación del vehículo, montado a bordo del vehículo, utilizado para asegurar si el conductor es el conductor autorizado. Un primer proceso de identificación del conductor es llevado a cabo en el conductor del vehículo y se determinan si él o ella es un conductor autorizado o no autorizado del vehículo. Normalmente, la prueba solamente confirmará si la persona objeto de la evaluación es un conductor autorizado. Si el proceso de identificación no confirma que él o ella es el autorizado, se asumirá y actuará como si se hubiera confirmado que no están autorizados. Con independencia del resultado del primer proceso de identificación, a continuación, se lleva a cabo un segundo proceso de identificación del conductor en el conductor y posteriormente se intenta, determinar si él o ella es un conductor autorizado o no autorizado. El primer y segundo procesos de identificación del conductor son llevados a cabo con un intervalo de tiempo entre ambos, y este intervalo de tiempo depende de la naturaleza del trabajo llevado a cabo por el conductor. Por ejemplo, el intervalo entre las confirmaciones de identificación será diferente para conductores de suministro urbano, que hacen frecuentes paradas y entradas/salidas del vehículo, en comparación con conductores de largo recorrido que hacen solamente unas pocas paradas durante el día y que presentan muchas menos oportunidades de que conductores no autorizados puedan llegar a conducir el vehículo. Finalmente, se realizarán medidas correctoras (correcciones) para evitar un impacto potencialmente negativo cuando el conductor actual del vehículo se determina que es un conductor no autorizado basándose en, como mínimo, uno de los procesos de identificación realizados. Si bien el camión no será llevado a una parada inmediata en base al fallo del ID del conductor como conductor autorizado, tales cosas como las notificaciones a la oficina central pueden ser afectadas telemáticamente o se puede impedir que el vehículo vuelva a arrancar después de que el conductor haya hecho la parada siguiente.

Se prevé que los procesos de identificación del conductor pueden ser diferentes uno de otro, o similares.

La identificación del segundo conductor puede ser iniciada inmediatamente después de una determinación de si el conductor es un conductor no autorizado en el primer proceso de identificación del conductor.

De manera alternativa, el proceso de identificación del segundo conductor puede ser llevado a cabo solamente cuando no se puede determinar que el conductor es un conductor autorizado basándose en la realización del procedimiento de identificación del primer conductor.

En, como mínimo, una realización, uno de los procesos de identificación es una prueba de identificación pasiva que no requiere interacción consciente por el conductor, en asociación con la realización de los procesos de identificación del conductor. En un ejemplo, la prueba de identificación pasiva comprende el escaneado de una característica física del conductor, a partir de la que se compara una imagen a un conjunto de imágenes de control representativo de conductores autorizados del vehículo.

Como mínimo, uno de dichos primer y segundo procesos de identificación del conductor es una prueba de identificación activa que requiere interacción consciente por el operador en asociación con la realización de, como mínimo, uno de los procesos de identificación del conductor. Un ejemplo sería la colocación de un dedo o una mano en un escáner. De manera alternativa, la prueba de identificación activa puede incluir la emisión de una petición al conductor de que introduzca un número de identificación personal en el sistema que identifica el conductor como conductor autorizado. Otra forma de prueba de identificación activa comprende de la lectura de información de codificación ("hard-coded") en una tarjeta de identificación presentada por el conductor. El sistema puede requerir entonces que el conductor introduzca un número de identificación personal en el sistema que corresponde al número de identificación ("hard-coded") leído de la tarjeta de identificación. De manera similar, la prueba de identificación activa puede comprender la emisión de una instrucción al conductor de que articule una frase predeterminada, registrando la frase como modelo de voz y comparando este modelo con un conjunto de modelos de voz de conductores autorizados del vehículo.

En una variante del desarrollo de la invención, el primer y segundo procesos de identificación son de dos tipos diferentes entre sí, y son llevados a cabo con intervalos de tiempo al azar entre ellos.

En otro aspecto de la invención, se da a conocer un sistema de verificación automatizado que aprecia que uno de los temas por los que los expertos en factores humanos luchan en esta área es cuándo y cómo se debe verificar un conductor. Dado que la utilización de vehículos comerciales difiere en la aplicación, algunos conductores pueden salir y entrar de su vehículo veinte veces al día, mientras que algún conductor puede hacerlo solamente dos o tres veces al día. A efectos de mantener un nivel de seguridad suficientemente elevado, sin que el sistema sea molesto para el conductor, se pueden utilizar varias estrategias distintas. Una de ellas es llevar a cabo una verificación automática mientras se lleva a cabo la conducción. Por ejemplo, un reconocimiento facial (verificación) puede ser llevado a cabo durante la conducción sin que el conductor sea consciente de ello. Si esta prueba falla, se puede sugerir al conductor que introduzca su código PIN o se puede utilizar otro método. La verificación puede ser llevada a cabo con intervalos al azar.

En otro aspecto inventivo, si un vehículo está equipado con varios métodos de verificación, con ellos se puede solicitar al conductor que utilice diferentes métodos en diferentes momentos. Si la elección del método y tiempo se hace al azar, el conductor no tendrá forma de saber cuándo o cómo verificarse a sí mismo, la implementación de este tipo de falta de predicción en el sistema incrementa el nivel de seguridad puesto que un impostor no sabría cuándo o cómo tendría que verificarse a sí mismo.

En otro aspecto de la invención, se aprecia que en sistemas biométricos no es la propia (imagen) biométrica la que se verifica (correspondencia), sino un modelo o plantilla de la imagen biométrica; es decir, se extrae un modelo o plantilla de la biometría medida y se compara con un modelo o plantilla existente en la base de datos. Uno de los problemas con la correspondencia, con respecto a un modelo almacenado (o la propia medición biométrica), es el hecho de que la biometría de una persona puede variar a lo largo del tiempo, mientras que el modelo almacenado no varía. Por ejemplo, la huella dactilar de una persona puede variar debido a una cicatriz, o bien una palabra clave de voz debido a enfermedad o a la edad. Una solución a este problema consiste en actualizar el modelo (de forma manual o automática). Una actualización automática puede ser conseguida por un sistema de verificación multimodal, es decir, un sistema de verificación que utiliza más de un conjunto de biometría/código PIN/tarjeta inteligente. Entonces, se pueden utilizar uno o varios métodos de verificación para verificar el conductor, mientras que uno de estos métodos no utilizado actualiza su modelo (si el proceso de verificación ha sido satisfactorio). A título de ejemplo, el conductor entra en su vehículo y recibe la sugerencia de identificarse utilizando su código PIN, huella dactilar y reconocimiento facial. El sistema lo verifica utilizando el código PIN y el reconocimiento facial, y utiliza la biometría de la huella dactilar para actualizar el modelo de la huella dactilar de la base de datos.

En un aspecto relacionado con el modelo biométrico de la huella dactilar, un tema crucial es dónde almacenar el modelo. Básicamente, existen tres alternativas: (i) una base de datos en el camión; (ii) una base de datos en la oficina central (requiere comunicación en tiempo real entre el vehículo y la oficina central); y/o (interconexión) de una base de datos que el conductor lleva consigo, tal como una tarjeta inteligente. Una opción consiste en utilizar la tarjeta digital de tacógrafo del conductor para almacenar modelos de verificación. La tarjeta es una tarjeta inteligente, y por lo tanto, es adecuada para este tipo de almacenamiento, pero lo más importante es algo a lo que el conductor está obligado por la ley (por lo menos, en Europa) y por lo tanto, el conductor la lleva en todo momento.

En otro aspecto inventivo, la redundancia es instituida en la apreciación de la incertidumbre típicamente relacionada a sistemas de verificación de identificación conocidos. La realización de un método de reconocimiento

facial puede ser afectado, por ejemplo, por las condiciones de luz. Con la utilización de varios métodos (por ejemplo, reconocimiento facial y código PIN) la redundancia se consigue en el sistema. Por ejemplo, un conductor está conduciendo por la carretera y se lleva a cabo un reconocimiento facial automático programado y éste falla por alguna razón (las condiciones de luz pueden ser malas, u otro similar). El conductor recibe entonces la sugerencia de verificarse a sí mismo utilizando la huella dactilar y el código PIN.

Finalmente, se debe apreciar que cada uno de los aspectos descritos anteriormente, solo o en combinación, puede ser implementado en un contexto telemático. Es decir, el sistema de verificación puede informar/recibir información y similares a/desde una oficina central o una red de seguridad a nivel de empresa/nivel nacional/nivel internacional. Por ejemplo, se puede evitar que los expresidarios puedan transportar artículos peligrosos al verificar sus datos biométricos detectados con respecto a una base de datos nacional/internacional de delincuentes.

BREVE DESCRIPCIÓN DE LA INVENCION

La presente invención, junto con los objetivos antes mencionados y otros, y así como sus ventajas, se podrá comprender mejor a partir de la descripción detallada siguiente de las realizaciones, en las que se muestra esquemáticamente:

- Figura 1 etapas de registro/correspondencia de usuarios en los métodos de verificación más habituales;
- Figura 2 huella dactilar con crestas y valles que forman un modelo que se caracteriza por líneas irregulares e incoherentes;
- Figura 3 varios tipos de características distintas a analizar en una huella dactilar, por ejemplo, bucles, arcos y espirales;
- Figura 4 un escáner capacitivo para escanear un dedo;
- Figura 5 un método RD para escanear la huella debajo de la superficie real de la huella dactilar;
- Figura 6 un escáner de iris;
- Figura 7 un iris escaneado;
- Figura 8 una termografía facial para el reconocimiento facial, con utilización de una cámara de infrarrojos, un modelo térmico, fundado en el modelo de vasos sanguíneos faciales de la persona, que es único para cada persona;
- Figura 9 una imagen de la retina para el reconocimiento de una retina;
- Figura 10 formación de la imagen de la retina;
- Figura 11 escáner de la geometría de la mano que mide la longitud de los dedos, anchura, grosor, y curvatura;
- Figura 12 esquema general de un sistema de verificación implementado, mostrando con flechas la forma en la que las diferentes partes se comunican entre sí;
- Figura 13 imagen de partes del sistema montado en el camión;
- Figura 14 dos ejemplos de interfaz gráfico de usuario;
- Figura 15 imagen de un simulador;
- Figura 16 imagen de un simulador;
- Figura 17 esquema de prueba con una verificación inicial completa con un paro para tomar café, seguido de una breve verificación, utilizando una huella dactilar o voz y otra verificación mientras se efectúa la conducción;
- Figura 18 gráfico de la puntuación promedio de cada participante con respecto a utilidad y satisfacción;
- Figura 19 gráfico con respuestas de participantes antes y después de la prueba;
- Figura 20 tabla de huellas dactilares como método de verificación;
- Figura 21 tabla de escaneado de iris como método de verificación;
- Figura 22 tabla de verificación de voz como método de verificación;
- Figura 23 tabla de reconocimiento facial como método de verificación;
- Figura 24 tabla de termografía facial como método de verificación;
- Figura 25 tabla de escaneado de retina como método de verificación;
- Figura 26 tabla de exploración de movimientos de labios como método de verificación;
- Figura 27 tabla de reconocimiento de geometría de la mano como método de verificación;
- Figura 28 tabla de claves de PIN y escaneado como método de verificación;
- Figura 29 tabla de tarjetas como método de verificación;
- Figura 30 tabla de RFID como método de verificación; y
- Figura 31 tabla de estadísticas de la escala de aceptación de "van der Laans".

DESCRIPCIÓN DETALLADA

Los temas de seguridad reciben una elevada prioridad en todo el mundo. Esto ha afectado también a la industria del automóvil, lo cual ha dado lugar a la pregunta de si sería posible incrementar la seguridad al implementar un sistema de verificación del conductor en vehículos comerciales. Las cuestiones que serán exploradas en esta descripción son, por ejemplo, qué tipo de verificación utilizar y a quién beneficiaría este sistema. Esta sección contiene antecedentes, un objetivo, y las restricciones a la presente aplicación. Para conseguir un resumen de la aplicación, esta sección cuenta con una guía de lectura.

Debido a las crecientes amenazas terroristas, se llevan a cabo grandes inversiones en investigación y desarrollo, a efectos de aumentar la seguridad en la sociedad. El Departamento de Seguridad Nacional (Department of Homeland Security) (USA) es un ejemplo de este esfuerzo. Sin tener en cuenta la forma en que es presentada, la seguridad es un tema que ha pasado a ser cada vez más importante, especialmente después de los ataques terroristas contra el World Trade Center en 2001. Ya se han introducido muchos cambios en la legislación, especialmente en USA. Por ejemplo, existe una propuesta de legislación de que todos los camiones que lleven mercancías peligrosas deben tener un sistema de verificación biométrica del conductor. Esto es debido a que el gobierno de Estados Unidos desea impedir que los delincuentes (según los registros del FBI) sean conductores de mercancías peligrosas. Las demandas de un sistema de verificación flexible, seguro y fiable son, por lo tanto, elevadas dado que hay unos 8 millones de conductores profesionales de camiones en Estados Unidos. La UE (Unión Europea) junto con otras asociaciones y países, también han hecho grandes inversiones en investigación de seguridad y gestión de crisis.

Un ejemplo de las exigencias crecientes de seguridad es que varios aeropuertos, como por ejemplo, el aeropuerto de Amsterdam Schiphol y el aeropuerto de Umeå, en Suecia, han probado la utilización de la verificación biométrica de sus pasajeros. Después de un año de actuación piloto en 2001, un sistema de paso de frontera automático, que utiliza reconocimiento de iris, es actualmente permanente en el aeropuerto de Ámsterdam de Schiphol.

Para atender las exigencias del mercado y los cambios de la legislación, nuevos productos tienen, frecuentemente, sistemas de seguridad más avanzados que los productos anteriores, utilizando técnicas más avanzadas de identificación y de verificación. Un ejemplo es el de las libretas de notas con escáneres de huellas dactilares incorporadas.

El contrabando, ataques terroristas, y robos de mercancías valiosas son escenarios que comportan habitualmente vehículos robados. La industria del transporte es, por lo tanto, un segmento natural a estudiar a efectos de mejorar la seguridad pública. Una idea central, cuando se incrementa la seguridad en el transporte, consiste en verificar que el conductor es el mismo que se indica.

La invención combina dos competencias distintas y resulta en una prueba de posibles técnicas que pueden ser adecuadas para la identificación del conductor, pero también en una evaluación de las opiniones del conductor sobre el sistema. Las entrevistas y encuestas indicarán las opiniones del conductor antes y después de comprobar un prototipo. La comparación entre lo que significa la seguridad para el interesado/los fabricantes y la forma como se corresponde con los conceptos de capacidad de utilización, seguridad e intimidad del conductor, será llevada también a cabo.

VENTAJAS DEL SISTEMA DE VERIFICACIÓN DEL CONDUCTOR

Se utilizan los camiones para varias finalidades. Por lo tanto, se requiere un sistema flexible que pueda adaptarse a situaciones variadas. Por lo tanto, se presenta múltiples retos cuando se tiene que diseñar un sistema de este tipo. Es deseable cumplir las máximas exigencias posibles, aunque es imposible constituir un sistema universal. A continuación, se muestran algunas situaciones variadas, en las que podría ser ventajosa la identificación del conductor.

En América del Sur, hay problemas importantes con vehículos robados. Esto ha llevado a un proceso común por el que, cuando se transportan artículos de valor, el conductor llama a la compañía de seguro cada 10 minutos para asegurar que todo está conforme. Si un vehículo está dotado de un sistema de verificación, el sistema podría asegurar de manera continuada a la compañía de seguros que el vehículo ha sido conducido por el conductor apropiado, permitiendo, por lo tanto, que el conductor se centre en su conducción.

Un sistema de verificación podría permitir que un contratista de transportes se asegurara de que el conductor no ha sido sentenciado previamente por mala conducta en el tráfico. Para almacenar la información con respecto a los conductores, se requeriría una base de datos. Si la base de datos estuviera conectada con las autoridades, se podría llevar a cabo una comprobación del archivo, casi a tiempo real.

Un contratista de transportes, que tiene simultáneamente un dispositivo de verificación del conductor y un vehículo con un dispositivo de bloqueo por alcohol montado en el mismo, podría recibir una "marca de conductor de confianza". Entonces, los clientes estarían asegurados de que sus mercancías son transportadas por un conductor "de confianza". La cooperación con la asociación nacional de la carretera y las empresas de seguros podría tener como resultado costes de seguro de vehículo más reducidos.

Una ventaja adicional para la utilización de un sistema de verificación podría consistir en que los conductores de confianza, verificados, podrían ser favorecidos en el paso de estaciones de pasada o estaciones de peaje. Esto facilitaría la labor para los conductores y haría el transporte más eficaz.

Una verificación, asociando los parámetros registrados de un conductor específico, podría controlar si alguno conduce durante más tiempo de las 4,5 horas legisladas (legislación europea) sin un descanso. En este caso, se podría enviar un aviso al conductor y también al contratista del transporte.

5 En Suecia, se han dado casos de desestimación, debido al hecho de que los acusados se han culpado entre sí. En el caso de un accidente o delito, un sistema de verificación podría asegurar a los investigadores de quién conducía realmente el vehículo en aquel específico momento.

10 Si un vehículo ha sido robado y existe demanda de verificación, el impostor no llegará lejos, hasta que el sistema revele el robo. Esto permite tomar medidas más rápidas si el vehículo ha estado involucrado en un delito.

15 Las aduanas Suecas tienen un proceso llamado "Servicetrappan" (escalera de servicio) a efectos de simplificar el proceso de aduanas para empresas de confianza. El proceso consiste en una serie de etapas de calificación. Cuanto mayor es la calificación de la empresa, más fácil es el paso a través de las aduanas. Un sistema de verificación del conductor podría formar parte de este proceso, ofreciendo a los contratistas de transporte con conductores, verificados y de confianza, un rango más elevado y, por lo tanto, un paso más eficaz por las aduanas.

20 Además, si existe un sistema de verificación en el camión, el conductor se podría beneficiar del mismo, dado que sería posible adecuar automáticamente los ajustes del puesto de conducción de acuerdo con las preferencias personales del conductor. Por ejemplo. Los ajustes para el asiento del conductor, control del clima, y estéreo, se podrían ajustar automáticamente. Esto se encuentra, no obstante, fuera del objeto de esta invención.

25 Hay dos objetivos principales con la presente aplicación. Uno consiste en encontrar métodos apropiados para la verificación del conductor y para construir un prototipo de un sistema de verificación que puede ser utilizado para la comprobación y el desarrollo posterior. El otro objetivo consiste en estudiar la forma en la que los conductores perciben este sistema y cómo su concepto se adapta a la demanda creciente de una mayor seguridad.

30 Estos objetivos se pueden resumir del modo siguiente: "Estudiar las posibilidades de utilizar métodos de verificación disponibles para diseñar un sistema de verificación del conductor de un camión con seguridad contra impostores, que no es intrusivo, que es fácil de utilizar, y que es flexible".

Si bien, los métodos de verificación que se describen pueden ser utilizados en casi cualquier tipo de vehículo, la preferencia de esta aplicación será de los camiones comerciales y la industria del transporte.

35 Se implementarán tres métodos biométricos y se comprobarán en el prototipo. La selección del método se basará principalmente en la teoría de lo que se ha explicado durante el trabajo, pero el precio y el tiempo de suministro también afectarán a las decisiones.

40 Un GUI ha sido desarrollado para facilitar la comunicación entre el sistema de verificación y el usuario. No obstante, no se mencionará teoría alguna con respecto a la ciudad del usuario y diseño, dado que el autor que ha desarrollado el GUI poseía ya los conocimientos de antemano. Además, es el sistema, no el GUI, aquel al que se enfoca esta invención.

45 Un sistema de verificación en un vehículo abre muchas posibilidades para aumentar la seguridad. Algunas de las cuestiones que se investigarán son el tipo de verificación a utilizar y a quién beneficiará este sistema. No obstante, el tema de seguridad no es el único tema a considerar cuando se construya este sistema de verificación. La intimidad del conductor y conceptos de seguridad deben ser tomados también en cuenta. Estos diferentes enfoques llevan a diferentes soluciones al problema, diferentes perspectivas de seguridad, seguridad e intimidad se explican, por lo tanto, en esta descripción. Todo ello sirve también para clarificar lo que significan estos términos y mostrar porqué es importante para esta invención.

SEGURIDAD

55 Hay diferentes tipos de seguridad, tales como seguridad personal, de empresa, pública, y de país. Todos estos aspectos hacen difícil dar una sola definición. Un concepto comúnmente aceptado, no obstante, es que la seguridad consiste en las calidades o medidas tomadas para reducir la probabilidad de que ocurran incidentes no deseados.

60 Los temas de seguridad, dentro de esta tesis, incluyen todas las aplicaciones mencionadas anteriormente. La seguridad pública y la seguridad de país son temas a considerar cuando se tengan en cuenta los riesgos de ataques terroristas. Los riesgos, junto con el transporte de mercancías peligrosas, afectan también a la seguridad pública. El riesgo de vehículos robados se dirige a la seguridad de la empresa. Finalmente, la seguridad personal se dirige a los riesgos y también a las ventajas que pueden proceder de la implementación de un sistema de verificación del conductor. Estos diferentes temas se explicarán más adelante.

65

INTIMIDAD

El objetivo principal de un sistema de verificación consiste en aumentar el nivel de seguridad. Una forma de hacerlo es utilizar métodos biométricos. El problema es que, en sí mismos, constituyen una amenaza puesto que se pueden constituir como amenaza a la intimidad de una persona. Por lo tanto, la intimidad del usuario es otro tema que se tendrá que tomar en cuenta.

La intimidad se puede definir como el derecho a tener un espacio personal para proteger la propia individualidad y para ser capaz de mantener ciertas cosas para uno mismo, sin exposición a las autoridades públicas, superiores u otros. Los métodos biométricos pueden proporcionar un sentimiento de una vigilancia global del tipo “Gran Hermano” (tal como en “1984” de George Orwell). En este caso, los métodos se podrían percibir como violaciones de la intimidad de una persona.

SEGURIDAD

La protección y la seguridad no son exactamente lo mismo, aunque están íntimamente relacionadas. La seguridad se puede definir como el caso o la situación en la que una persona puede hacer algo sin tener temor de que pueda ocurrir algo indebido. Una buena protección puede resultar, por lo tanto, en una percepción de seguridad.

Aunque todos los métodos ofrecen seguridad en su utilización, una persona puede no desear utilizarlos si los percibe como intrusivos o cree que pueden dañarle de algún modo. El concepto que el usuario de un sistema debe ser tomado en consideración, porque, con independencia de lo seguro que es un método, una persona que no confíe en él no lo utilizará. No importa si el conductor ha usado un método o no, siempre tendrá sus propias opiniones con respecto al mismo. No obstante, su concepto no está siempre de acuerdo con los hechos y la realidad. Por ejemplo, el escaneado de iris se considera uno de los métodos más exactos y también un método seguro en su utilización, pero a muchas personas no les gusta la idea de utilizar un sistema que explora los ojos. Una persona que teme que este escaneado pueda dañar los ojos, no percibirá el sistema como seguro.

Las cosas desconocidas, frecuentemente, infunden temor a las personas, por lo tanto, la información es importante dado que el conocimiento puede disminuir los sentimientos negativos. Tal como se ha indicado anteriormente, las personas tienden a creer que el escaneado es un método de verificación poco confortable, pero una prueba llevada a cabo en la empresa SAS demostró otra cosa. Evaluaron dos sistemas de verificación distintos en el aeropuerto de Umeå, las huellas dactilares y el escaneado de iris. Pasajeros frecuentes formaron parte de la prueba y utilizaron la verificación de huellas dactilares la mitad del tiempo, y el escaneado del iris la otra mitad. La mayor parte de los participantes era positiva en cuanto a la utilización de biometría (78% creyó que SAS debería introducir la verificación biométrica de los pasajeros) y, en este caso, el escaneado del iris se calificó ligeramente más alto que la verificación de las huellas dactilares. Esto significa que los usuarios tienen que ser convencidos de que el sistema es beneficioso para ellos y para su trabajo; de otro modo, podrían no estar de acuerdo en su utilización.

VERIFICACIÓN DEL CONDUCTOR APROPIADO PARA EL VEHÍCULO

Hay muchos métodos distintos de verificación en el mercado actual, alguno de ellos se encuentran ya en utilización, otros lo estarán pronto. A pesar de ello, no hoy en día no se verifica quién está realmente en un vehículo. La intención de ello es introducir algunos de los diferentes métodos para la verificación y relacionar sus ventajas y desventajas desde el punto de vista de la automoción y también del usuario. La sección comprende una introducción a la biométrica y descripciones de diferentes métodos biométricos. Los PIN (números de identificación personal), palabras clave y diferentes tipos de tarjetas, son también métodos de verificación. Dado que se utilizan frecuentemente en la actualidad, se supone que son bien conocidos por el lector y, solamente, se mencionarán brevemente en esta descripción.

Una ventaja general de todos estos métodos, es que el usuario tiene que parar su tarea habitual para llevar a cabo la verificación. Esto aumenta la conciencia de riesgo y puede influir al usuario para que ponga más atención y cuidado.

INTRODUCCIÓN A LOS MÉTODOS BIOMÉTRICOS

La palabra biometría tiene origen en el latín y se puede traducir en “medición de la vida”. La biometría se refiere usualmente a estudios estadísticos de las características de organismos vivos que pueden ser medidas. Por otra parte, la biometría es más bien utilizada para el análisis para identificar seres humanos por medición de sus características. Los métodos biométricos han sido utilizados para la identificación y verificación desde finales del siglo 19. Cuando se hace referencia a métodos de verificación/identificación biométrica en esta invención, ello significa métodos que analizan una o varias características exclusivas del cuerpo de una persona, tal como manos, cara u ojos.

El método más apropiado de verificación varía dependiendo dónde y por qué se va a utilizar. No obstante, hay tres exigencias fundamentales que se deben atender para decidir el método a utilizar. Para conseguir el método ideal

de verificación, la característica a medir debe ser única, ello significa algo característico de aquel individuo; algo permanente, lo que significa que no debe variar a lo largo del tiempo, y finalmente debe ser también universal, lo que significa que todo el mundo debe tenerla. La aceptabilidad, así como la accesibilidad de las características analizadas por un método, deben ser también tomadas en consideración. Una característica biométrica es aceptable si su medición no se percibe como intrusiva por el usuario. Si una característica es fácil de presentar a un sensor, esa característica se designa como accesible.

Básicamente, hay tres formas por las que una persona se puede identificar a sí misma; tener algo, por ejemplo una tarjeta de acceso; saber algo, por ejemplo una palabra clave o un PIN, ser alguien, utilizando métodos biométricos para la identificación.

La mayor parte de los diferentes métodos que se describen pueden ser utilizados, tanto para la verificación como para identificación, pero se debe observar la distinción entre los dos términos.

15 Identificación Cuando se utiliza un método para averiguar quién es una determinada persona dentro de un grupo grande, ello se llama identificación. A ello se hace referencia como “comparación de uno a muchos”. Significa la búsqueda dentro de un grupo grande para hallar un individuo que corresponde a la característica utilizada para la identificación.

20 Verificación Cuando se utiliza un método para analizar si una persona es quién dice ser, ello se llama verificación. A ello se hace referencia en algunos casos como “comparación uno a uno”. En este caso, es necesario solamente comparar la característica de una persona con respecto a los datos que se han almacenado a nombre de esa persona.

25 Esta invención se enfocará en la verificación desde que el conductor se supone que es conocido por la empresa. El sistema es utilizado, por lo tanto, solamente para verificar que es el conductor realmente esperado el que lleva a cabo la conducción.

30 Existen una serie de ventajas que hacen que la utilización de métodos biométricos de verificación sean dignos de consideración; las características biométricas no pueden ser olvidadas; los atributos físicos no pueden ser colocados equivocadamente; los atributos físicos son más difíciles de falsificar que las tarjetas de identidad; los modelos de huellas dactilares y otras características biométricas no pueden ser averiguadas o rebeladas tan fácilmente como, por ejemplo, una palabra clave.

35 Un problema con los sistemas de seguridad biométricos es la extensión de los daños que puede provocar, en el caso de que alguien logre realmente robar la información de identidad. Si una persona pierde una tarjeta de identidad o si alguien encuentra el PIN secreto para poner en marcha la alarma de robo, es siempre posible conseguir una nueva tarjeta o cambiar el código. No obstante, si las huellas dactilares de una persona son copiadas, es imposible conseguir otras nuevas. La persona no sería ya capaz de utilizar sus huellas para la verificación dado que siempre habría el riesgo de que otra persona dijera que es él.

40 En el caso de robos, es importante actualizar las bases de datos involucradas y registrar elementos de identidad robados, de manera que un impostor eventual no las pueda utilizar. Uno de los secuestradores del 11 de Septiembre de 2001 utilizó un pasaporte robado a un ciudadano saudí en Estados Unidos cinco años antes. Con una base de datos actualizada, esto podría, quizás, haber sido evitado. Si los pasajeros, haciendo referencia nuevamente a 2001, hubieran tenido también la necesidad de identificarse biométricamente, habría sido más difícil que los terroristas hubieran logrado su propósito. No obstante, los métodos de verificación biométrica no son la solución perfecta. Un impostor puede atacar la base de datos o la conexión entre la base de datos y el escáner a efectos de puntear o manipular el sistema. Por lo tanto, aunque el objetivo es encontrar una solución suficientemente segura, es imposible eliminar por completo todos los riesgos.

PROCESO DE VERIFICACIÓN

55 Esta sección proporcionará una visión general de los métodos de verificación más habituales. Muchos de ellos utilizan las siguientes etapas de registro/correspondencia de los usuarios, según la figura 1.

- Captación de Datos** El sensor escanea el sujeto.
- 60 Pre-proceso de señal** Por ejemplo, eliminando ruidos ambientales en un sistema de reconocimiento de voz.
- Extracción de la característica** Analizar las diferentes características y crear una plantilla o modelo basado en un subconjunto de los datos captados.
- 65 Registro/correspondencia** Añadir el modelo a la base de datos (registro) o compararla con modelos que ya se encuentran en la base de datos (correspondencia).

Decisión

Una correspondencia satisfactoria autoriza al individuo, el fallo rechaza la autorización.

5 Los modelos se realizan principalmente por dos razones. Una consiste en reducir la cantidad de datos almacenados y la otra es la de reducir la complejidad de la siguiente fase de correspondencia. Otra ventaja de los modelos consiste en, si se utiliza por ejemplo un escáner de huellas dactilares, que no se almacena la imagen completa de la huella, sino un modelo de una característica única. Esto hace difícil utilizar el modelo para reproducir la huella.

10

DETECCIÓN VITAL

Un impostor puede intentar utilizar un engaño o eliminar el dedo del usuario autorizado para pasar un escáner de huellas dactilares.

15 Lo mismo se puede decir del escaneado de iris y de la geometría de la mano. Algunos sistemas de reconocimiento de voz pueden ser manipulados por una grabadora de cinta y un sistema de reconocimiento de cara por una fotografía de un usuario autorizado. No obstante, hay medidas para evitar estos casos. Un sistema de verificación biométrica puede ser dotado de detección vital para asegurar que la muestra recogida procede de un ser humano. La detección vital tiene que adecuarse al método de verificación. Por lo tanto, se explicará la forma en la que se puede implementar la detección vital para cada método.

20

MÉTODOS BIOMÉTRICOS PARA VERIFICACIÓN

El procedimiento básico para los sistemas de verificación, ha sido explicado anteriormente en esta sección. Descripciones de varios métodos de verificación biométrica distintas: su historial, forma en qué funcionan, ventajas y desventajas que tienen, se explicarán a continuación.

25

VERIFICACIÓN DE HUELLAS DACTILARES

30 Las huellas dactilares son, probablemente, el método de identificación biométrica más extendido y bien conocido. A finales del siglo 19 y principios del siglo 20 se desarrollaron varios tipos distintos de métodos de identificación. Normalmente, estos métodos llevan a cabo un cierto tipo de clasificación por jerarquización, referente a unos pocos modelos principales. Observando la huella dactilar, las crestas y los valles forman un determinado modelo que se caracteriza por líneas irregulares y poco coherentes. Los escáneres actuales son muy rápidos y exactos, y el método empieza a resultar aceptado para utilización corriente (ver figura 2).

35

La comparación de la impresión completa requiere mucho tiempo de proceso y, por lo tanto, los aparatos de escáner se centran usualmente en características especiales, por ejemplo, el lugar en el que las crestas terminan o se dividen en dos. Estas características se designan como indicios o "minutiae". Los escáneres utilizan algoritmos complejos para averiguar y analizar estos indicios, a efectos de hacer la comparación. La idea básica consiste en medir las posiciones relativas de los indicios, de la misma manera que se reconoce una parte del firmamento por las posiciones relativas de las estrellas. Existen varios tipos de características distintas de la impresión, a efectos de análisis, por ejemplo, bucles, arcos y espirales (ver figura 3).

40

45 Los sistemas de búsqueda automática actuales se llevan a cabo habitualmente utilizando algoritmos de datos para clasificar y comparar un nuevo modelo codificado a partir de la huella dactilar escaneada, con una colección de plantillas almacenadas.

45

Los escáneres de huellas dactilares son principalmente ópticos o capacitivos, aunque existen otras tecnologías, tales como radiofrecuencia (RF), ultrasonidos, o dispositivos de escáner de silicio.

50

Un escáner óptico es básicamente una pequeña cámara digital que usualmente toma una imagen invertida de la huella dactilar para determinar si la imagen es suficientemente satisfactoria.

55 Si la imagen es demasiado oscura o demasiado brillante, el escáner cambia automáticamente el tiempo de exposición para permitir que entre más o menos luz antes de tomar una nueva imagen.

55

Un escáner capacitivo utiliza un conjunto de pequeñas placas, cada una de ellas menor que la anchura de una cresta, y conectada a un amplificador inversor. Cuando se coloca el dedo sobre el escáner, el dedo y las placas forman un condensador simple. Una carga de referencia es enviada a las placas, provocando que los condensadores se carguen. Dependiendo de la distancia entre las placas y el dedo (si es una cresta o un valle), el amplificador correspondiente presentará un voltaje distinto. Estos voltajes forman la "imagen" de la huella dactilar. Esto hace más difícil utilizar un simple papel con una imagen en blanco y negro de la imagen para desorientar al escáner capacitivo. Además, los dispositivos de escáner capacitivos se pueden hacer más pequeños que los ópticos (ver figura 4).

60

65

Una tecnología de escaneado de huellas dactilares, desarrollada recientemente, es el escaneado RF, que utiliza una señal de radio de baja energía para escanear la impresión. La RF tiene la ventaja de que escanea la impresión por debajo de la superficie real de la huella dactilar y, por lo tanto, es menos sensible a la suciedad, averías, y defectos (ver figura 5).

5 Otra distinción a realizar cuando se explican los dispositivos de escáner es la que existe entre un escáner de barrido y un escáner de área. En un escáner de barrido, el dedo es arrastrado por delante del sensor, mientras que en un escáner de área, el dedo es colocado sobre un sensor y mantenido en esta posición hasta que el escaneado se ha terminado. La mayor parte de los escáneres actuales son sensores de área, pero este modelo tiene algunos inconvenientes. El sensor se ensucia. Esto no afecta solamente al comportamiento del escaneado; muchas personas tienen repugnancia en la colocación del dedo sobre un sensor sucio. Existen problemas con las imágenes latentes. Esto significa que la imagen escaneada anteriormente permanece en la superficie del sensor y se reactiva durante el escaneado en la segunda huella dactilar.

15 El individuo puede colocar el dedo oblicuamente sobre el sensor. La mayor parte de dispositivos de escáner no toleran un ángulo de rotación superior a 20-30 grados.

Los sensores (particularmente, sensores capacitivos) tienen un coste por unidad de área. Un sensor de área en un escáner de barrido se puede hacer más pequeño y, por lo tanto, menos oneroso.

20 El escáner de barrido tampoco es una solución perfecta. Los temas principales son que habitualmente se requiere un cierto tiempo para conseguir una técnica de barrido correcta, y que las pasadas deben ser reconstruidas formando una huella dactilar, lo que puede ser engorroso en cuanto al tiempo. Por lo tanto, existen muchos parámetros distintos a considerar cuando se escoge un escáner para circunstancias específicas. Por lo tanto, es un tema importante el determinar la técnica de sensor a utilizar.

25 Un escáner óptico puede ser confundido por una imagen de la impresión, y un escáner capacitivo por un molde. Un molde puede ser realizado a base de gelatina, silicona, o incluso plastilina ("play-doh"). Para crear un molde, se requiere el dedo real. Sin embargo, para obtener una imagen que pueda confundir un escáner óptico, es suficiente disponer de algo que haya tocado la persona específica, tal como un vaso, para crear una imagen de la huella dactilar de dicha persona. Por lo tanto, el escáner óptico es más fácil de confundir. Hay otros numerosos métodos para confundir o engañar al sistema, tal como luces de destellos, calor, humedad, o diferentes tipos de materiales en polvo. No obstante, estos métodos para confundir el sistema son inútiles si el escáner está dotado de lo que se llama detección de vitalidad.

35 La detección de vitalidad puede ser llevada a cabo por una serie de maneras; analizando la temperatura, pulso, flujo sanguíneo, oximetría del pulso, resistencia eléctrica, EGG, permisividad dieléctrica relativa, deformaciones de poros o de la piel, o combinaciones de estos. Los métodos de detección de vitalidad son más o menos fáciles de obviar. Un problema principal es que el escáner determine si la impresión escaneada es parte del dedo, una imagen delgada como una hoja, o un molde fijado a la huella dactilar. Un nuevo método que utiliza la sudoración podría ser la solución, pero este se encuentra en desarrollo y, por lo tanto, no es posible indicar si realmente funciona bien.

40 Cada uno de los diez dedos tiene una huella única, lo que hace posible utilizar cualquier dedo a efectos de verificación. Los gemelos idénticos pueden tener huellas dactilares similares, pero no idénticas, dado que incluso los gemelos tienen sus huellas dactilares exclusivas. Se dice que una persona deja, como mínimo, veinticinco huellas dactilares perfectas cada día, y un problema principal con las huellas dactilares es que éstas se pueden copiar muy fácilmente.

50 Muchas personas ponen inicialmente su dedo en posición incorrecta sobre el escáner, dado que suponen que sus huellas dactilares se encuentran en la punta de los dedos, cuando en realidad el dedo debe ser colocado un poco más abajo para proporcionar una imagen que pueda ser procesada a efectos de verificación. Algunos dispositivos escáner están diseñados para facilitar el posicionado correcto del dedo utilizando, por ejemplo, salientes o rebajes de guiado.

55 Se debe observar que no todas las personas pueden utilizar este método; en realidad, llega al 5% las que tienen huellas dactilares que no pueden ser leídas por dispositivos escáner de huella dactilar. Las cicatrices, callos, u otros defectos afectar al resultado y hay personas que pueden tener los bordes y los valles tan delgados o dañados que la resolución del escáner no es suficientemente satisfactoria. Además, aunque la mayor parte de personas considera este método no intrusivo, algunas tienen aversión al escaneado de las huellas dactilares debido a las asociaciones que se pueden realizar de tipo forense.

60 Aunque se dice que cada dedo tiene una huella dactilar única, se detectan dos modelos principales en el 98% de todas las observaciones, lo cual aumenta el riesgo de equivocaciones. En la actualidad, el examen visual tradicional ha sido sustituido por la automatización. Se han producido errores cuando se tiene que identificar una

65

persona de la que únicamente se dispone de la huella dactilar. Sin embargo, cuando se plantea el verificar la identidad de una persona en una base de datos delimitada, se trata de un método muy fiable.

ESCANEADO DEL IRIS

5 El principio de este método se formuló en 1936, aunque no se aplicó hasta los años 1990. Toda la biométrica comercial del iris que existe en la actualidad se deriva de algoritmos realizados por el profesor John Daugman en 1994.

10 Un escáner de iris toma una imagen del ojo utilizando una cámara digital normal. La imagen es habitualmente de 120 píxeles de radio y el resultado es habitualmente una imagen de 8 bits de un iris. Cuando se capta la imagen, la primera etapa en el proceso de creación del modelo consiste en localizar la pupila y el iris. Después de ello, el anillo que tiene lugar cuando la pupila es recortada de la imagen es transformada en un disco utilizando una transformación polar. El programa de análisis utiliza entonces una serie de algoritmos para crear un modelo basado en las diferentes características (ver figura 6).

15 La detección de vitalidad puede ser implementada permitiendo que entre luz visible en el ojo y detectando si el tamaño de la pupila cambia o no. Esto requiere una fuente de luz muy potente o que la persona se encuentre muy cercana al escáner. Esta detección de vitalidad no se explicará, por lo tanto, adicionalmente, dado que no sería adecuada en un camión y, por lo tanto, se encuentra fuera del ámbito de esta solicitud de patente.

20 Existen más de 266 características independientes en el iris. El iris es único, no solamente para cada persona, sino también para cada ojo. Habitualmente, unas 170 de las 266 características se utilizan para formar el modelo a efectos de comparación. Otros métodos de verificación biométrica utilizan solamente desde 15 a un máximo de 35 características significativas independientes para el análisis. Por lo tanto, dado que existen tantas características en el modelo del iris, el método es muy fiable a efectos de verificación. Las características físicas, tales como nuestro aspecto facial y nuestra voz cambian a lo largo del tiempo, pero el iris, a parte de ciertas fluctuaciones de color en los primeros años, es invariable a lo largo de toda la vida humana. Esto es una gran ventaja puesto que no será necesaria la engorrosa actualización de la base de datos (ver figura 7).

30 Una prueba de la fiabilidad de estos métodos se puede encontrar en el sistema de reconocimiento de iris de los Emiratos Árabes Unidos, para impedir que los extranjeros expulsados puedan entrar nuevamente en el país. Se escanean, aproximadamente, 600 personas al día, y en la actualidad, la base de datos consiste en unos 355.000 iris. Se han realizado más de 1,6 millones de búsquedas hasta el momento, y no se ha detectado ninguna falsa correspondencia. El análisis estadístico del programa sugiere que la probabilidad de una correspondencia falsa es menor de 1 a 80 mil millones.

35 La tasa de registro es muy buena; todos los iris pueden ser analizados, excepto aquellas personas con ciertas dificultades de visión. Además, hay aplicaciones que captan automáticamente una imagen del iris, desde distancias que llegan a los tres pies, haciendo, por lo tanto, el proceso menos intrusivo.

No obstante, algunos sistemas tienen problemas en el escaneado de personas con ojos muy oscuros. Además, las lentes de color o bifocales pueden ser problemáticas, así como las lentes muy potentes.

45 Una desventaja del escaneado de iris es que todos los equipos son fabricados bajo licencia de Iridian Technologies Inc. Esta licencia hace que el equipo y, por lo tanto, el método en su conjunto, sean onerosos. Además, si el método tuviera que ser implementado en un vehículo, las condiciones de iluminación variables presentarían previsiblemente problemas. Si el fondo es demasiado oscuro, sería imposible un escaneado apropiado y lo mismo pasa para la iluminación directa dentro de la cámara. El problema de la luz solar se puede solucionar si la cámara se montara en el espejo retrovisor, protegiéndola de la luz directa del sol. Esto podría también incrementar las posibilidades de utilizar el escáner durante la conducción, dado que el conductor miraría al espejo regularmente. No obstante, esa solución es más adecuada para automóviles, dado que los camiones no tienen espejos retrovisores dentro de la cabina. Esa solución no es, por lo tanto, aplicable dentro de los límites de esta solicitud.

RECONOCIMIENTO DE VOZ

55 Este método identifica las personas basándose en las diferencias de su voz. La persona articula una frase previamente definida en el micrófono; el sistema capta la muestra de la voz y crea un modelo basado, por ejemplo, en la agudeza, cadencia y/o tono. El proceso es el mismo que para la verificación. La persona articulará la frase predefinida en el micrófono y el sistema extrae un modelo para compararlo con los modelos almacenados en la base de datos. Una ventaja de la utilización del reconocimiento de voz es que resulta difícil de engañar sin tener equipos de grabación/reproducción de alto rendimiento. La razón de ello es que el sistema de verificación de voz puede utilizar un micrófono que capta frecuencias no registrables, por ejemplo, por un dictáfono. Aunque la palabra clave o contraseña sería gravada satisfactoriamente para engañar al sistema, la frase hablada se podría alterar haciendo inútil la copia no autorizada. Además, se requeriría un sistema de reproducción sofisticado a efectos de reproducir todas las frecuencias de manera apropiada. La necesidad de equipos de alto rendimiento se puede apreciar como

un tipo de detección de vitalidad.

Una desventaja del reconocimiento de voz es que los modelos de voz requieren más espacio de almacenamiento que otros tipos de información biométrica. Como consecuencia, la verificación de voz puede requerir más tiempo que otros métodos, debido a la mayor cantidad de datos a analizar. Esto puede ser enojoso para el usuario dado que tendría que esperar la verificación. Otro problema es que la salud, estado emocional, fatiga y edad son factores que afectan las características de la voz de una persona. Por lo tanto, no se puede confiar en la verificación de voz como único método de autorización.

10 RECONOCIMIENTO FACIAL

Un método que ha recuperado atención últimamente es el reconocimiento facial. Alphonse Bertillon de la policía de París formuló el primer modelo para identificación visual en 1883. Su sistema fue llamado antropometría y se basaba en varias mediciones anatómicas complicadas de las dimensiones de la cabeza, longitud de un dedo, la altura de la cara y características especiales, tales como el color de los ojos, cicatrices y el color del pelo. Este método no era fiable y fue sustituido por otro por las huellas dactilares. Recientemente se han llevado a cabo pruebas con cámaras de vigilancia en Inglaterra a efectos de identificar delincuentes. Estas pruebas han demostrado que es muy difícil identificar personas de esta manera, especialmente si la cámara no consigue una imagen clara o si la persona ha alterado sus características, por ejemplo con barba o gafas. A pesar de la falta de resultados fiables para la identificación, el método funciona satisfactoriamente a efectos de verificación.

El principio es simple y similar al análisis utilizado en los métodos de verificación anteriormente descritos. Una imagen de la cara del sujeto es tomada y analizada con un ordenador para encontrar características destacadas tales como las cuencas de los ojos o las esquinas de la boca. Los resultados del análisis se almacenan en un modelo. Cuando se intenta verificar una persona se toma una imagen y se crea un modelo basándose en la nueva imagen. El nuevo modelo se hace corresponder con el que está almacenado en la base de datos. Un ordenador personal actual puede comparar el modelo con miles de modelos de una base de datos en menos de un segundo.

Hay diferentes técnicas para extraer características significativas de la imagen, tales como el filtrado Gabor o las llamadas caras propias o "eigenfaces". Estas técnicas son bastantes complicadas y dado que no es esencial para el objetivo de esta invención el describirlas en detalle, el lector interesado podrá acudir a las referencias que se indican para conseguir más información.

Una ventaja con el reconocimiento facial es que las personas tienden a encontrar este método cómodo, dado que estudia la cara de una persona lo cual es lo mismo que los humanos hacen para identificarse entre sí. Para conseguir resultados más exactos, el reconocimiento facial puede ser utilizado conjuntamente, por ejemplo, con el movimiento de los labios y el reconocimiento de la voz. Se han llevado a cabo investigaciones intentando mejorar los algoritmos para identificación facial para conseguir estabilidad contra el envejecimiento, condiciones de iluminación o expresión facial.

No obstante, en la actualidad no existe una solución absoluta y la base de datos necesitaría ser actualizada de manera continua.

Una decisión importante a realizar cuando se considera el reconocimiento facial es qué tipo de cámara se debe escoger; una cámara digital normal o una cámara de infrarrojos? Cuando la cámara utiliza rayos infrarrojos, el método es llamado termografía facial (ver la sección siguiente).

TERMOGRAFÍA FACIAL

La termografía facial es un tipo especial de reconocimiento facial. Con la utilización de una cámara de infrarrojos se puede ver un modelo térmico basado en los vasos sanguíneos faciales de una persona. Este modelo es único para cada persona y es difícil de falsificar (ver figura 8).

Una cámara de infrarrojos funciona aproximadamente de igual manera que una cámara ordinaria, siendo la diferencia el que es sensible a la luz infrarroja que es una radiación electromagnética en un intervalo aproximadamente de 760 nm – 0,5 mm. Esto hace la luz infrarroja invisible al ojo humano. Se debe observar que la luz visible es también una forma de radiación electromagnética, pero de diferente longitud de onda que la luz infrarroja. La luz infrarroja es designada en algunos casos radiación térmica y es emitida por todos los objetos con una temperatura superior a cero absoluto. Por lo tanto, la cámara consigue una imagen de la temperatura del objeto. Dado que diferentes partes de la cara tienen diferente temperatura debido a la forma de la cara y a las variaciones de flujo sanguíneo, ello se puede utilizar para verificación.

Aunque la termografía facial analiza el modelo térmico facial de una persona, no diferencia en modo alguno si la persona se encuentra en reposo, haciendo ejercicio o al aire libre. Se ha demostrado mediante estudios que las cámaras IR son bastante insensibles a estas circunstancias. Otra ventaja es que el escaneado es independiente de las condiciones de la luz visual, dado que la cámara funciona en el intervalo de la longitud de onda de infrarrojos y,

por lo tanto, es "ciega" a la luz visible.

Se han realizado comparaciones entre la utilización de cámaras normales con respecto a cámaras IR para verificación facial, que en su mayor parte han sido favorables a las cámaras IR, puesto que son independientes de las condiciones de iluminación. No obstante, un problema con las cámaras IR es que las gafas de cualquier tipo son completamente opacas a las mismas. Esto significa que el área alrededor de los ojos puede provocar problemas si la persona lleva usa gafas o si la persona lleva habitualmente gafas y se las quita sin actualización de la base de datos.

10 ESCANEADO DE LA RETINA

El reconocimiento de la retina fue formulado en los años 19, pero no fue hasta los años 80 en los que la tecnología fue desarrollada suficientemente para hacer el método comercialmente viable. El escaneado de la retina es un método rápido y muy exacto que utiliza láser para analizar el modelo de vasos sanguíneos de la retina. Cuando se toma la imagen de la retina, el sistema habitualmente almacena un modelo basado en las características extraídas de la imagen de manera similar a los métodos anteriormente mencionados (ver figura 9).

El escaneado de la retina se considera que es el método de verificación biométrica más exacto, puesto que el modelo de los vasos sanguíneos es único para cualquier persona y no cambia a lo largo del tiempo. La vasculatura de la retina desaparece en segundos si el sujeto deja de vivir, asegurando, por lo tanto, que la imagen captada ha sido obtenida de un ser humano vivo. Se ha demostrado mediante estudios que, aunque la retina no es fácil de escanear, el tiempo necesario para conseguir la imagen de la retina es menor que el tiempo requerido para la formación de una imagen de una huella dactilar. (Ver figura 10).

La cámara debe tener elevada resolución y el método requiere una alineación precisa del ojo para ser capaz de efectuar el escaneado. La captación de la imagen se puede efectuar desde una distancia que llega a los tres pies. No obstante, no es seguro en qué condiciones ambientales son válidas estas cualidades.

30 RECONOCIMIENTO DEL MOVIMIENTO DE LOS LABIOS

La forma en que las personas mueven los labios al hablar difiere de una persona a otra, por lo tanto, se ha desarrollado un método de reconocimiento del movimiento de los labios. Mientras una persona habla se utiliza una cámara para tomar una serie de imágenes, (en sucesión rápida) de la boca y el área circundante. Se utiliza un ordenador para analizar el movimiento de pequeñas arrugas en el área alrededor de la boca. Estos movimientos son representados por un campo de vectores situado sobre la imagen. El campo de vectores es comparado con campos de vectores de la base de datos en analogía con otros métodos anteriormente indicados. El equipo utilizado es básicamente el mismo que para el reconocimiento facial.

El reconocimiento del movimiento de los labios no es suficientemente exacto para que sirva como método único de verificación. Se sugiere, por lo tanto, que se utilice conjuntamente, por ejemplo, con el reconocimiento de voz.

Un caso especial de reconocimiento de labios es lo que se llama reconocimiento de la sonrisa. Los movimientos musculares de la parte inferior de la cara, activados por la sonrisa, son diferentes de una persona a otra. Estos músculos son casi imposibles de controlar a voluntad y son visibles incluso si el sujeto intenta mantener una determinada expresión facial, evitando la risa. Dado que no hay sistemas funcionales en el mercado, no se comentarán adicionalmente.

45 RECONOCIMIENTO DE LA GEOMETRÍA DE LAS MANOS

Un escáner de geometría de la mano mide la longitud de los dedos, la anchura, grosor y curvatura. El sistema consiste en una superficie plana con una serie de salientes, una fuente de luz, un espejo y una cámara.

La mano es situada sobre la superficie plana, con la palma de la mano dirigida hacia abajo y los dedos guiados por los salientes. El espejo es utilizado para proyectar el lateral de la mano en la cámara y las imágenes conseguidas son analizadas (ver figura 11).

A diferencia, por ejemplo, de las huellas dactilares, las manos de una persona no son únicas. Por lo tanto, este método no puede ser utilizado para objetivos de identificación, sino meramente de verificación. De acuerdo con Lichtermann y otros, el reconocimiento de la geometría de las manos no es adecuado para objetivos de automoción debido a las dificultades de los equipos. Dado que el artículo fue escrito el año 2000, es razonable pensar que cinco años de desarrollo pueden haber disminuido las dimensiones de los equipos. No obstante, los sistemas de geometría de la mano necesitan todavía aproximadamente nueve pulgadas entre la cámara y la mano a efectos de captar una imagen adecuada para el análisis. Esto es demasiado para hacer el equipo adecuado para su montaje dentro de un camión.

TRAZOS BIOMÉTRICOS SENCILLOS

5 Trazos biométricos sencillos son, por ejemplo, la edad, sexo, altura, peso, raza y color del pelo y de los ojos. Estos datos biométricos son vagos y alguno de ellos pueden cambiar a los largo de la vida, siendo también más fáciles de falsificar, por ejemplo, que las huellas dactilares. Los datos biométricos sencillos no se pueden utilizar, por lo tanto, para identificación o verificación segura. No obstante, los datos biométricos sencillos pueden ser utilizados como complemento de otros métodos biométricos. Un control del peso se podría implementar en un vehículo como incremento del escaneado de las huellas dactilares.

10 **OTROS MÉTODOS DE VERIFICACIÓN**

15 Las personas han sido capaces de identificar otros seres humanos utilizando datos biométricos característicos durante un largo tiempo, pero las formas más comunes de confirmar la identidad en la actualidad son las tarjetas, transpondedores, contraseñas y los PIN (Personal Identification Number (“Número Personal de Identificación”). La mayor parte de personas están acostumbradas a estos métodos de verificación, pero para ayudar en la comparación de los diferentes métodos de verificación, se llevará a cabo una breve descripción de cada uno de los métodos.

CONTRASEÑAS Y PINS

20 Las contraseñas y los PIN no necesitan excesiva presentación. Se puede suponer que todas las personas que lean la presente solicitud de patente han utilizado ambos métodos cuando han accedido, por ejemplo a su ordenador, han retirado dinero de un ATM (Asynchronous Transfer Mode (“Modalidad de Transferencia Asíncrona”)) o han puesto en marcha su teléfono móvil.

25 La ventaja principal es que el sistema es muy sencillo. Un teclado y un ordenador es todo lo que se necesita. Otra ventaja es que es fácil de utilizar, las personas están acostumbradas al mismo y no lo consideran intrusivo.

30 Los inconvenientes son que los códigos y las claves pueden ser fácilmente copiados, robados u olvidados. Las personas tienden también a tener contraseñas relativamente simples de adivina, tales como el nombre de su perro o la edad de sus hijos. Esto podría hacer más fácil que un impostor pueda adivinar la contraseña real y, por lo tanto, pasar la verificación.

TARJETAS

35 Hay varios tipos de tarjetas para los objetivos de identificación/verificación. La diferencia entre ellas es la forma en la que se utiliza la tarjeta en el proceso de verificación.

40 Los permisos de conducir y otras tarjetas ID requieren que alguien realice visualmente la correspondencia entre la fotografía y la persona real.

Las tarjetas de acceso tienen una banda magnética para almacenar información y algunos tipos utilizan un PIN para verificar que la persona que tiene la tarjeta es el propietario legítimo. La banda magnética es leída por el ATM, terminal de acceso o registro de caja.

45 Una tarjeta inteligente es básicamente un ordenador sencillo con las dimensiones de una tarjeta de crédito. Tiene un microprocesador y una memoria incorporada en la tarjeta. Estas tarjetas son más versátiles que una tarjeta de crédito normal, puesto que se puede almacenar mucha más información en la memoria de la tarjeta inteligente que en una banda magnética. Es habitual utilizar un PIN para verificar que el poseedor de la tarjeta es el propietario legítimo. No obstante, el microprocesador de la tarjeta inteligente presenta posibilidades de implementar métodos más sofisticados, tales como la tecnología Match-On-Card™ desarrollada por Precise Biometrics. Esta tecnología implica que la correspondencia real es realizada por el ordenador en la tarjeta inteligente en vez de hacerlo un ordenador externo, tal como en el procedimiento normal.

IDENTIFICADOR POR RADIOFRECUENCIA (RFID)

55 El RFID es un método de almacenamiento y recuperación de datos desde una posición alejada utilizando dispositivos llamados etiquetas de RFID. Estas etiquetas son activas o pasivas. La diferencia entre ellas es que una etiqueta pasiva no tiene suministro de potencia. En vez de ello, capta potencia por inducción magnética a partir del dispositivo lector. Esto significa que una etiqueta pasiva debe ser mantenida cerca del dispositivo lector durante la lectura real, mientras que una etiqueta activa puede ser leída desde varios metros. Una etiqueta pasiva, debido a la falta de suministro de potencia, puede ser realizada más reducida que una etiqueta activa. Las etiquetas pasivas más pequeñas son aproximadamente de un cuadrado de 0,4 milímetros y con un espesor de un adhesivo, mientras que las tarjetas activas más pequeñas tienen básicamente el tamaño de una moneda.

65 Las etiquetas RFID pueden ser utilizadas para objetivos de verificación de la misma manera que las tarjetas. La diferencia principal es que se requiere simplemente mantener la etiqueta contra el escáner (etiqueta pasiva) o

llevarla suficientemente cerca del escáner (etiqueta activa) a efectos de realizar la verificación.

SISTEMAS DE VERIFICACIÓN MULTIMODAL

5 Un sistema de verificación biométrica multimodal consiste en dos o más métodos de verificación biométrica que funcionan conjuntamente. Un sistema que utiliza solamente un método es llamado unimodal. Al utilizar varios métodos simultáneamente, los sistemas multimodales son desde luego más caros, pero, tal como se indica más adelante, tienen ventajas por la utilización de más de un método de verificación.

10 A continuación, se explica un ejemplo de la invención para explicar la forma en qué funcionan los sistemas multimodales. Una forma de comprender un sistema multimodal sería imaginar un sistema que consiste en dos de los métodos de verificación biométrica anteriormente explicados, por ejemplo, huellas dactilares y escaneado del iris. Esto proporcionaría la posibilidad de escoger entre tres configuraciones.

15 El individuo puede escoger un método que sea el más apropiado en aquél momento debido a factores ambientales o de otro tipo. Por ejemplo, si las manos del conductor están sucias, escanear el iris, si el interior de la cabina está oscuro, escanear la huella dactilar.

20 El individuo utiliza ambos métodos independientes entre sí y el sistema evalúa ambos resultados para tomar la decisión. Esta configuración se ha demostrado empíricamente que es capaz de reducir la Tasa de Rechazos Falsos (False Rejection Rate) (FRR) sin aumentar la Tasa de Aceptaciones Falsas (False Acceptance Rate) (FAR). Si la correspondencia para uno de los métodos de verificación no es satisfactoria, pero el otro método proporciona una correspondencia válida, el individuo puede pasar la verificación.

25 El sistema requiere que el individuo pase ambos métodos independientes entre sí. Esto incrementa el nivel de seguridad, puesto que es más difícil engañar dos métodos que uno solo. Un inconveniente es que estos sistemas tienden a tener una Tasa de Rechazos Falsos elevada.

30 Cuando se utilizan sistemas multimodales, se puede mejorar la seguridad o la comodidad, no ambos al mismo tiempo. Un inconveniente de los sistemas multimodales es que la verificación consiste en varias tareas y, por lo tanto, requiere más tiempo, lo que puede ser poco cómodo para el usuario.

SISTEMAS BIOMÉTRICOS MÚLTIPLES

35 Los sistemas multimodales descritos en la sección anterior son un caso especial de los llamados sistemas múltiples. Utilizan varias mediciones pero no necesariamente diferentes métodos.

Existen básicamente cinco tipos de sistemas de verificación múltiple:

40 **Correspondencia múltiple** Sistema de correspondencia múltiple que analiza un escaneado en dos o varias formas distintas o con dos algoritmos distintos, por ejemplo (utilizando escaneado de huellas dactilares) correspondencias basadas en indicios (minutiae) y no indicios.

45 **Sensor múltiple** Un sistema se llama sistema de sensor múltiple cuando se utilizan dos o más sensores distintos para escanear el mismo objeto.

Multimodal Los sistemas multimodales utilizan dos o más métodos diferentes, por ejemplo, reconocimiento de voz y reconocimiento facial.

50 **Unidades múltiples** Un sistema de unidades múltiples escanea dos o varias unidades de la misma característica, por ejemplo, los dedos índice y medio o el ojo derecho y el ojo izquierdo.

55 **Impresión múltiple** Los sistemas de impresión múltiple escanean la misma característica una serie de veces, solicitando, por ejemplo, al sujeto, que diga su contraseña tres veces para un sistema de verificación de voz.

60 Todos estos sistemas tienen sus evidentes ventajas y desventajas. Dado que se ha decidido previamente implementar tres métodos, se pondrá énfasis en un sistema multimodal, por lo que los otros métodos múltiples no serán explicados adicionalmente.

TRABAJO PREPARATORIO

65 Debido a los dos objetivos propuestos, se han utilizado varios métodos de trabajo distintos y, por lo tanto, se han conseguido diferentes tipos de resultados. En esta sección, el método y los resultados son interconectados a efectos

de proporcionar al lector una imagen del proceso en funcionamiento. Cada fase se describe separadamente seguida de su resultado. Se supone que ello proporciona una idea más clara de cuáles son las decisiones que se realizaron en las diferentes etapas en todo el proceso y la forma en la que continúa el trabajo basándose en estas decisiones.

5 ESTUDIO DE LAS ENCUESTAS

Para evaluar las opiniones de los conductores en la elección de los métodos a implementar, se realizó una encuesta de conductores en una etapa previa.

10 LAS DOS ENCUESTAS DISTINTAS

15 La encuesta fue dividida en dos documentos llamados encuesta de actitud y encuesta de método, respectivamente. La primera preguntaba, por ejemplo, las rutinas en el trabajo, conocimiento de métodos biométricos e impresiones de seguridad y protección en el trabajo. La segunda proporcionaba una corta explicación de cada método biométrico descrita en la sección 2. Se pidió a los que respondían que facilitaran comentarios espontáneos de cada método. Algunas de las cuestiones pedían al encuestado que calificara las respuestas entre 1 y 5, siendo 1 la respuesta más negativa y 5 la respuesta positiva, mientras que algunas preguntas solamente pedían respuestas de más reflexión. Todas las preguntas tenían un espacio para reflexiones y comentarios.

20 La razón para realizar dos documentos distintos era impedir que los encuestados miraran las cuestiones siguientes y, por lo tanto, pudieran verse influenciados por los hechos en las descripciones de los diferentes métodos de verificación. Dado que la encuesta fue dividida en dos partes, los conductores fueron obligados a contestar la primera parte antes de recibir la siguiente.

25 La encuesta fue distribuida de dos maneras. Los primeros en dar sus opiniones fueron conductores de autobús que se habían parado en un descanso en una parada de autobuses, justamente fuera de Gothenburg. Se pidió a numerosos conductores que llenaran la encuesta, pero solamente 12 aceptaron hacerlo. Como agradecimiento para los encuestados, se les regalaron artículos de bombonería.

30 En segundo lugar, una empresa de transporte de Gothenburg aceptó distribuir la encuesta entre sus conductores. Las experiencias anteriores han mostrado que no habría tantas contestaciones como encuestas distribuidas y, por lo tanto, se facilitaron 25 encuestas a la empresa de transporte con la esperanza de recuperar, como mínimo, la mitad de ellas dentro del límite de tiempo de una semana. Diez encuestas fueron contestadas y devueltas a tiempo.

35 Había una versión inglesa y una versión sueca de la encuesta, de manera que todos los conductores podían tener la posibilidad de contestar el cuestionario con independencia de si eran suecos o no. Esto era importante en la parada de camiones local, puesto que muchos de los conductores hablaban poco o ningún sueco. Todas las encuestas distribuidas en la empresa de transportes estaban escritas en sueco.

40 RESULTADOS DE LA ENCUESTA DE ACTITUD

45 Once de los encuestados trabajaban en la distribución, diez conducían en largas distancias y uno conducía tanto en larga distancia como en distribución. Doce de los conductores fueron los únicos que conducían sus camiones particulares, los otros compartían sus camiones con un promedio de otros cinco conductores. Habían trabajado durante un promedio de 15 años, variando de uno año a 38.

50 Ocho conductores conocían métodos biométricos, por ejemplo, todos conocían la verificación por huellas dactilares. Si bien esta fue la única respuesta de algunos, otros pudieron mencionar también otros varios métodos. Solamente un conductor no había utilizado nunca un método de verificación biométrica. Nueve de los conductores que no habían tenido experiencias de sistemas biométricos se mostraban positivos ante la idea de utilizarlos para verificación, cuatro eran más restrictivos o contrarios al conjunto de la idea y los otros ocho no eran positivos ni negativos. La calificación promedio fue de 3,6.

55 Ocho conductores apreciaron desventajas con un sistema de verificación biométrica, mientras que once no las apreciaban. Tres conductores no contestaron la pregunta. Por otra parte, eran apreciables las ventajas para 15 conductores, mientras que 5 no pudieron apreciar ninguna y dos no contestaron la pregunta. A la pregunta de dónde se deberían mantener los datos biométricos, 15 de los conductores contestaron que preferirían que se mantuvieran en una tarjeta inteligente que pudieran llevar al salir del vehículo. Cinco creyeron que el almacenamiento se debía mantener en la empresa de transporte y dos lo deseaban en el vehículo. Se debe observar que algunos conductores escogieron más de una opción y tres no contestaron.

60 RESULTADOS DE LA ENCUESTA DE MÉTODO

65 La verificación por huellas dactilares fue, de modo marcado, el método más apreciado; todos creyeron que era el más barato y más fácil de utilizar. Incluso los que no deseaban métodos de verificación biométrica en el vehículo preferían las huellas dactilares. No obstante, cuatro conductores mostraban preocupación de que las manos sucias

provocarían problemas. Dos encuestados imaginaron escenarios en los que perdían sus dedos o eran raptados para poner en marcha el vehículo, pero aunque podían apreciar estas desventajas, también podían apreciar ventajas. Además, cuando se les preguntó con respecto a otros métodos, los conductores contestaron en algunos casos que preferían utilizar las huellas dactilares (en vez del método en cuestión).

5 Con respecto a otros métodos, la mezcla de respuestas positivas y negativas hizo difícil sacar conclusiones de si el método era adecuado o no. Merece ser mencionado, dado que seis de los conductores lo comentaron, que se sentían escépticos en cuanto a la verificación de voz, dado que es muy habitual que un conductor trabaje aunque tenga un constipado o la garganta irritada. Dos de ellos tenían una mala experiencia con la tecnología de reconocimiento de voz y, por lo tanto, eran escépticos en cuanto a la verificación por voz.

ENTREVISTA TELEFÓNICA CON LOS CONTRATISTAS DE TRANSPORTE

15 Un sistema de verificación, tal como el de la invención, sería no solamente importante para los conductores, sino también para los diferentes contratistas de transporte. Para conseguir una idea de las diferentes exigencias por parte de los contratistas de transporte se realizó una serie de entrevistas telefónicas.

FORMA EN LA QUE SE LLEVARON A CABO LAS ENTREVISTAS TELEFÓNICAS

20 Se pidió una entrevista telefónica a diez oficinas de Gothenburg escogidas al azar. Tres de ellas fueron entrevistadas y una cuarta recibió la encuesta como e-mail, la contestó y la devolvió de la misma manera. Las cuestiones eran casi las mismas que en las encuestas de conductores, solamente que en este caso se les preguntaba verbalmente y estaban ligeramente ajustadas para adaptarse a las empresas en vez de a los conductores. Las preguntas fueron leídas con volumen de voz fuerte al informante y se les explicó en caso necesario. Las respuestas fueron escritas por el entrevistador.

30 Resultó difícil conseguir la persona adecuada para la entrevista y aún cuando esto ocurría, era difícil encontrar alguien que tuviera tiempo para contestar las preguntas. Dado que las respuestas fueron muy similares, dieron una indicación de lo que las empresas consideraban importante. Se debe observar que debido al bajo número de informantes las respuestas no se han especificado siempre en el número exacto.

RESULTADOS DE LA ENTREVISTA TELEFÓNICA CON CONTRATISTAS DE TRANSPORTE

35 Las condiciones de trabajo dentro de las cuatro oficinas entrevistadas eran variables, por ejemplo, estaban representadas tanto las de transporte a larga distancia como las de distribución, así como las de mercancías peligrosas y mercancías de alto valor. Las dimensiones de la empresa variaban desde ocho conductores a 76. Solamente una de las empresas utilizaba personal externo en caso de enfermedad u otra ausencia inesperada.

40 Las respuestas eran principalmente positivas y las empresas parecían conocer más con respecto a los diferentes métodos de verificación que los conductores de la encuesta. La demanda principal era que no debía ser caro, pusieron énfasis en que deseaban mucha seguridad con un coste reducido. El mayor temor era de que si había el peligro de que los conductores perdieran un ojo o un dedo entonces no valía la pena. El mayor escepticismo era con respecto a la tecnología. “¿Qué ocurre si falla?” era una pregunta habitual. La mayor parte de ellos veían también problemas si le ocurría algo al conductor, un accidente u otra cosa que le incapacite para desplazar el vehículo. 45 “Debe haber una manera de que el vehículo pueda ser desplazado de todos modos”.

50 La verificación por las huellas dactilares era el método más apreciado dado que todas las empresas eran positivas con respecto al mismo. Dos personas eran muy contrarias con respecto a los análisis de los ojos. Una tercera comentó que sería mejor con verificación de huellas dactilares porque no es tan caro. Ninguno confiaba en un sistema de verificación utilizando reconocimiento de voz con la justificación de que es habitual que los conductores trabajen aunque se encuentren enfermos o con la voz ronca. El reconocimiento facial se creyó que era más caro que la verificación de huellas dactilares y se temió que no se adecuara bien a aumentos de peso o a que la misma persona llevara barba o no. Ninguno de los otros métodos suscitó optimismo alguno. La geometría de las manos, por ejemplo, se creyó que era innecesaria, dado que se percibía que no era tan fiable como la verificación de las huellas dactilares. Además, incrementaría el riesgo de perder toda una mano en vez de “solo un dedo”.

60 Varios de los informantes no creyeron que sus empresas necesitaban esta seguridad tan elevada. En vez de ello, indicaron la necesidad de dispositivos de bloqueo por alcohol. Si tenían que escoger algo se decidirían por la verificación de las huellas dactilares. Una de las personas era más positiva al conjunto de la idea que las otras y una era más negativa. Se debe observar que la persona que era más negativa con respecto a los métodos biométricos para verificación era partidaria de la idea de la llamada identificación del estilo del conductor. Los vehículos actuales pueden controlar y almacenar mucha información, por ejemplo, duración de la jornada, consumo de combustible, cambios de velocidad y técnica de frenado. Viendo esta información, puede ser posible observar el estilo de conducción de un conductor. Esto no sería suficiente para verificar una persona, pero si el modelo cambiaba drásticamente se podría suponer que alguna otra persona se podría haber hecho cargo del vehículo. El informante al 65 que le gustaba la idea de la identificación del estilo del conductor sugería que se debería integrar con la detección de

somnolencia y detección de si el conductor estaba tomando medicamentos u otras sustancias.

Aunque las empresas no percibían que necesitaran un sistema de verificación en aquel momento, lo consideraron positivo si resultaba más difícil robar sus vehículos.

5

REFLEXIONES CON RESPECTO A LA FORMA EN QUE LOS MÉTODOS SE ADAPTAN AL OBJETIVO

Hay varios métodos de verificación distintos en el mercado en la actualidad; todavía no hay un método perfecto para el objetivo de esta invención. La teoría debe llevar a reflexiones y discusiones con respecto a la adecuación de los métodos en un contexto de un camión. Todos los métodos tienen sus pros y contras, pero no ha sido posible probarlos. Por lo tanto, es importante evaluar teóricamente los diferentes métodos entre sí para tener la posibilidad de escoger cuáles se deben implementar en el prototipo de prueba. Esta sección describe los resultados de la discusión y las comparaciones teóricas.

10

EL MÉTODO IDEAL

15

Las características más deseables para el sistema de verificación se han relacionado para tener una base para la selección de los métodos a implementar. Estos criterios han sido escogidos, dado que aparecieron durante las discusiones y generación de ideas con respecto a la forma en que debería funcionar un sistema ideal.

20

Facilidad de utilización No debía ser necesaria ninguna formación extensa para hacer funcionar el equipo. Debía ser lo más intuitivo posible y debía ser automatizado en el grado máximo.

25

Velocidad El proceso de verificación no debe requerir mucho tiempo, unos pocos segundos como máximo. El alistamiento debe ser también rápido. Además, el método no debe consistir en demasiadas tareas diferentes.

30

Flexibilidad El sistema debe estar construido para gestionar diferentes conductores que pueden cambiar turnos. Debe ser posible verificar el conductor mientras está conduciendo a efectos de evitar que el conductor verificado ponga en marcha el motor solamente siendo luego expulsado del vehículo por un impostor.

35

Coste El sistema no debe ser excesivo, puesto que de otra manera los propietarios de los camiones no considerarán su compra.

Aceptación de usuario El sistema no debe ser intrusivo. Aparte de ello, el usuario y el propietario del camión deben sentir que el sistema es significativo y beneficioso para ellos.

40

Seguridad El sistema debe ser seguro contra ataques.

Exactitud El sistema debe conseguir un TER (Total Error Rate ("Tasa Total de Error")) suficientemente bajo.

45

Adecuación Los métodos del sistema deben adecuarse a las diferentes características de entorno de los vehículos, tales como espacio, iluminación, temperatura, ruido, vibraciones y humedad.

50

Integrabilidad Un equipo que se integra fácilmente en el vehículo puede mantener reducidos los costes y hacer el sistema más fácil de utilizar, puesto que no habrían muchas tareas nuevas que dominar. El equipo necesario no debería ser voluminoso, puesto que de otro modo sería difícil de montar en el vehículo.

55

Fiabilidad El sistema no debe averiarse nunca ni debe fallar con la verificación, de otro modo sería incapaz de impedir que personas no autorizadas pusieran en marcha el vehículo. Esto puede provocar que el conductor o el propietario desconfíen del sistema. En el mismo sentido, no debe fallar nunca en conceder acceso al conductor apropiado.

NOCIONES CON RESPECTO A LOS DIFERENTES MÉTODOS

60

Esta sección contiene algunas anotaciones argumentando en favor o en contra de los diferentes métodos de verificación. Los temas y reflexiones siguientes están relacionados con los criterios del sistema ideal que se han descrito anteriormente. Estas ideas han influido en diferentes aspectos de la invención.

65

NOCIONES CON RESPECTO A LA VERIFICACIÓN DE HUELLAS DACTILARES

5 La tecnología de las huellas dactilares está bien comprobada en el sentido de que ha sido utilizada y desarrollada durante un largo tiempo. Los dispositivos de escáner se pueden hacer pequeños y poco onerosos y el método es considerado no intrusivo por la mayor parte de personas. Una amplia variedad de marcas se encuentran disponibles en el mercado, lo que facilita buenas oportunidades de encontrar un producto adecuado a las exigencias requeridas.

10 Una forma de incrementar la seguridad para un sistema de verificación consistiría en utilizar más de un dedo para la verificación. Hay dos formas diferentes de hacerlo; o bien el sistema requiere el escaneado de un conjunto predefinido de dedos o el sistema requiere al azar cuál es el dedo a escanear el aquél momento específico. Un inconveniente de estas alternativas es, desde luego, que si se requiere un conjunto de huellas, un impostor puede intentar robar la totalidad de las huellas de una persona. En este caso, el incremento de protección podría tener lugar a costa de la seguridad del usuario.

15 Es interesante considerar, con respecto a la perspectiva de la automoción, que muchos conductores trabajan mucho con sus manos, haciendo que las manos se ensucien o muestren desgaste, lo cual puede afectar al resultado del escaneado. Si el escáner se ensucia, el escaneado adecuado puede resultar difícil. Esto se puede solucionar utilizando un escáner de barrido, puesto que no tiende a ensuciarse en la misma medida que un escáner de contacto.

20 Siempre existirá la posibilidad de que personas no autorizadas intenten engañar el sistema. Si bien la detección de vitalidad protege contra copias o el escenario horrible en que el impostor roba todo el dedo (o la mano), es imposible conseguir un sistema absolutamente seguro. Se pueden utilizar drogas o amenazas para forzar al conductor autorizado para que ponga su dedo en el escáner. Como resumen, el escaneado de huellas dactilares es un método rápido, económico y no intrusivo que puede ser integrado fácilmente en el vehículo.

NOCIONES CON RESPECTO AL ESCANEADO DE IRIS

30 El escaneado de iris se considera que es un método de verificación exacto, fiable y seguro. De acuerdo con la literatura existente, existe en la actualidad un equipo disponible que puede tomar una imagen desde una distancia de un metro aproximadamente, consiguiendo todavía suficiente calidad para comparar la imagen con respecto a un modelo. Esto significa que puede ser posible instalar una cámara en la cabina de manera tal que la cámara no moleste al conductor ni oscurezca su campo de visión. No obstante, no está claro que estas aplicaciones sean adecuadas para vehículos y todavía menos claro si es posible escanear mientras se conduce, dado que no se han llevado a cabo pruebas en esta área.

35 El escaneado del iris es, por lo tanto, rápido y puede no ser intrusivo, no obstante, su adecuación, así como la integridad, fallan en este método y el equipo es caro debido a la licencia a pagar.

NOCIONES CON RESPECTO AL RECONOCIMIENTO DE VOZ

40 Un sistema para la verificación por voz debe ser integrado fácilmente en un vehículo, quizás utilizando equipos existentes, tales como el sistema de manos libres para el teléfono móvil. Debe ser posible realizar verificación de voz mientras se conduce, como mínimo, en el sentido de que la mayor parte de personas son capaces de hablar y conducir al mismo tiempo. Si el conductor utiliza el teléfono móvil u otro sistema de comunicación verbal, la demanda de verificación se puede suprimir durante algunos minutos. En el caso en el que el conductor escucha el equipo de estéreo, se sugiere que el sonido se enmudezca durante la verificación.

50 La cabina de un camión moderno está aislada contra ruidos, lo que es sensible cuando se entra en la misma. Debido al aislamiento contra ruidos, el ruido de fondo del motor, del viento y del tráfico circundante es bastante constante. Por lo tanto, debe ser posible utilizar un filtro adaptativo para eliminar ruido de la muestra de voz durante la verificación. Sin embargo, aunque la mayor parte de cabinas de camiones están bien aisladas, los sistemas de verificación de voz se han desarrollado para utilización en el interior de oficinas, por lo que resulta difícil decir si es adecuado o no sin probar el sistema en un entorno de un vehículo.

55 El lado negativo es que la base de datos tendrá que ser actualizada continuamente dado que la voz de una persona y su acento cambian a lo largo del tiempo. Además, la voz de una persona puede cambiar rápidamente debido a cuestiones de salud y a factores emocionales. Estos aspectos han provocado que ciertas personas desconfíen de esta tecnología.

60 Dado que el enfoque de esta invención consiste en verificar la identidad de un conductor, se sugiere la utilización de una frase de verificación predefinida. Si cada conductor tiene una contraseña única, tanto la propia frase como la muestra de voz, se pueden utilizar para verificación. La verificación de voz es, por lo tanto, un método poco oneroso, que se puede implementar fácilmente en un camión. No obstante, debido al entorno ruidoso y al hecho de que la luz presenta cambios a lo largo del tiempo, es incierto que funcione adecuadamente en situaciones reales.

65

NOCIONES RESPECTO AL RECONOCIMIENTO FACIAL

5 El reconocimiento facial es sensible a las condiciones de luz, pero puede ser una alternativa antes de poner en
 10 marcha el vehículo, puesto que es posible añadir mayor iluminación de la cabina durante la verificación. No
 obstante, no se recomienda proceder de este modo durante la conducción, dado que puede provocar la distracción
 del conductor. Las condiciones de luz cambian a lo largo del día, por lo que no es claro que el reconocimiento facial
 pueda ser utilizado mientras se conduce. Una imagen tomada durante la noche puede no ser una imagen
 suficientemente similar para ser almacenada a efectos de que el sistema consiga la verificación. Diferentes
 condiciones de luz serán objeto de prueba dado que una cámara en el vehículo proporciona muchas otras
 15 posibilidades, tales como detección de somnolencia, control de la cabina, etc. No obstante, estas posibilidades se
 encuentran más allá del objetivo de esta invención, por lo que no se investigarán de manera adicional.

15 La parte correspondiente al consumo de tiempo del reconocimiento facial es la creación de un modelo. Durante la
 verificación, el sistema puede necesitar tomar tres o más imágenes para asegurar que, como mínimo, una de ellas
 es suficientemente satisfactoria. La creación del modelo requiere aproximadamente 3-5 segundos, lo que significa
 que la totalidad del proceso de verificación requerirá aproximadamente 10-15 segundos, lo que es demasiado
 tiempo.

20 Un efecto secundario interesante es el hecho de que la cámara utilizada toma imágenes realmente de la persona
 que intenta conducir el vehículo. Si un impostor conduce un vehículo, la verificación fracasará, pero de todos modos
 se tomarán imágenes y se almacenarán. Estas imágenes pueden ser utilizadas cuando se intente identificarle.

25 Como resumen, el reconocimiento facial es adecuado para el usuario, poco oneroso y es un método no intrusivo. No
 obstante, no ha sido posible encontrar investigaciones con respecto a la verificación facial en entornos que se
 parezcan a una cabina de un vehículo, y por lo tanto, no es claro que el método sea adecuado para el objetivo.

NOCIONES CON RESPECTO A TERMOGRAFÍA FACIAL

30 Una idea con respecto a la utilización del reconocimiento facial es que podría ser posible utilizarlo para la
 verificación automatizada durante la conducción. Esto, no obstante, será solamente posible si el sistema no es
 demasiado sensible a los cambios de las condiciones de luz. Tal como se ha explicado anteriormente, la
 termografía facial y el reconocimiento facial son prácticamente iguales; la diferencia es el tipo de cámara utilizada.
 La termografía facial utiliza una cámara IR, lo que significa que el método no es tan sensible a las condiciones de
 luz en comparación con el reconocimiento facial. Es difícil decir que la termografía facial corresponda al método
 35 ideal, puesto que no se han llevado a cabo pruebas y no hay ningún equipo de desarrollo disponible.

NOCIONES CON RESPECTO AL ESCANEADO DE LA RETINA

40 Los actuales equipos de escaneado de la retina han disminuido en tamaño y en coste, solucionando por lo tanto,
 algunos de sus problemas prácticos. Un problema más importante es el hecho de que ciertas personas tienen
 aversión a que sus ojos sean escaneados. Además, el método no es adecuado para la utilización en un vehículo,
 especialmente durante la conducción, puesto que el conductor tendría que mirar en una dirección específica
 durante el escaneado. Puede presentar problemas el mantener los ojos concentrados en un punto único durante un
 tiempo suficiente para la verificación, y esto puede afectar negativamente a la seguridad en el tráfico. Por lo tanto,
 45 con la tecnología actual, este no es un método a utilizar con los objetivos de esta invención.

NOCIONES CON RESPECTO AL RECONOCIMIENTO DE LA GEOMETRÍA DE LA MANO

50 La principal ventaja del reconocimiento de la geometría de la mano es que este método es completamente
 insensible a la suciedad, callosidades y cicatrices (dentro de límites razonables). Dado que son varias
 características de la mano completa las que se miden, no importa si los dedos están sucios o si la persona se ha
 cortado accidentalmente, etcétera. El equipo es económico y la verificación requiere menos de un segundo, pero el
 equipo voluminoso hace que el método no sea apropiado para los objetivos de automoción.

NOCIONES RESPECTO A SISTEMAS MULTIMODALES.

55 Con un sistema multimodal, se pueden conseguir diferentes niveles de seguridad combinando diferentes métodos.
 Para la utilización diaria puede ser suficiente con la verificación de las huellas dactilares. Cuando se conduce en
 áreas peligrosas o transportando mercancías peligrosas, la verificación puede ser realizada utilizando varios
 60 métodos (por ejemplo, simultáneamente, huellas dactilares y escaneado del iris), aumentando, por lo tanto, el nivel
 de seguridad.

65 Un aspecto interesante de los sistemas multimodales es que pueden ser utilizados para la actualización automática
 de la base de datos modelo. Se puede imaginar un sistema de verificación que utiliza tres métodos de verificación
 a la par, por ejemplo, PIN, huellas dactilares, y reconocimiento facial. Cuando el sistema requiere la verificación de
 un conductor, analiza las tres características. Si dos de los métodos se llevan a cabo satisfactoriamente, la base de

datos puede ser actualizada utilizando la tercera muestra. De este modo, si el PIN es correcto y el escáner de huellas dactilares proporciona una correspondencia aceptable, el sistema puede tomar una imagen de la cara para actualizar la base de datos modelo. Esto puede ahorrar mucho tiempo dado que el sistema actualiza continuamente la propia base de datos reduciendo así el mantenimiento del sistema.

5

SELECCIÓN DE MÉTODOS PARA IMPLEMENTACIÓN DE PROTOTIPO

El análisis teórico de los diferentes métodos de verificación, condujo a las nociones y reflexiones, que se han indicado en la sección anterior. Las nociones y el análisis SWOT forman la plataforma principal para la selección de métodos de verificación para la implementación de prototipo.

10

SELECCIÓN DE MÉTODO

No existe un método de verificación único que pueda cumplir los criterios del sistema ideal. Las decisiones finales de qué métodos utilizar se basan en un equilibrio entre exactitud y coste, así como entre facilidad de utilización y facilidad de falsificación. Los otros criterios del sistema ideal no difieren significativamente entre los métodos y, por lo tanto, no se han considerado durante la selección. Los pros y los contras para cada método han sido discutidos, así como el precio y plazo de entrega.

15

MÉTODO SELECCIONADO

Las razones para descartar un método están indicadas a continuación, seguido de las razones para escoger los métodos que se tenían que implementar.

20

25 Termografía facial Las cámaras IR son más costosas que las cámaras normales, pero dado que el método es muy exacto y difícil de falsificar, es definitivamente un área a examinar de manera detallada. Desafortunadamente, se han llevado a cabo pocas investigaciones con respecto a la termografía facial a efectos de verificación y los autores han sido incapaces de encontrar una empresa que fabrique equipos para este tipo de verificación.

30

Escaneado del iris Un equipo de desarrollo para el escaneado del iris cuesta \$25000-\$35000, lo que se encuentra más allá del presupuesto del proyecto.

35 Movimiento de labios El reconocimiento de movimiento de labios necesita otro método de verificación para ser completamente fiable. La idea es implementar tres métodos para la verificación, para comprobar su adecuación y compararlos entre sí. Para conseguir la posibilidad de diferentes niveles de seguridad, los tres métodos deber ser fiables por sí mismos, por lo que el reconocimiento de movimiento de labios no es una opción.

40

Escaneado de retina El escaneado de retina no es adecuado para objetivos de automoción debido a la exacta alineación de los ojos necesaria.

45 Geometría de las manos El equipo requerido para el escaneado por geometría de las manos es demasiado voluminoso para su montaje en la cabina.

Los tres sistemas restantes, verificación de huellas dactilares, reconocimiento de voz y reconocimiento facial son todos adecuados para su montaje en un vehículo y hay fabricantes que pueden ofrecer equipos de desarrollo a precios y plazos de entrega razonables.

50

Para hacer la integración del sistema lo más fácil posible se deseaba que todos los sistemas fueran compatibles con la misma plataforma. Esto, junto con la capacidad de facilitar un soporte, eran los dos criterios principales a la hora de elegir el fabricante.

55

Los PIN son actualmente habituales, y el método puede ser fácilmente implementado en un vehículo utilizando el teclado para el teléfono móvil. Por lo tanto, se implementa también un sistema de verificación por PIN. Esto permitiría también una comparación entre un método de verificación común y los sistemas biométricos.

Tal como se indica en los resultados de la encuesta, muchos de los encuestados prefirieron que los modelos biométricos se almacenaran en una tarjeta que se pudieran llevar consigo cuando dejaban el vehículo. Para mostrar la posibilidad de integrar el almacenamiento del modelo con el tacómetro digital, un lector de tarjetas inteligente se incluyó también en el sistema.

60

Como resumen, los métodos escogidos para el sistema prototipo son: huellas dactilares, reconocimiento facial, reconocimiento de voz y verificación de PIN y tarjeta.

65

CASOS DE UTILIZACIÓN

5 Los diferentes tipos de situaciones de trabajo y de áreas en las que se utilizan los camiones presentan diferentes retos para un sistema de verificación. Las reflexiones sobre cómo el sistema podría ser utilizado condujeron al desarrollo de una serie de casos de utilización. Al crear casos de utilización realistas, se indican las ventajas y también la demostración de la necesidad real de un sistema de verificación del conductor.

DESARROLLO DE LOS CASOS DE UTILIZACIÓN

10 Estos casos de utilización se basan en debates e intercambio de ideas durante el proceso de elección de métodos para la implementación.

VERIFICACIÓN MULTIMODAL UTILIZANDO TODOS LOS MÉTODOS BIOMÉTRICOS

15 Este es el nivel de seguridad más elevado, destinado a vehículos que transportan mercancías peligrosas o valiosas, o durante la conducción en áreas de alto riesgo. El conductor verifica su identidad utilizando todos los métodos para asegurar que es la persona apropiada. A continuación, hay algunos ejemplos de la forma en la que puede tener lugar esta verificación.

20 El conductor ha llegado a su base para iniciar el día de trabajo. Al entrar en el vehículo inserta su tarjeta inteligente (integrada en la tarjeta para el tacógrafo) en el dispositivo lector, marca su código PIN y, a continuación, pone su dedo sobre el escáner. El PIN es correcto y el dedo se verifica en comparación con la tarjeta, de manera que el sistema pide una muestra de voz. El conductor dice su contraseña en el micrófono. Aparece un mensaje del sistema indicando al conductor que se siente en su posición normal de conducción, a efectos de llevar a cabo la verificación facial. Los datos registrados son analizados y comparados con los datos modelo almacenados en la tarjeta inteligente-la verificación fue satisfactoria. Se enviaron el nombre, y el número de identificación de empleo, encriptados, a la oficina central.

25 El conductor lleva a cabo el proceso de verificación, pero falla en uno de los métodos. Un mensaje del sistema informa al conductor la verificación que ha fallado. El proceso continua igual que en el ejemplo anterior y, como mínimo, un método tiene éxito. El nombre y número de identificación de empleo son enviados, encriptados, a la oficina principal, junto con información sobre la verificación o verificaciones que han fallado.

30 En un viaje de larga distancia, el conductor hace la siesta en su cabina. Al despertar sale para estirar las piernas antes de continuar el viaje. La puerta del pasajero se abre y un impostor sube y se sienta en el asiento del conductor. El impostor intenta arrancar el vehículo pero no tiene éxito con la verificación, por lo tanto, el vehículo queda inmovilizado. Se envía un aviso inmediatamente a la oficina central y el sistema toma una imagen de la persona que se ha puesto detrás del volante. Esta imagen es enviada también a la oficina central.

VERIFICACIÓN MULTIMODAL UTILIZAND ODOS MÉTODOS BIOMÉTRICOS

35 El objetivo de este caso de utilización es el de asegurar que la persona que se sienta en el asiento del conductor es el conductor apropiado. Se han desarrollado cuatro situaciones diferentes a este nivel seguridad, tal como se indica más adelante. Se debe observar que es posible tener el vehículo equipado solamente con dos métodos de verificación biométrica. No obstante, también hay una posibilidad de tener todo el equipo necesario para todos los métodos y luego alterar al azar el que se debe utilizar en cada ocasión.

40 El conductor ha llegado a la base para empezar el día de trabajo. Al entrar en el vehículo inserta su tarjeta inteligente (integrada en la tarjeta para el tacógrafo) en el dispositivo lector, marca su código PIN y, a continuación, coloca su dedo sobre el escáner. El PIN es correcto y el dedo es verificado con respecto a la tarjeta. El sistema pide una muestra de voz, de manera que el conductor indica su contraseña en el micrófono. Los datos registrados son analizados y comparados con los datos del modelo almacenados en la tarjeta inteligente-la verificación ha sido satisfactoria. El nombre y número de identificación de empleo son enviados, encriptados, a la oficina principal.

45 El mismo escenario anterior, pero en vez del sistema de verificación de voz, un mensaje de sistema aparece indicando al conductor que se siente en una posición normal de conducción para llevar a cabo la verificación facial. Los datos registrados son analizados y comparados con los datos modelo almacenados en la tarjeta inteligente.

50 El conductor falla uno o varios de los métodos, pero tiene éxito, por lo menos, con un método. El nombre de conductor y número de identificación de empleo son enviados, encriptados, a la oficina principal, junto con la información con respecto a la verificación o verificaciones en las que ha fallado.

55 Ninguna de las verificaciones es satisfactoria, por lo tanto, el vehículo es inmovilizado, y se envía inmediatamente un aviso a la oficina principal.

60

VERIFICACIÓN BIOMÉTRICA INDIVIDUAL A DIFERENTES NIVELES DE SEGURIDAD

5 Se sugiere esta verificación en una parada corta, después de que el conductor ya ha sido verificado con varios métodos o si el nivel de seguridad hace insuficiente un solo método biométrico. Los niveles de seguridad pueden ser discutidos, desde luego, pero en estos ejemplos se clasifican como alto, medio y bajo nivel de seguridad. A continuación, se indican algunos ejemplos de alta seguridad.

10 El conductor está descargando su carga en una de muchas paradas durante el día. El vehículo está parado con el motor todavía en marcha. Una vez terminada la descarga, el conductor sube nuevamente al camión, es una parada corta, por lo tanto, solamente se requiere una verificación, cuyo método será establecido al azar. En este caso, el sistema requiere la verificación de huellas dactilares, de manera que el conductor pone el dedo en el escáner para verificar que él es todavía el que conduce el vehículo. Mientras el sistema verifica el conductor, este puede arrancar, mientras su nombre y número de identificación de empleo son enviados, encriptados, a la oficina principal para su confirmación.

15 El conductor se ha parado para comprar snacks en una parada de camiones, es una parada rápida, con el motor todavía funcionando, por lo que solamente se requerirá uno de los métodos disponibles para la verificación antes de salir otra vez. Un impostor se sienta en el asiento del conductor, lo que inicia la verificación. Dado que no se realiza ninguna verificación satisfactoria, el sistema toma una imagen con la cámara y la envía, junto con un aviso, a la oficina principal, el camión queda inmovilizado.

20 El sistema de verificación está destinado a aumentar la protección, pero no debe afectar al trabajo ordinario del conductor. Para hacerlo lo más fácil posible, el nivel medio de protección facilita al conductor más independencia que el nivel más elevado.

25 El conductor hace una de varias paradas durante el día para descargar una parte de la carga. El vehículo está parado con el motor en marcha. Una vez terminada la descarga, el conductor sube nuevamente al camión. Al sentarse, pone su dedo en el escáner para verificar su identidad. El sistema comprueba que es OK para la comprobación de la huella dactilar, en este caso, o el conductor debe utilizar uno de los otros métodos. En este caso, el sistema requiere otro tipo de verificación, por lo que se pide al conductor que verifique su identidad facilitando su contraseña. La verificación tiene éxito y el conductor puede marcharse, mientras su nombre y número de identificación de empleo son enviados, encriptados, a la oficina principal para su confirmación.

35 El conductor se ha parado para descargar una parte de la carga. El motor está todavía funcionando. El conductor vuelve al vehículo y marca su código PIN. Dado que el conductor está estresado, marca un número equivocado, prueba una y otra vez pero no recuerda el código correctamente-la verificación falla. El sistema informa al conductor que la verificación ha fallado y le pide que verifique su identidad utilizando alternativamente el escaneado de las huellas dactilares. La verificación es satisfactoria y el conductor puede salir. El nombre del conductor y el número de identificación de empleo son enviados, encriptados, a la oficina principal para su confirmación, junto con la información de la verificación de PIN que ha fallado.

40 Un nivel bajo de seguridad puede requerir solamente un método de verificación. Esto significa que puede ser suficiente para el vehículo el disponer de un equipo para un único método de verificación. También proporciona la posibilidad de tener varios métodos en un camión y, dependiendo, por ejemplo, de la carga, ruta o duración del descanso, solamente se pide un método. Un sistema de verificación en el vehículo se puede suponer que aumenta la protección. No obstante, con un método solamente, existe naturalmente un riesgo más elevado de que ocurran fraudes que con varios métodos de verificación.

45 El conductor está descargando su carga en una de las muchas paradas que realiza durante el día. El vehículo está parado con el motor en marcha. Una vez terminada la descarga, el conductor sube nuevamente al camión. Se sienta y pone su dedo sobre el escáner para verificar su identidad. Dado que el sistema ha verificado el conductor, este sale conduciendo el vehículo y su nombre y número de identificación de empleo son enviados, encriptados, a la oficina principal para su confirmación.

50 El conductor ha parado para descargar su carga. Dado que el conductor ya se ha identificado anteriormente durante el mismo día, un solo método de verificación será suficiente, aunque el vehículo tiene un nivel alto de seguridad. Otro conductor, que también tiene tarjeta inteligente con sus datos biométricos almacenados, toma el lugar del conductor e intenta verificar su identidad. El sistema advierte que la tarjeta ha sido sacada y que se ha puesto otra, de manera que una sola verificación no será suficiente. El conductor verifica su identidad con todos los métodos y la información es enviada, encriptada, a la oficina principal, donde se descubre rápidamente que no es el conductor apropiado el que está conduciendo el vehículo.

55 El conductor se ha parado a comprar snacks en una parada de camiones. Es una parada rápida con el motor en marcha, por lo que se requerirá solamente uno de los métodos disponibles para la verificación antes de salir otra vez. Un impostor se sienta en el asiento del conductor, lo que pone en marcha la verificación. Dado que no se lleva

65

a cabo una verificación satisfactoria, el vehículo es inmovilizado. El sistema toma una imagen con la cámara y la envía, junto con un aviso, a la oficina principal.

5 El conductor entra en el vehículo. Pone su dedo sobre el escáner, pero no tiene éxito con la verificación. Dado que este era el único método disponible, se envía inmediatamente un aviso de la verificación que ha fallado a la oficina principal. El vehículo queda inmovilizado.

VERIFICACIÓN MANUAL DURANTE LA CONDUCCIÓN

10 Un posible escenario podría ser el de un impostor que fuerza al conductor a verificar su identidad y luego hacerlo al salir del vehículo. Para evitar este riesgo y otros similares, el conductor debe ser verificado también durante la conducción. A continuación, se indican algunos ejemplos para explicar esta idea.

15 El vehículo está en la carretera. Aparece un mensaje del sistema pidiendo al conductor que indique su contraseña para verificar su identidad. El conductor lo hace y tiene éxito con la verificación. Su nombre y número de identificación de empleo son enviados, encriptados, a la oficina principal.

20 El conductor se encuentra en un recorrido de larga distancia. Aparece un mensaje del sistema pidiendo al conductor que indique su contraseña para verificar su identidad. El conductor lo hace, pero la verificación falla dado que ese día su voz es ronca. El conductor prueba otras dos veces pero la verificación falla, de manera que el sistema le pide que ponga un dedo en el escáner. En este caso, la verificación tiene éxito. El nombre del conductor y el número de identificación de empleo son enviados, encriptados, a la oficina principal, junto con la información de la verificación que ha fallado.

25 El vehículo se encuentra en la carretera. Aparece un mensaje del sistema pidiendo al conductor que ponga un dedo en el escáner para verificar su identidad. El conductor no puede verificar su identidad con ninguno de los métodos. Se envía inmediatamente un aviso a la oficina principal, junto con una fotografía del conductor no verificado, tomada por la cámara, para verificación facial. Dado que el conductor fue verificado antes de poner en marcha el vehículo, el nombre del conductor y el número de identificación de empleo son enviados, encriptados, a la oficina principal, junto con la información de la verificación que ha fallado durante la conducción.

35 Un vehículo con un equipo para varios métodos de verificación, se encuentra en la carretera. Aparece un mensaje del sistema pidiendo al conductor que ponga un dedo en el escáner para verificar su identidad. No se realiza la verificación dentro de los tres minutos siguientes, enviando, por lo tanto, un aviso a la oficina principal.

El vehículo se encuentra en la carretera. Aparece un mensaje del sistema pidiendo al conductor que ponga un dedo en el escáner para verificar su identidad. La verificación falla, y dado que este es único método para la verificación en este vehículo, se manda un aviso inmediatamente a la oficina principal.

40 VERIFICACIÓN AUTOMÁTICA DURANTE LA CONDUCCIÓN

Esta verificación es realizada sin intervención del conductor. Esto implica varias ventajas, por ejemplo, no se estorba al conductor, aunque se verifique su identidad, mientras está conduciendo, y un impostor no sabe siquiera que el sistema intenta identificarlo. Para hacer posible una identificación automática, el vehículo debe proporcionar un equipo de reconocimiento facial. A continuación, se indican algunos ejemplos de verificación automática durante la conducción.

50 El vehículo se encuentra en la carretera. El sistema toma imágenes del conductor y compara las características con el modelo de la tarjeta inteligente del tacógrafo. La verificación tiene éxito y el nombre del conductor y el número de identificación de empleo son enviados, encriptados, a la oficina central.

55 El conductor se encuentra en una misión de larga distancia en un vehículo con varios métodos posibles de verificación. El sistema intenta verificar el conductor con respecto al modelo de la tarjeta inteligente del tacógrafo. La verificación falla, por lo que aparece un mensaje del sistema pidiendo al conductor que ponga un dedo sobre el escáner. Esta vez la verificación tiene éxito. Un encriptado del nombre del conductor y el número de identificación de empleado son enviados a la oficina central junto con información sobre la verificación que ha fallado.

60 En una situación similar a la anterior, la verificación falla, de manera que se pide al conductor que ponga un dedo en el escáner. Ningún método de verificación tiene éxito, de manera que se envía inmediatamente un aviso a la oficina central junto con una fotografía del conductor no verificado tomada por la cámara a efectos de verificación facial.

65 El vehículo se encuentra en la carretera. La verificación automática falla y aparece un mensaje del sistema pidiendo al conductor que ponga un dedo sobre el escáner para verificar su identidad. No se hace verificación dentro de los tres minutos siguientes, por lo tanto, se envía un aviso a la oficina central junto con información con respecto a la verificación facial que ha fallado y la ausencia de verificación por medio de cualquier método adicional.

DISEÑO E IMPLEMENTACIÓN DEL SISTEMA PROTOTIPO

5 Cuando los sistemas de verificación fueron escogidos y el equipo había llegado, era el momento de montar el sistema. El sistema fue desarrollado utilizando un sistema de desarrollo iterativo, lo cual resultó en el sistema mostrado en esta sección. Una visión general del sistema de verificación implementado se indica a continuación y las exigencias de software para dicho sistema se explican junto con la descripción de la implementación.

HARDWARE

10 Los fabricantes para el hardware fueron escogidos principalmente a partir de tres criterios: coste, plazo de entrega y compatibilidad. La primera parte de esta sección describe el hardware y la segunda parte describe el resultado de la implementación.

HARDWARE DEL SISTEMA

15 El equipo utilizado para este proyecto es el indicado y descrito más adelante.

20 El sistema de verificación de huellas dactilares utilizado es un BioCore II de Precise Biometrics AB, Suecia. Es un sistema incorporado, por lo que el hardware estaba incluido en el equipo.

El sistema de verificación facial es un VeriLook SDK 1.1 de la firma Neurotechnologija Inc., Lituania. La cámara, una Logitech QuickCam 4000 Pro, fue escogida con respecto a las recomendaciones de Neurotechonologija Inc.

25 Para el reconocimiento de voz se adquirió una licencia de VoiceKey SDK de SpeechPro Inc., Rusia. La cámara de verificación facial tenía un micrófono incorporado para utilizar a efectos de conferencia por Internet, esto era una ventaja, puesto que el micrófono podría ser utilizado para el sistema de verificación de voz. No obstante, debido a la falta de tiempo, el reconocimiento de voz no fue implementado en el sistema.

SISTEMA DE VERIFICACIÓN IMPLEMENTADO

30 A continuación se indicará de modo general el sistema de verificación implementado, mostrando las flechas las diferentes partes que comunican entre sí. (Ver figura 12)

Lector SC	Lector de tarjetas inteligentes norma ISO7816.
Escáner de huellas dactilares	Escáner de huellas dactilares RF, que envía imágenes de la huellas dactilares a BioCore II.
Cámara	Cámara web norma VGA fijada al PC principal con intermedio de USB.
Micrófono	El micrófono incorporado en la cámara.
BioCore II	Sistema de verificación de huellas dactilares incorporado. Recibe imágenes de huellas dactilares procedentes del escáner de huellas dactilares. Envía y recibe modelos hacia/desde el PC principal y gestiona el proceso real de verificación de huellas dactilares.
PC principal	Un PC que recoge datos del escáner de huellas dactilares (a través de BioCore II, micrófono y cámara. El ordenador tiene también una base de datos de modelos y algoritmos para evaluar los resultados para proporcionar/denegar autorización.
PC pantalla	El PC de la pantalla utiliza el GUI y presenta información en la pantalla táctil montada en la consola central de la cabina del camión.
Pantalla táctil	Pantalla táctil con una anchura de 7" del monitor TFT montado en el tablero de la cabina del camión. Utilizada para presentar información e instrucciones y para servir como teclado durante la verificación del PIN.

35 COLOCACIÓN DEL EQUIPO

40 Antes de implementar el sistema en el simulador, se discutió la colocación del equipo. Habían planes para situar el escáner de huellas dactilares en la palanca de cambio de marchas, pero dado que faltaba en el simulador, el escáner fue colocado en el volante. El sistema de reconocimiento facial requiere una imagen recogida desde un ángulo que no supere 5 grados en ninguna dirección. Esto proporcionaba dos posibilidades de colocación de la cámara, por encima del conjunto de instrumentos o en el techo encima del parabrisas. Con esta última colocación, el sistema se comportó poco satisfactoriamente, por lo tanto, la cámara fue situada por encima del conjunto de instrumentos. El panel tenía una abertura que se acoplaba bien con la pantalla. Este montaje proporcionó también

una colocación auténtica al teclado. A continuación se adjunta una imagen de las partes del sistema montado en la cabina del camión. (Ver figura 13)

SOFTWARE

5 Los tres fabricantes ofrecieron equipos de desarrollo para un entorno C++ y, por lo tanto, esta plataforma de desarrollo fue la escogida. La implementación real (por ejemplo, el propio código) no es importante para el objetivo de los resultados de la invención y, por lo tanto, no se describirá de manera detallada.

INTERFAZ GRÁFICO DE USUARIO (GUI)

El objetivo del GUI era el de permitir al usuario y al sistema comunicarse entre sí. La fase de diseño y también el resultado se presentan en esta sección.

DESARROLLO DEL GUI

15 En primer lugar, se esquematizó sobre papel un prototipo “low-fi”, un documento para cada mensaje que sería mostrado durante la prueba. Había mensajes escritos e ilustraciones y algunos de los mensajes tenían dos o tres versiones. Los mensajes escritos se encontraban todos en sueco, dado que este idioma se suponía que sería la lengua principal para los participantes en la prueba. Se llevó a cabo también una búsqueda de sonidos adecuados para suplementar los mensajes. El “GUI low-fi” fue mostrado individualmente a cinco empleados de VTEC que tenían poca o ninguna experiencia en el diseño de interfaces GUI a efectos de captar sus reacciones. Se les mostró primero una versión de los mensajes en la sucesión en la que aparecerían en la prueba. En segundo lugar, se les mostraron versiones alternativas y se les pidió que indicaran sus opiniones sobre cuál utilizar.

25 El GUI low-fi fue mostrado a continuación a una persona con gran experiencia en el trabajo con interfaces GUI y situaciones de prueba. El escenario de prueba, así como el GUI fueron debatidos y se añadieron dos anotaciones. Entonces el GUI fue implementado en Macromedia Director MX.

RESULTADO DEL GUI IMPLEMENTADO

30 Cada una de las fases del proceso de verificación tenía un mensaje escrito (en Sueco) una ilustración y un sonido. Se utilizaron dos sonidos distintos para atraer la atención del conductor a la pantalla. El primero servía como indicación de que se solicitaba una nueva tarea, o que la tarea reciente se había llevado a cabo satisfactoriamente. El segundo sonido fue utilizado para mostrar si la verificación había fallado o había tenido lugar un error. Adicionalmente, la imagen se ponía de color verde en caso de éxito y rojo en caso de fallo. A continuación se indican dos ejemplos del GUI. (Ver figura 14)

SIMULADOR DE CONDUCCIÓN

40 Era necesario un simulador para posibilitar circunstancias lo más reales posibles durante la prueba del prototipo del sistema. VTEC tiene un simulador que fue suministrado para esta prueba. El simulador tiene tres proyectores que iluminan una pantalla arqueada grande. Este tipo de montaje está destinado a aumentar la percepción de desplazamiento real y para posibilitar que el conductor perciba el entorno de manera más natural que cuando se utiliza solamente un proyector y una pantalla plana. Una cabina Volvo FHI2 es situada en medio del recinto, delante de la pantalla. Era posible conectar altavoces con sonido de motor simulado.

50 El simulador había sido utilizado recientemente para pruebas con un automóvil, por lo que la cabina y el simulador no estaban todavía completamente sincronizados. Habían características adicionales que no estaban muy bien adecuadas a la prueba y los autores no tuvieron posibilidad de cambiarlas. Por ejemplo, en el interior, el conductor tenía gas y freno, pero no freno de estacionamiento, embrague, palanca de cambios ni control de crucero. El depósito estaba siempre vacío y no se ajustaron ni el tacómetro ni el odómetro para representar un camión. Dado que no había freno de estacionamiento, el simulador tenía que ser desconectado si el conductor necesitaba hacer una parada y salir del vehículo. Mientras el freno estaba presionado, el simulador no se desplazaba, pero cuando se liberaba el freno (por ejemplo, cuando salía el conductor de la cabina) el vehículo situado continúa desplazándose hacia delante lentamente. (Ver figuras 15 y 16).

PREPARACIONES ANTES DE LA PRUEBA

60 La idea de poner un sistema de verificación dentro de un camión condujo a varias cuestiones con respecto a cuándo sería utilizado este sistema, para qué podría ser utilizado y con qué frecuencia se debería realizar la verificación. Algunas de las cuestiones hipotéticas pueden ser contestadas con ayuda de la prueba de simuladores; otras requieren más investigación y pruebas auténticas.

65 Las preparaciones para la prueba consistieron principalmente en cuatro partes; preparar las cuestiones de la entrevista, diseñar un escenario para el simulador, encontrar un número satisfactorio de sujetos de prueba

apropiados y llevar a cabo una prueba piloto. Tal como se ha mencionado anteriormente, las cuestiones con respecto a cuándo y de qué forma se debería llevar a cabo la verificación se presentaron durante el trabajo preparatorio. Las entrevistas y el escenario de la prueba se diseñaron a efectos de contestar a estas cuestiones (entre otras).

5

ENTREVISTAS

Al acercarse la prueba, las cuestiones de la encuesta se ajustaron para adecuarse a las entrevistas. Para posibilitar una comparación con los resultados de las encuestas anteriores, se hicieron muchas preguntas similares.

10

DESARROLLO DE LAS PREGUNTAS PARA LA ENTREVISTA

Se prepararon dos entrevistas. La primera se mantuvo antes de la prueba del simulador y la segunda, más exhaustiva, se debía realizar posteriormente. Algunas de las preguntas de la entrevista anterior fueron repetidas para comprobar si el conductor había cambiado de opinión durante la prueba. Las preguntas fueron leídas y comentadas por los dos científicos de conducta para ver si algunas de las preguntas debían ser redefinidas, debían recibir añadiduras o debían ser eliminadas.

15

LAS PREGUNTAS

20

La primera entrevista empezó con preguntas con respecto a las rutinas de trabajo del conductor. Las preguntas trataron también temas tales como seguridad y lo que ello significaba para el conductor. Después de investigar los conocimientos del conductor sobre biométrica, se presentaron los diferentes métodos utilizados en la prueba para posibilitar reacciones espontáneas. Se preguntó también al conductor si podía ver alguna ventaja o desventaja en un sistema de verificación.

25

En la segunda entrevista se hicieron preguntas con respecto a la experiencia en pruebas. Se le pidió al conductor que evaluara los diferentes métodos y nuevamente que diera su opinión con respecto a posibles ventajas y desventajas.

30

Muchas de las preguntas fueron calificadas siempre de 1 a 5, de manera que 1 significaba una opinión negativa y 5 una opinión positiva.

35

EL ESCENARIO DE PRUEBAS

Para averiguar lo que se necesitaba en la implementación en el simulador y para intentar ver lo que sería posible someter a prueba, se diseñó un escenario de la prueba.

40

DISEÑO DEL ESCENARIO

Estas nociones sirvieron como inspiración durante la creación del escenario de la prueba. Se definió mediante investigación de ideas y discusiones y ello condujo a un escenario final de la prueba en el que se incluyeron varios aspectos de la prueba. Se deseaba probar el mayor número posible de métodos, tanto en posición de reposo como en condiciones de conducción. Al mismo tiempo, el escenario debería ser lo más realista posible, evitando el riesgo de que pudiera contener demasiadas tareas distintas en la reducida duración de la prueba. De otro modo, el participante de la prueba podría percibir que debe verificar su identidad de manera extremadamente frecuente, lo que no ocurriría en la vida real. El resultado fue un escenario equilibrado pero exhaustivo.

45

EL ESCENARIO DE PRUEBAS

50

El escenario de pruebas empieza con una verificación inicial completa. El conductor debe invertir cierto tiempo para acostumbrarse al simulador antes de pedirle la verificación de las huellas dactilares mientras conduce. Después de aproximadamente la mitad del tiempo en el simulador, tenía que realizar un "paro para un café". Después del paro, el conductor tenía que pasar por una verificación corta utilizando huellas dactilares o voz. Se le pedía todavía otra verificación durante la conducción antes de la terminación de la prueba, siendo esta vez una verificación de voz. Se realizaron dos verificaciones automáticas durante la conducción, una al principio y otra después de la parada. Si fallaban, se pedía al conductor verificación de las huellas dactilares, pero si eran satisfactorias no sería informado sobre las mismas durante la prueba. (Ver figura 17)

55

RECLUTAMIENTO DE LAS PERSONAS DE LA PRUEBA

60

El reclutamiento de conductores de camión para la prueba se confió a una empresa externa, se les pidió que reclutaran 20 conductores y también se les indicó que se deseaba una mezcla de conductores de trayectos largos y conductores de distribución. Durante el reclutamiento los conductores fueron informados que participarían en una prueba de simulador de conducción en la que se evaluaría la capacidad de utilización y aceptación por parte de usuario. El objetivo de esta información vaga con respecto a la prueba durante la fase de reclutamiento fue recibir

65

una mezcla satisfactoria de conductores con diferentes antecedentes y expectativas.

PRUEBA PILOTO

5 Se llevaron a cabo pruebas piloto antes de la prueba real para posibilitar la mejora del sistema y para ajustar el escenario y las entrevistas.

Las preguntas que se deseaba que fueran contestadas en la prueba piloto eran, por ejemplo:

10 ¿Es realista el escenario? ¿Hay demasiadas/pocas tareas, en demasiado tiempo o tiempo no suficiente? ¿Deberían ocurrir los eventos en un orden distinto?

¿Está bien diseñado el GUI? ¿Está claro lo que hay que hacer en todo momento? ¿Se puede oír el sonido y es adecuado en este momento específico?

15 ¿Es aceptable la colocación de la cámara? ¿Puede usted alcanzar con facilidad el sensor de huellas dactilares y el teclado? ¿Parece torpe deletrear la contraseña al aire en vez de hacerlo directamente en un micrófono?

20 ¿Son las preguntas de la entrevista significativas y están correctamente formuladas? ¿Hay demasiadas/demasiado pocas preguntas?

¿Dura demasiado la prueba o se pueden añadir tareas adicionales? ¿Se siente bien siendo filmado y observado por un supervisor de la prueba en la cabina?

25 PROCEDIMIENTO DE PRUEBA PILOTO

Se pidió la participación de empleados en VTEC con diferentes experiencias de conducción de camiones; entre ellos un científico del comportamiento al que se le preguntó de manera específica que diera opiniones sobre las entrevistas. En total participaron seis varones. Tres de ellos pasaron todo el proceso de pruebas con entrevistas, encuesta de aceptación y escenario simulador. Los otros tres no fueron entrevistados, sino simplemente enrolados en el sistema, instruidos con respecto al simulador y pruebas del escenario. Se probaron diferentes condiciones de luz para ver las exigencias para la verificación facial.

35 RESULTADOS DE LA PRUEBA PILOTO

La prueba piloto implicó modificaciones en el sistema para aumentar la estabilidad y capacidad de utilización y para hacer la prueba lo más auténtica y exhaustiva posible. Se añadió un tercer sonido, de manera que el usuario recibía realimentación auditiva cuando marcaba un dígito, en vez de solamente los asteriscos que aparecen en pantalla durante la verificación del PIN. Algunas de las preguntas de la entrevista fueron ajustadas para mayor especificidad.

40 No se pudieron enrolar participantes (para reconocimiento facial) si era demasiado oscuro y resultaba evidente que la luz de las pantallas del simulador por sí misma no era suficiente para el registro. Por otra parte, la sala no debe estar excesivamente iluminada, dado que esto afecta la calidad de la imagen del simulador. Cuando se experimenta con mayor iluminación dentro de la cabina se presentaron problemas con personas que llevaban gafas, dado que el exceso de luz provocaba reflejos. Eventualmente se encontró un ajuste de iluminación que hizo posible enrolar a todos los sujetos de la prueba y que éstos fueran verificados por el sistema. Una observación interesante durante estos experimentos de iluminación fue que era posible identificar algunas personas (que no llevaban gafas) con menos luz en la sala que lo que había ocurrido cuando se había enrolado.

50 LA PRUEBA

Esta sección describe la prueba final del sistema prototipo. La primera parte describe cómo se llevaron a cabo las pruebas y las entrevistas, la segunda parte presenta los resultados.

55 EL PROCEDIMIENTO DE PRUEBA

El sistema de verificación fue comprobado en un simulador, tal como se ha mencionado anteriormente, para hacer la situación de la prueba lo más auténtica posible. Desafortunadamente, dos conductores tuvieron que cancelar, por lo que solamente 18 de los conductores invitados pudieron asistir, todos ellos varones. Los conductores fueron sometidos a prueba y entrevistados uno a uno.

ANTES DE LA PRUEBA DE SIMULADOR

65 Cuando llegó el participante de la prueba que se designará también en adelante como el conductor, fue recibido por el supervisor de la prueba. Fue informado tanto verbalmente como por escrito de sus derechos y obligaciones, por ejemplo, que su anonimato estaba garantizado y que podría interrumpir la prueba en cualquier momento. Se le

explicó que sería entrevistado en primer lugar con respecto a su trabajo y a continuación conduciría el simulador antes de ser entrevistado nuevamente con respecto a su experiencia de la prueba. El supervisor de la prueba pidió permiso para registrar las entrevistas.

- 5 Uno de los inventores era supervisor de la prueba durante todas las pruebas; el otro actuó como técnico y era el responsable de los registros y de las grabaciones de vídeo.

PRIMERA ENTREVISTA

- 10 La fase de prueba empezó con una entrevista con respecto al día ordinario de trabajo del conductor, rutinas en el trabajo, sus opiniones sobre protección y qué tipo de conocimiento y de experiencia tenía sobre biométrica. La primera entrevista duró aproximadamente 20 minutos y fue realizada en una sala de conferencia próxima al simulador. El supervisor de la prueba escribió las respuestas del conductor o las interpretó y las calificó de 1 (valor negativo) y 5 (valor positivo) dependiendo del tipo de pregunta. Si la respuesta a una pregunta de calificación era vaga, se preguntaba al conductor que la calificara entre 1 y 5. En el caso de que el conductor parecía haber entendido mal una pregunta, se le explicaba por el supervisor de la prueba.

PREPARACIÓN

- 20 Después de la entrevista inicial, se mostró el simulador al participante y se le pidió que se sentara y que ajustara el asiento y el volante para una posición de conducción normal y confortable. Antes de empezar la preparación, el técnico verificó que la cámara pudiera tener una visión clara del conductor y, en caso necesario, se pidió al conductor que bajara el volante.
- 25 Se le dio un pin al conductor y entonces empezó la fase de preparación. Se le mostró qué parte de la huella del dedo tenía que colocar sobre el escáner. Dado que el escáner estaba colocado sobre el volante, el participante tenía que utilizar el pulgar de la mano derecha, puesto que los otros dedos serían difíciles de poner en la posición adecuada para el escaneado. Tenía la posibilidad de probar unas pocas veces para colocar el pulgar sobre el escáner para acostumbrarse a la colocación apropiada. Después de ello, se realizó la huella dactilar. El técnico pidió entonces al conductor que mirará recto hacia delante a la pantalla del simulador igual que si estuviera conduciendo, lo cual se hacía para captar el modelo para reconocimiento facial. Para la verificación de voz, se le pidió al conductor que dijera una frase que durara por lo menos tres segundos, para hacer posible que el ordenador la analizara. Se le explicó que el micrófono estaba incorporado en la cámara, de manera que lo único que tenía que hacer era decir la contraseña en voz alta. El conductor recibió como contraseña "Mi nombre es Nombre de pila, "apellido". Tal como se ha indicado anteriormente, la función de la verificación de voz era solamente simulada.

INSTRUCCIONES DEL SIMULADOR

- 40 Cuando se terminó el registro, el conductor recibió la tarjeta inteligente y se le dijo que ésta era su tarjeta de tacógrafo digital personal durante la prueba. Se le pidió entonces que saliera del vehículo para recibir instrucciones con respecto al simulador y al escenario de la prueba.

- 45 El conductor fue informado de que sería filmado durante la prueba y que tenía pleno derecho de interrumpir la prueba en cualquier momento si no se sentía cómodo. Se le indicó que algunas personas sienten náuseas en el simulador, aunque normalmente no se marean en los vehículos. La atención del conductor fue dirigida a la imagen del simulador, que en aquel momento estaba parada en mitad de una carretera. Se le indicó que el supervisor de la prueba se sentaría a su lado dentro de la cabina para guiarle a lo largo de la ruta. Se le dieron instrucciones de que conduciría en la carretera durante un cierto tiempo, luego giraría a la derecha y continuaría hasta llegar a un pueblo. En el pueblo se pararía para un descanso, después del cual el escenario continuaría con otro par de minutos de conducción. El conductor fue informado de los equipos existentes en el simulador y los equipos faltantes (mencionados en *el simulador de conducción*). Se le indicó al conductor que imaginara que el escenario duraba una noche, en vez de los 20 minutos de conducción real.

- 55 Después de estas breves instrucciones, se le pidió al conductor que volviera a entrar en la cabina para empezar la prueba. El supervisor de la prueba entró en el vehículo desde el otro lado y empezó la simulación cuando el conductor estaba sentado y la puerta cerrada.

LA PRUEBA DE SIMULADOR

- 60 El conductor se sentó en el asiento de conducción. El supervisor de la prueba entró en el vehículo desde el otro lado y empezó el escenario cuando el conductor cerró la puerta. Al poner la tarjeta inteligente, empezó la verificación inicial. Esta primera verificación consistía en todos los cuatro métodos y se permitió que el conductor fallara cada uno de los métodos tres veces antes de que el sistema pasara al método siguiente. Si el conductor pasaba, como mínimo, dos de los tres primeros métodos, se consideraba que la totalidad de la verificación inicial era satisfactoria. El cuarto método era el reconocimiento de voz, que fue solamente simulado durante la prueba.

Tal como se ha descrito anteriormente, la prueba empezó en una carretera simulada. Después de un cierto tiempo, el supervisor de la prueba puso en marcha la primera verificación durante la conducción, que era el reconocimiento facial automatizado. Se debe observar que el conductor no había sido informado sobre esta verificación, excepto si fallaba. En caso de que la verificación automatizada fallara, el sistema pediría al conductor que verificara su identidad utilizando verificación de huellas dactilares. Si esto fallaba también, el sistema le pediría al conductor que marcara su PIN.

El participante de la prueba continuó conduciendo y después de un cierto tiempo, el supervisor de la prueba puso en marcha la etapa siguiente que era la segunda verificación durante la conducción. Apareció un diálogo del sistema pidiendo al conductor que verificara su identidad utilizando las huellas dactilares, en caso de que la verificación fallara, se pedía al conductor una verificación por PIN.

Después de un cierto tiempo de conducción, la carretera conducía a un pequeño pueblo en el que se pidió al conductor que parara para un descanso. (Este tuvo lugar aproximadamente 12-13 minutos desde el momento en el que el conductor había entrado en el vehículo para empezar la prueba). El conductor y el supervisor de la prueba salieron del camión y pasaron a otra sala donde se le ofreció un refresco al conductor. Esto tenía dos finalidades; la primera era de simular un descanso corto iniciando un proceso de verificación más corto cuando intentara salir nuevamente. El segundo era proporcionar al conductor la oportunidad de darle al supervisor de la prueba comentarios y reacciones espontáneos sobre la primera parte de la prueba. Para posibilitar comparaciones estadísticas con otros sistemas de automoción, se facilitó una escala de aceptación (56) a los conductores durante el descanso. Dado que el idioma de los participantes era el sueco, todos ellos recibieron una versión de la escala de aceptación en sueco. La escala consiste en nueve pares de palabras contrarias, siendo cinco destinadas a reflejar la utilidad y cuatro la satisfacción. Añadiendo las respuestas con respecto a la utilidad y la satisfacción, respectivamente, se pudo calcular un promedio a partir de ello, y por lo tanto, se pudo calificar la utilidad y la satisfacción entre -2 y +2. El supervisor de la prueba explicó que era solamente el sistema de verificación, no el simulador, el que se tenía que evaluar. Si el conductor no comprendía la escala de aceptación leyendo las instrucciones escritas, el supervisor de la prueba las explicaba adicionalmente y entonces dejaba que el conductor rellenara las respuestas en privado.

Algunos conductores se llevaron la "tarjeta de tacógrafo" al salir para el descanso, pero la mayor parte la dejaron en el dispositivo de lectura. Se continuó la prueba por parte del supervisor al encontrarse al conductor nuevamente en su lugar en el asiento del conductor después del descanso. Si el conductor había dejado su tarjeta, el sistema empezaba nuevamente con la verificación. Si el conductor se había llevado la tarjeta, el sistema empezaba preguntando por la tarjeta antes de empezar la verificación. Para los diez primeros participantes de este sistema, pidió al conductor que verificara su identidad utilizando huellas dactilares y para los ocho restantes se utilizó verificación por voz. Si fallaba esta verificación única, se pedía al conductor que marcara su PIN. El escenario se programó de manera tal que el GUI anunció "verificación de voz satisfactoria" después de unos 6 segundos desde la petición de verificación. Para evitar que los participantes descubrieran la simulación, se les recordó por el supervisor de la prueba, si no habían pronunciado la contraseña suficientemente pronto.

Después de un cierto tiempo, la carretera conducía a una ciudad y el supervisor de la prueba puso en marcha la segunda verificación automática durante la conducción, que era similar a la primera recientemente descrita. Si el sistema no era satisfactorio con la verificación, se informaba al conductor sobre el fallo y se le pedía que verificara su identidad de manera sustitutiva utilizando las huellas dactilares. En caso de que la verificación hubiera fallado también, se le indicaría al conductor que marcara su PIN.

El participante continuó conduciendo después de lo cual el supervisor puso en marcha el último proceso de verificación, verificación de voz durante la conducción. Poco tiempo después de esta verificación, se indicó al conductor que estacionara y detuviera el vehículo.

ENTREVISTA DE SEGUIMIENTO

Después de la prueba, se llevó al conductor nuevamente a la sala de conferencias para ser entrevistado de nuevo. La segunda entrevista trató sobre la experiencia que el conductor había sacado de la prueba en su conjunto, indicando cada uno de los métodos de verificación, el GUI y el escenario.

Se le preguntó al conductor sus experiencias de la primera verificación inicial y las verificaciones durante la conducción (escaneado de las huellas dactilares y reconocimiento de voz, respectivamente). Si las verificaciones automáticas habían tenido éxito, el conductor fue informado de su existencia. Se le animó a indicar sus opiniones sobre la utilización de estos métodos y sobre a la idea de tener que hacer otro tipo de verificación en el caso de que la automática hubiera fallado. Se pidió a los conductores que no habían sido verificados satisfactoriamente por la verificación automática con respecto a sus experiencias, el tener que hacer otro tipo de verificación durante la conducción. También se les animó a que indicaran sus opiniones sobre la verificación automática mientras conducían. Para posibilitar comparaciones de los diferentes métodos y verificaciones que habían tenido lugar en la prueba, el conductor recibió las mismas preguntas para cada ocasión, respectivamente. Las preguntas repetidas eran para calificar (de 1 a 5) si la verificación/método era complicado o fácil, pesado en cuanto a tiempo o rápido,

extraño o razonable, aburrido o divertido, sin interés o interesante, e innecesario o necesario.

Se interrogó al conductor sobre sus ideas con respecto a la protección y a la implementación de un sistema de verificación en un vehículo. Se le animó a indicar sus impresiones anteriores a la prueba y después de la prueba, para ver si la prueba había cambiado su opinión. Antes de terminar la sesión, se le preguntó al conductor si deseaba añadir algo, si faltaba alguna cosa en la prueba, o si tenía algunas preguntas que hacer.

RESULTADOS DE LAS PRUEBAS

Esta sección empieza con una introducción de los participantes de la prueba. Después, los resultados de la primera entrevista, la prueba de simulador y la entrevista detallada siguientes, serán presentados. Todas las entrevistas fueron mantenidas en suceso, por lo que las contestaciones presentadas en esta descripción son traducciones hechas por los autores.

El promedio de edad de los participantes era de 41 años, con una desviación estándar de once años. El participante más joven tenía 23 años y el mayor, 60 años. Los participantes habían trabajado como conductores de camión durante un promedio de 18 años, variando de tres a cuarenta. Cuatro de los conductores conducían puramente vehículos a larga distancia, seis de los conductores conducían principalmente en el área local de Gothenburg y los otros ocho restantes conducían en recorridos mixtos.

RESULTADOS DE LA PRIMERA ENTREVISTA

A la pregunta de lo que significaba "protección" para ellos, la mayor parte de conductores hablaron de vehículos seguros. Cuando la cuestión fue especificada en protección contra acciones delictivas, la mayor parte de conductores hablaron de la alarma de gas que muchos conductores de largo recorrido tienen en sus vehículos. Todos los conductores dijeron que se sentían seguros en su trabajo, excepto uno que no se calificó ni de seguro ni de inseguro. El promedio de la calificación fue 4,78 con una desviación estándar de 0,55. El entorno o área en el que uno está conduciendo puede afectar al sentimiento de seguridad, de acuerdo con diez de los conductores. Tres de ellos creyeron que el tiempo era también un factor junto con el entorno. De acuerdo con tres de los conductores, hay otras cosas que pueden afectar a su sentimiento de seguridad, por ejemplo, el tipo de carga que están transportando. Dos de los conductores se sintieron seguros en cualquier caso, y no apreciaron factores que afectaran este sentimiento de seguridad.

Todos, excepto uno, utilizaron una tarjeta en su trabajo para conseguir acceso a lugares o áreas específicas. El que no utilizaba tarjeta alguna utilizaba un PIN para tener acceso. Ocho de los conductores utilizaba tanto tarjetas como PIN.

Once de los conductores compartían su vehículo con uno, o más, otros conductores. Los otros tenían su propio vehículo personal, pero algunos de ellos dijeron que en caso de enfermedad, otros conductores podían conducir el vehículo, y también ocurría que prestaban su vehículo a otra persona.

Solamente dos conductores pudieron mencionar métodos biométricos sin ayuda alguna del entrevistador. Dos no pudieron aportar ningún otro método aunque se les indicó la verificación de las huellas dactilares como ejemplo. A pesar de que tres conductores habían sido verificados/identificados con métodos biométricos, ninguno de ellos sentía oposición hacia los mismos. Los que nunca habían utilizado ningún sistema biométrico puntuaron en un promedio de 4,20 en una escala de 1 (negativo) a 5 (positivo), con una desviación estándar de 1,42. Entre ellos, once eran positivos y todos ellos puntuaron 5. Un conductor puntuó 1, dos puntuaron 2, y el otro puntuó 3, con el significado de que ni negativo ni positivo.

Cuando se les preguntó sobre los posibles inconvenientes de la utilización de métodos de verificación biométrica, seis conductores apreciaron riesgos. Por otra parte, dos de estos conductores podrían apreciar también posibilidades o ventajas para los sistemas biométricos. Diez conductores pudieron apreciar solamente ventajas y positividad. Los otros dos restantes no contestaron a las preguntas.

RESULTADOS DEL ESCENARIO DE PRUEBAS

El sistema funcionó bien a lo largo de las 18 pruebas. Esta sección explicará brevemente el resultado. Se debe observar que los resultados simplemente explican la frecuencia con la que los participantes lograron pasar la verificación. Los autores han probado el sistema brevemente en cuanto a una falsa aceptación. No ha tenido lugar ningún caso.

VERIFICACIÓN INICIAL

La verificación inicial consistía en todos los métodos de verificación implementados. Como mínimo, uno de los métodos tuvo éxito en todos los participantes, por lo que todo quedó aprobado para poner en marcha el motor.

Todos los 18 participantes tuvieron éxito con la verificación de PIN. Uno marcó el código erróneamente una vez pero tuvo éxito en su segundo intento.

5 La verificación de las pruebas dactilares fue satisfactoria para 14 participantes. Uno de estos 14 participantes necesitó más de un intento. Algunos de los participantes fueron guiados en cuanto al lugar donde poner el pulgar si fallaba el sistema en la localización de la huella. (Tal como se ha descrito en lo anterior con respecto a la teoría, es un problema habitual, que el dedo no se coloque correctamente.)

10 Un solo intento fue suficiente para un reconocimiento facial satisfactorio para 11 de los participantes. En definitiva, el reconocimiento facial tuvo éxito en 16 participantes.

El reconocimiento de voz fue simulado y, por lo tanto, todos los participantes pasaron la prueba, aunque algunos de ellos necesitaron que se les recordara lo que había que decir.

15 Uno de los participantes no fue verificado por la verificación de huellas dactilares ni reconocimiento facial, pero fue aprobado dado que el PIN había sido correcto. Dos de los otros participantes no fueron verificados por la verificación de huellas dactilares. En estos casos, el reconocimiento facial requería dos intentos antes de alcanzar verificaciones satisfactorias. La verificación facial o la verificación de huellas dactilares provocó problemas en la verificación de tres de los participantes restantes. A pesar de ello, todos fueron verificados satisfactoriamente dado que todos los métodos pudieron ser comprobados más de una vez.

PRIMERA VERIFICACIÓN DURANTE LA CONDUCCIÓN (RECONOCIMIENTO FACIAL AUTOMÁTICO)

25 El sistema reconoció automáticamente 13 de los participantes. Dos de los que no habían sido reconocidos automáticamente tuvieron que marcar su PIN, dado que también había fallado la verificación de las huellas dactilares.

SEGUNDA VERIFICACIÓN DURANTE LA CONDUCCIÓN (VERIFICACIÓN DE HUELLAS DACTILARES)

30 La verificación de huellas dactilares fue satisfactoria para 13 de los conductores, entre los cuales 10 pasaron en el primer intento. Los restantes pasaron la verificación de PIN en el primer intento.

RESULTADOS DE LA ESCALA DE ACEPTACIÓN (DURANTE EL PARO DE DESCANSO)

35 Las preguntas que habían sido contestadas durante el paro de descanso mostraron que el sistema era percibido como más útil que satisfactorio. Ver a continuación la calificación promedio de cada participante con respecto a la utilidad y satisfacción (entre una escala de -2 y +2). (Ver figura 18)

40 Dado que la escala se supone que presenta cinco preguntas sobre la utilidad del sistema y cuatro preguntas sobre la satisfacción, se hizo un cálculo de las contestaciones para ver si el conductor había puntuado de manera similar en todas las cuestiones de satisfacción y en todas las cuestiones de utilidad, respectivamente. Se utilizó Alpha de Cronbach para este cálculo. En este caso, la estadística de fiabilidad para la escala de aceptación puntuó 0,787 para la utilidad y 0,698 para la satisfacción, lo que indica que los conductores percibieron las cuestiones tal como se había pretendido.

45 Las cuestiones variaron entre los participantes dado que todas las preguntas habrían recibido, como mínimo, una calificación máxima, y todas ellas habrían recibido, como mínimo, una calificación mínima. Ninguno de los conductores percibió el sistema como inútil, pero tres de ellos lo calificaron con tendencia a malo y tres no lo calificaron ni como malo ni bueno. Las calificaciones de utilidad puntuaron de promedio 0,80 con una desviación estándar de 0,72 y la satisfacción puntuó con un promedio de 0,24 con una desviación estándar de 0,89. Algunos de los conductores percibieron el sistema como irritante. Los comentarios verbales indicaron que era, especialmente la verificación durante la conducción, lo que provocaba la irritación. Por lo tanto, el sistema no le gusta a todo el mundo, pero hubo más contestaciones positivas que negativas.

55 VERIFICACIÓN DESPUÉS DE LA PARADA CORTA DE DESCANSO (VERIFICACIÓN DE HUELLAS DACTILARES/VOZ)

60 Los primeros diez participantes utilizaron verificación de huellas dactilares antes de poner en marcha el vehículo después del descanso. Nueve de estos diez fueron verificados, ocho de ellos en sus primeros intentos. El participante que no fue verificado satisfactoriamente tuvo que marcar su código para ser autorizado. La verificación de PIN fue satisfactoria en el primer intento.

65 Los ocho participantes restantes utilizaron reconocimiento de voz. Esta verificación fue simulada, de manera que todos aprobaron, aunque el instructor de la prueba tuvo que recordar a algunos de los conductores lo que tenían que decir.

TERCERA VERIFICACIÓN DURANTE LA CONDUCCIÓN (VERIFICACIÓN FACIAL AUTOMÁTICA)

5 La verificación automática verificó satisfactoriamente 15 de los participantes, 12 de ellos fueron verificados en el primer intento. La siguiente verificación de huellas dactilares tuvo éxito en el primer intento para dos de los tres participantes restantes. El tercero tuvo que marcar su PIN, dado que la verificación de las huellas dactilares había fallado también. Fue verificado satisfactoriamente por medio de su PIN en el primer intento.

CUARTA VERIFICACIÓN DURENTE LA CONDUCCIÓN (VERIFICACIÓN DE VOZ)

10 La cuarta verificación durante la conducción era el reconocimiento de voz y, dado que era simulado, todos los participantes la pasaron.

RESULTADOS DE LA ENTREVISTA DE SEGUIMIENTO

15 La entrevista preguntaba cuestiones específicas con respecto a los diferentes métodos, así como otras preguntas más generales relativas a los métodos biométricos y a la verificación. Además, los conductores fueron preguntados sobre el GUI y los sonidos relacionados con el mismo. Todo esto es presentado en esta sección y, por lo tanto, ha sido dividido en diferentes partes.

20 LA PRIMERA RESPUESTA AL SISTEMA

La primera respuesta de los conductores después de la prueba fue básicamente positiva. Nueve de los conductores percibió la prueba como realista. Siete de los conductores creyó que era una visión del futuro. Un conductor encontró la prueba no realista y el conductor restante no dio una respuesta específica a la pregunta.

25

EL GUI Y SUS SONIDOS

30 Todos los conductores menos uno dieron la calificación más alta (5) al GUI. Esta persona le dio el grado 3, por lo que el GUI fue calificado con un promedio de 4,89. Doce de los conductores habían percibido los sonidos relacionados con el GUI. *“incluso me di cuenta de las diferencias entre cuando es correcto y cuando es erróneo”* dijo uno de los conductores como respuesta a la pregunta de si era bueno o malo el disponer de sonidos los conductores lo calificaron con un promedio de 4,5 con una desviación estándar de 1,24. Parece que a los conductores o les gustó o no les gustó los sonidos, puesto que diez de los doce conductores que habían percibido los sonidos los marcó 1 ó 5. La calificación promedio fue de 3,38, con una desviación estándar de 1,89, por lo que es difícil decir si los sonidos ayudaban o molestaban.

35

40 Los conductores manipularon el GUI por sí mismos e hicieron espontáneamente lo que se suponía que harían aunque no habían recibido instrucciones de antemano. En algunos casos, deseaban empezar y le pidieron al supervisor de la prueba si podían introducir la tarjeta antes de que el GUI hubiera empezado, pero en estos casos el primer mensaje se mostró habitualmente antes de que el supervisor de la prueba hubiera tenido tiempo de contestar. Una persona marcó erróneamente el tercer dígito, a continuación se dirigió al supervisor de la prueba: “He marcado el número erróneo, ¿qué debo hacer ahora?” el supervisor de la prueba le animó a probar de hacer lo que él creyera que era apropiado, después de lo cual utilizó instintivamente el botón apropiado para borrar el dígito erróneo y continuar normalmente.

45

LA VERIFICACIÓN INICIAL

50 Todos los conductores encontraron que la primera verificación, antes de empezar el viaje, era fácil. La calificación promedio para la facilidad de utilización era de 4,89, con una desviación estándar de 0,32. (Dos calificaron 4, el resto calificó 5). Diez de los conductores creyeron que era razonable hacer esta verificación. Uno no sabía si era razonable o si resultaba raro. Los siete restantes creyeron que era raro o un poco raro. A la pregunta de la necesidad, la calificación promedio fue de 3,14, con una desviación estándar de 1,80. Con todas las preguntas resumidas, esta primera verificación recibió la calificación promedio de 3,71, con desviación estándar de 0,68.

55 VERIFICACIÓN FACIAL AUTOMÁTICA

60 Cuando se les explicó que había tenido lugar una verificación automática utilizando la cámara, muchos de los conductores creyeron que era una buena idea. Los conductores que no fueron verificados por la cámara y que tuvieron que hacer la verificación de las huellas dactilares creyeron que era muy razonable. Los que habían sido verificados sin saberlo eran muy positivos frente a la idea de que se habían fallado deberían pasar una verificación de huellas dactilares.

65 Uno de los cuatro en los que falló el sistema de verificación fue negativo en cuanto al sistema. Con respecto a los otros, no es posible sacar ninguna conclusión de la correlación entre la verificación satisfactoria/fallo y la percepción del sistema por parte del conductor. A uno de ellos no le importó ni siquiera el hecho de que el sistema había intentado la verificación automática ni que tuviera que hacer otras verificaciones al fallar el sistema en la

verificación automática. Sin embargo, otro dijo que era bueno que el sistema llevara a cabo la verificación automática, pero que si no era satisfactoria, debería alertar al conductor para que se sentara correctamente, de manera que la verificación pudiera tener lugar. A la cuarta persona no le gustó ninguna de las verificaciones durante la conducción y, por lo tanto, no le gustó la verificación automática. *“Cuantas menos cosas ocurran durante la conducción, mejor.”*

VERIFICACIÓN DE HEULLAS DACTILARES DURANTE LA CONDUCCIÓN

La primera verificación durante la conducción, cuando los conductores tenían que realizar un escaneado de huellas dactilares, no fue percibida tan fácil como la primera verificación. La verificación de huellas dactilares durante la conducción fue calificada de 3,19 con un promedio, con una verificación estándar de 1,67. Esta verificación tendió más a ser percibida como rara en vez de razonable. En una escala de 1 (rara) a 5 (razonable) el escaneado de huellas dactilares mediante la conducción se calificó con un promedio de 2,94, con una desviación estándar de 1,86. La cuestión de si esta verificación era necesaria o no se calificó 3,11 con una desviación estándar de 1,78. Como calificación global, la calificación de huellas dactilares durante la conducción fue calificada de 3,19 con una desviación estándar de 0,38.

VERIFICACIÓN DESPUÉS DEL DESCANSO (HUELLAS DACTILARES/VOZ)

Después del paro de descanso, los primeros diez conductores se verificaron a sí mismos por las huellas dactilares, los otros ocho utilizaron la verificación de voz. Independientemente del método que utilizaron, todos los conductores calificaron esta verificación como fácil. Con los dos métodos a la vez, esta verificación fue calificada como 4,17, con tendencia a razonable en vez de rara, con una desviación estándar de 1,50. La necesidad fue calificada como una 3,78 con desviación estándar de 1,83. Con todas las preguntas incluidas y ambos métodos añadidos, la verificación fue de 4,12 con una desviación estándar de 0,68.

Los que habían utilizado la verificación de huellas dactilares después del descanso, la calificaron con un promedio de 4,60 con tendencia a razonable, con una desviación estándar de 0,97. La necesidad fue calificada con un promedio de 4,40, con una desviación estándar de 1,35. Una persona falló la verificación de huellas dactilares y, por lo tanto, tuvo que marcar también su PIN. A pesar de ello, calificó con un 5 tanto en la facilidad de utilización como por encontrar este sistema razonable, pero calificó con un 3 la cuestión de necesidad.

Los que habían tenido que hacer la verificación de voz después del descanso, calificaron con un promedio de 3,63, con desviación estándar de 1,92, la pregunta de si esta verificación era rara (1) o razonable (5). No se calificó ni como necesaria ni como innecesaria, dado que el promedio de esta pregunta fue de 3,00 con una desviación estándar de 2,14. A algunos de los conductores se les tuvo que recordar la contraseña. Esto se hizo solamente para evitar que los participantes descubrieran que esta verificación era simulada.

VERIFICACIÓN DE VOZ DURANTE LA CONDUCCIÓN

La segunda verificación durante la conducción fue simulada, por lo tanto, nunca falló, aunque algunos conductores cometieron pequeños fallos cuando expresaron la contraseña. Alguno de los conductores que no había utilizado la verificación de voz después de la verificación inicial necesitó que se le recordara la contraseña. Todos los conductores que habían utilizado la verificación de voz después del descanso contestaron rápidamente al sistema. La verificación fue percibida como fácil, dado que todos los conductores la puntuaron con un 5, sin excepciones. A la pregunta de si era razonable o extraño hacer esta verificación, el promedio de calificación fue de 3,41 con una desviación estándar de 1,84. Se consideró necesaria la última verificación, dado que se calificó con un promedio de 2,71 con una desviación estándar de 1,99. Con todas las preguntas resumidas, esta verificación se calificó con un 3,65, con la desviación estándar de 1,08.

GENERALIDADES RESPECTO LOS MÉTODOS

Cuando se preguntó sobre los métodos de verificación en general, lo que sintieron los conductores por la utilización de las huellas dactilares, voz, verificación facial o código, la verificación de voz se calificó con el promedio más elevado de 4,61 y desviación estándar de 0,66. La verificación de huellas dactilares y la verificación de voz comparten la mayor calificación en cuanto a confianza. Ambos recibieron 4,28 como calificación promedio. La verificación de huellas dactilares tuvo una desviación estándar de 1,23, y la de voz 1,27. La verificación facial fue calificada 3,67 como promedio y la verificación de código 3,62 en la pregunta de confianza. Tenían desviaciones estándar de 1,61 y 1,60, respectivamente.

A algunos de los conductores no les gustó la colocación del escáner de huellas dactilares ni la pantalla del GUI. No querían retirar la vista de la carretera y sugirieron instrucciones verbales de forma alternativa y el GUI más próximo al volante o integrado en el conjunto de instrumentos. Otra sugerencia fue colocar el dispositivo de huellas dactilares al lado derecho del asiento del conductor.

Al final de la entrevista los conductores fueron animados a evaluar los métodos de verificación controlados según su orden de preferencia. El más preferido como número uno, el segundo caso dos y así sucesivamente. La mitad de los participantes prefirió identificación de huellas dactilares. El reconocimiento facial, reconocimiento de voz y PIN fueron preferidos por tres participantes cada uno de ellos. Respecto a la calificación promedio para esta evaluación de preferencia, las huellas dactilares fue el más aceptado y el reconocimiento facial resultó segundo, aunque el reconocimiento de voz no se clasificó muy lejos. Solamente dos conductores mencionaron la tarjeta. Uno de ellos creyó que era el segundo mejor método después del PIN, pero otro simplemente la calificó como último lugar, después de los demás métodos. Es posible que los conductores no percibieran la tarjeta como método de verificación, dado que se presentó como su tarjeta de tacógrafo, en este caso, se podría explicar que nadie más la mencionó.

Uno de los participantes creyó que la verificación de huellas dactilares era la menos fiable, si bien encontró que el reconocimiento facial era el mejor dado que ni siquiera se dio cuenta de él. Otro participante prefirió las huellas dactilares aunque las percibía como el método más difícil de utilizar. Aceptó el reconocimiento facial como el método más fácil, pero no le gustaba dado que se sintió incómodo por tener una cámara delante de él.

GENERALIDADES CON RESPECTO A TEMAS DE VERIFICACIÓN

Diez de los conductores hubieran querido tener este tipo de sistema en su vehículo. No obstante, solamente dos deseaban todos los métodos, ocho de los conductores creyeron que sería suficiente tener un método de verificación, uno no quería ningún método y el resto de los conductores tenían varias recomendaciones de más de un método pero no todos ellos. El número promedio de los métodos deseados en el sistema era de 1,72 con una desviación estándar de 1,32.

Cinco de los que antes de la prueba no apreciaban desventajas de tener verificaciones biométricas vieron desventajas después de la prueba. Cuatro de los que encontraban desventajas después de la prueba contestaron después de manera distinta. Uno que podía ver ventajas antes de la prueba no las veía posteriormente. Cinco conductores pudieron apreciar ventajas después de la prueba que no habían visto antes.

A 15 participantes que no habían utilizado nunca sistemas biométricos antes de esta prueba se les preguntó en la primera entrevista si eran positivos (5) o negativos (1) a los métodos de verificación biométrica. Después de la prueba de simulador se les pidió nuevamente qué pensaban ahora de los métodos de verificación biométrica, después de la prueba. Seis de los participantes puntuaron de manera más negativa después de la prueba que antes, tres participantes puntuaron de manera más positiva y seis participantes puntuaron igual que antes. Estas respuestas son presentadas en el diagrama anexo (ver figura 19)

Observando sus calificaciones, once de los 15 conductores eran positivos a los sistemas biométricos (puntuación 4-5), dos de ellos eran negativos (puntuación 1-2) y dos no eran ni positivos ni negativos (puntuación 3).

Es notable que varios de los participantes se describieron a sí mismos más positivos después de la prueba que antes, aunque no dieron una calificación más elevada que la anterior.

Dado que se pidió a los participantes después de la prueba que indicaran lo que habían puntuado antes, se supone que algunos de ellos dijeron de sí mismos que habían puntuado más bajo antes que lo que realmente habían puntuado.

Cuatro participantes entre la totalidad eran más positivos en cuanto a disponer de sistemas biométricos en el vehículo que en otras situaciones. Otros cuatro pensaban de modo opuesto, que los sistemas biométricos son OK, pero no en el vehículo. Los conductores restantes calificaron igualmente los sistemas biométricos en el vehículo y sistemas biométricos en general. Como calificación promedio, un sistema de verificación en el vehículo recibió 3,78 con desviación estándar de 1,35. Los sistemas biométricos en general recibieron un promedio de 3,76 con una desviación estándar de 1,48.

Varios conductores fueron positivos a la idea de un sistema de verificación en los vehículos, pero dijeron que no tenían necesidad del mismo en su trabajo diario. El hecho de que personalmente no habían estado expuestos a delitos o ataques, era un comentario frecuente de los conductores. Creyeron que podría ser más fácil contestar las preguntas de la entrevista si se vieran forzados a pensar en estos temas. Dado que se sentían seguros en su trabajo, dijeron que era difícil para ellos relacionarse con los problemas.

RESULTADOS TÉCNICOS GENERALES

Esta sección muestra algunas observaciones realizadas durante las pruebas con respecto a la tecnología.

SISTEMA DE VERIFICACIÓN POR HUELLAS DACTILARES

El sistema de huellas dactilares funcionó bien a lo largo de las pruebas. En unas pocas ocasiones el sistema no dio respuesta, pero esto es más probable que dependa de problemas con el puerto COM en el PC principal que en el sistema BioCore II. Ningún participante falló la fase de realización, aunque en algunos casos se requirieron varios intentos para conseguir una imagen suficientemente satisfactoria. Todos los participantes tuvieron éxito por lo menos una vez en su propia verificación utilizando las huellas dactilares.

SISTEMA DE VERIFICACIÓN FACIAL

El sistema de verificación facial tenía un comportamiento más estable que el de la verificación de las huellas dactilares. Ningún participante falló la realización de la prueba facial. No obstante, uno de los participantes no pudo empezar hasta después de haberse quitado la gorra de béisbol. Es posible que la gorra arrojara sombras sobre su cara que eran una complicación para el sistema.

También ocurrieron algunos problemas con las gafas. La razón de ello es que los reflejos en las gafas las pueden hacer opacas a la cámara. En una ocasión, la fase de realización tuvo que ser repetida, dado que el algoritmo de reconocimiento facial no logró localizar la posición de los ojos del conductor. Este conductor llevaba gafas y fue también el único en fallar las tres verificaciones faciales durante la prueba.

SISTEMA DE RECONOCIMIENTO DE VOZ

El sistema de reconocimiento de voz fue solamente simulado durante las pruebas y, por lo tanto, no es posible decir nada de la funcionalidad de este sistema.

ANÁLISIS Y RESUMEN DE LOS RESULTADOS

Los participantes eran más positivos que negativos con respecto al sistema de verificación y eran principalmente positivos a la idea del utilizar verificación biométrica en sus vehículos. La verificación de las huellas dactilares era, tal como se ha indicado, el sistema que preferían más participantes y también logró las calificaciones promedio más elevadas. Era también el método que conocían la mayor parte de los participantes. Los que pudieron participar en más ejemplos decían que habían visto algo en películas y habían hablado con respecto a escaneado de los ojos y reconocimiento facial/de voz, no obstante, parecía que incluso aquellos que podían mencionar otros métodos percibían estos métodos como futurísticos. Es posible que el sentimiento futurístico influenciara su elección del método preferido.

Varios participantes eran positivos al reconocimiento facial, pero no se debe olvidar que otros se sintieron controlados por el sistema y no les gustó la cámara. Un conductor dijo: *“me gusta la libertad que comporta este trabajo. Siempre que haga las cosas que se deben hacer, lo puedo hacer de la forma que a mi me gusta, no es asunto de nadie más. Con este sistema me sentí como si yo no tuviera ya el control. Era el sistema que me decía cuándo podía conducir o no”*. Este participante y otro más dijeron que pensarían en cambiar de trabajo si se imponía por ley la verificación de los conductores. Los restantes participantes no fueron tan drásticos pero comentaron que no estaban acostumbrados a utilizar un sistema como este. Las oportunidades de formación e información podrían aumentar la aceptación positiva del sistema.

Otro ejemplo de cuándo la información es importante para conseguir aceptación es que varios participantes cuestionaron la necesidad de verificación durante la conducción. No obstante, cuando el supervisor de la prueba y los participantes hablaron sobre ello después de las entrevistas y el participante preguntó sobre la verificación durante la conducción, el supervisor de la prueba facilitó este ejemplo: *“Imaginemos un conductor de camión que ha sido verificado y ha puesto en marcha el motor cuando observa que hay un cable que se tiene que fijar en la carga. Cuando el conductor sale de la cabina para arreglar el cable un impostor puede ocupar su sitio e intentar salir con el vehículo”*. Los participantes dijeron que esto era algo en lo que no habían pensado antes, pero dijeron que ello sucedía cuando salían de la cabina, después de haber puesto en marcha el vehículo. Con la explicación de porqué el conductor debía ser verificado durante la conducción, los participantes lo percibieron como razonable, aunque no deseaban ser molestados por una verificación de huellas dactilares. El reconocimiento facial o de voz fueron más apreciados durante la conducción.

Un sistema de verificación en vehículos comerciales debería ser desarrollado con respecto a la intimidación de los conductores. En este caso, será probablemente bien recibido, dado que la mayor parte de participantes tenían una actitud positiva ante la idea.

CONCLUSIONES

El sistema que ha sido probado es un prototipo y el sistema no es suficientemente estable para su utilización en la práctica. Con métodos de verificación especialmente adaptados para objetivos de automoción, combinados con el sistema de control incorporado en vez de ambos ordenadores, es probable que se pueda conseguir un sistema

estable, seguro y consistente. Se recomienda la verificación automática durante la conducción, no obstante, si los problemas de sensibilidad a la luz continúan el sistema de reconocimiento por voz parece ser el segundo mejor sistema. La razón de ellos es que el reconocimiento de voz no requiere gran atención por parte del conductor, pero el método tiene que ser probado antes de que sea posible decir que es realmente adecuado para su utilización en vehículos.

La verificación del PIN es un método adecuado desde un punto de vista técnico, pero la mayor parte de los usuarios preferían verificación biométrica, dado que el PIN es otro código que hay que recordar. El método funcionaba razonablemente bien en parado, pero no se sugiere su utilización durante la conducción, dado que algunos de los conductores casi perdieron el control del vehículo cuando marcaban el código. Lo mismo se puede decir para la exploración de las huellas dactilares, algo que los propios conductores comentaron.

Tal como se ha mencionado en los resultados, a algunos de los conductores no les gustaba esta colocación del escáner de huellas dactilares, pero aparte de ello, este método de verificación es rápido y fiable. Si los usuarios reciben formación, es muy probable que sea apropiado con el objetivo de verificar al conductor del camión. Las manos sucias no se supone que provoquen ningún problema, dado que todos los participantes entraron en la prueba y fueron verificados aunque la mayor parte de ellos llegaron a la prueba directamente del trabajo (por lo tanto, era una situación auténtica para el escaneado de los dedos, dado que era similar a si hubieran entrado en sus propios vehículos). El escáner debe ser colocado de manera que sea fácil escanear cualquiera de los dedos de la mano derecha en vez de lo que se hacía ahora, cuando solamente el pulgar podía ser utilizado para verificación. Un escáner más grande, preferentemente con guías para los dedos para encontrar la posición adecuada, facilitaría la verificación a los usuarios. Aunque la verificación de las huellas dactilares fue la preferida entre los participantes de la prueba, no debe ser el único método en un sistema de verificación, dado que no todo el mundo tiene huellas dactilares suficientemente distinguibles para escaneado.

La tecnología de reconocimiento facial no está suficientemente madura para estos tipos de aplicaciones dado que es demasiado sensible a la luz. No obstante, la verificación facial recibió una puntuación alta y la mayor parte de los conductores era positiva a la verificación automática. Esto indica que la verificación facial es preferida, desde el punto de vista del usuario. Sería importante asegurar a los conductores que no se encontraban continuamente bajo control, dado que algunos de los conductores se sintieron incómodos al mirar a una cámara durante la totalidad de la conducción. La forma en que se puede hallar este equilibrio entre el control del conductor y su intimidad se debe investigar todavía adicionalmente.

Varios de los conductores fueron positivos al sistema de reconocimiento de voz, pero dado que se simuló que tenía éxito en todos los casos, no fue posible sacar conclusiones sobre la forma en que se adaptaría realmente al contexto de los camiones. Especialmente por el hecho de que muchos conductores no confiaban en el mismo al inicio debido a experiencias desfavorables con sistemas de reconocimiento de voz, esta verificación falsa les dio una falsa confianza.

Las percepciones de los conductores sobre si los sonidos GUI ayudaban o solamente molestaban, variaban notablemente. Se sugiere, por lo tanto, que el usuario debe ser capaz de conectar/desconectar el sonido.

El mayor escepticismo sobre los contratistas de transporte interrogados se encontraba contra la tecnología. “¿Qué ocurre si falla?” era una pregunta corriente. La mayor parte de ellos veían también problemas si algo le ocurría al conductor, un accidente u otra cosa que le incapacitara para desplazar el vehículo. “Debe haber siempre una forma de desplazar el vehículo de uno u otro modo”. Asimismo, los participantes en la prueba pusieron énfasis en la importancia de una solución para el desplazamiento del vehículo en el caso de accidentes. Además, los participantes de la prueba pidieron posibilidades de cambiar el conductor de un vehículo con un aviso con poca anticipación. Se comentan soluciones a estos problemas en la sección 6.10, *aspectos en la automoción*.

Para resumir los resultados, se considera que es posible crear un sistema de verificación adecuado para un ambiente de automóvil. No obstante, no se debe olvidar que es casi imposible eliminar todos los riesgos. Por ejemplo, el IRA utiliza solamente personas desconocidas para las autoridades para cualesquiera operaciones importantes. Esta táctica es habitual en muchos ataques terroristas, tanto si son un suicida o un secuestrador de un avión. Otro ejemplo es que varios de los terroristas que llevaron el ataque contra el World Trade Center utilizaron sus propias identidades, por lo tanto, aunque todos los conductores serían identificados, sería imposible asegurar que sus vehículos no se utilizarían nunca en acciones terroristas. Hay numerosos ejemplos de sucesos no deseados a pesar de haber tomado precauciones. No obstante, un sistema de verificación en un camión intimidaría probablemente a los impostores y terroristas, lo que sería una ventaja tanto para el conductor como para el contratista de transporte y, a largo plazo, se extendería a toda la sociedad.

ESTUDIOS FUTUROS

Los descubrimientos que se han comentado dan un camino para buscar adicionalmente muchos aspectos distintos de la idea y las posibilidades de la verificación de conductores. Se han presentado muchas cuestiones durante el proceso de trabajo, pero no ha sido posible, dentro de un tiempo razonable, contestarlas todas ellas dentro de esta

invención. Este sistema simulado y las entrevistas dieron una idea de las opiniones de los conductores, pero a pesar de ello es importante probar el sistema bajo condiciones más reales. Por lo tanto, para futuros estudios se sugiere implementar el sistema en un camión real y hacer las pruebas. A continuación, se indican diferentes cuestiones de interés que se deben tomar también en consideración.

5 VERIFICACIÓN DE HUELLAS DACTILARES

Dado que algunos conductores se sentían poco cómodos con la colocación del sensor, sería interesante encontrar una colocación mejorada.

10 El sistema debe ser comprobado en conducciones reales, a efectos de investigar la forma en la que la suciedad, cicatrices, callosidades, etcétera, afectan el comportamiento del sistema.

15 RECONOCIMIENTO FACIAL

Para futuros estudios, se sugiere montar el sistema en un camión real y llevar a cabo pruebas en condiciones reales. Durante la prueba se debería filmar al conductor y se deberían medir las condiciones de luz en la cabina, a efectos de probar en qué circunstancias el sistema es funcional. Estas pruebas se deberían complementar con entrevistas a fondo con los usuarios para ver si aceptan tener una cámara dentro de la cabina. Este es un tema importante, dado que algunos de los conductores no se sentían cómodos con la cámara dirigida hacia ellos durante la prueba, mientras que a otros no les molestaba en absoluto y les gustaba la idea de la verificación automática. Este sistema podría necesitar restricciones en la forma en que podría ser utilizado, por lo que podría ser necesario crear nuevas leyes para estas circunstancias de control mediante una cámara.

25 Cuando la termografía se desarrolle en mayor medida, se debería considerar utilizar este método en el sistema de verificación. Entonces, el método debería ser probado durante diferentes circunstancias en tiempos variables a lo largo del día, preferentemente en un camión real.

30 En el límite entre los intervalos de longitud de onda visible e infrarroja, se puede encontrar el intervalo llamado NIR. El problema con la termografía facial es que no hay sistema de verificación viable disponible en el mercado, por lo que sería problemático utilizar un sistema normal de reconocimiento facial, dado que es sensible a las condiciones de luz. Utilizando una cámara NIR, podría ser posible resolver estos problemas, dado que la cara del conductor podría ser iluminada con diodos NIR, invisibles para él pero no para la cámara.

35 RECONOCIMIENTO DE VOZ

En primer lugar, es deseable comprobar un sistema de verificación de voz que funcione. Si los resultados son satisfactorios, el sistema debería ser probado en cuanto a su estabilidad en un camión real. Ello, dado que el nivel de ruido en el simulador no varía particularmente. El ruido se puede eliminar frecuentemente por filtrado y el sistema VoiceKey se adapta a nivel de ruido real (dentro de límites razonables). No obstante, se debe comprobar si las variaciones de ruido en un camión real se encuentran dentro de estos límites.

45 Dado que podría parecer algo torpe para el conductor el hablar en voz alta directamente en el aire, puede ser necesario implementar un micrófono cerca del asiento del conductor. Si el micrófono está dotado de un interruptor de potencia, los conductores pueden percibir que son ellos los que controlan cuando el sistema les puede "escuchar". A parte del sentimiento de torpeza que mencionaron algunos conductores durante la prueba, parece ser un método adecuado para su utilización durante la conducción. Si las instrucciones se dieran también de forma audible, podría parecer más natural para el conductor llevar a cabo la verificación de voz, dado que se acercaría a una conversación entre él y el sistema.

50 Sería interesante implementar un GUI solamente con imágenes y sonidos, junto con las instrucciones habladas desde el sistema, en vez del texto utilizado en este prototipo. Sería posible para el conductor desconectar/conectar las instrucciones de voz y los sonidos, de manera que cada individuo pudiera tener el sistema más adecuado para él.

55 ACCIONES APROPIADAS EN DIFERENTES SITUACIONES

60 ¿Qué debe ocurrir una vez que el conductor ha verificado su identidad? Hay varias posibilidades con respecto a la verificación y los eventos siguientes, y éstos se explican adicionalmente en los casos de utilización que se explican a continuación.

65 Un tema que no ha sido tomado en consideración ni discutido es: ¿qué debe ocurrir si la verificación no tiene éxito en absoluto? Considerando la verificación inicial (antes de poner en marcha el motor), hay principalmente cuatro posibilidades: el vehículo es imposible de poner en marcha; el vehículo puede ser puesto en marcha y salir de manera habitual, pero después de una cierta distancia, va disminuyendo la velocidad hasta la velocidad de caminar, sin otra posibilidad de aumentar su velocidad; el vehículo es capaz de arrancar y circular del modo

habitual, pero se envía un aviso al propietario, dejando a su albedrío el tomar las precauciones apropiadas; la verificación que ha fallado es registrada a bordo del vehículo, pero no se toman otras acciones.

5 Es siempre difícil evaluar las diferentes situaciones en comparación entre sí. Si el vehículo se desplaza aunque el conductor no es el conductor apropiado o ni siquiera un conductor autorizado, el riesgo de que el vehículo pueda ser utilizado para objetivos no deseados aumenta.

10 Por otra parte, si es imposible desplazar el vehículo sin un conductor autorizado, el riesgo de secuestro de vehículos con el conductor, aumenta. La cuestión de si la sociedad o el conductor deben tener la mayor prioridad puede cambiar dependiendo del tipo de carga que lleva en el vehículo y también de donde está situado el vehículo en el momento del fallo de la verificación.

15 ¿Qué se debe hacer si el conductor falla en la verificación de su identidad durante la conducción? Esta cuestión ha sido discutida también durante el proceso, pero para conseguir las respuestas apropiadas se deben llevar a cabo varias pruebas. Las posibilidades son muy parecidas a las anteriores con la modificación de que en los primeros dos ejemplos el vehículo se para o disminuye la velocidad a la velocidad de andar, respectivamente.

CUÁNDO DEBE TENER LUGAR LA VERIFICACIÓN

20 El momento en el que se debe solicitar la verificación, es también un tema importante. Si se deja correr libremente la imaginación, hay un número ilimitado de posibilidades y en algún lugar se tiene que trazar la línea de limitación. Los autores sugieren que el conductor debe verificar su identidad nuevamente cuando las puertas han sido abiertas y el sensor del asiento indica que alguien se ha sentado en el mismo. El sensor del asiento es el que pone en marcha la señal del cinturón de seguridad, y la mayor parte de camiones tienen sensores que comprueban si las
25 puertas están bien cerradas, de manera que ello sería fácil de implementar.

30 Si se desea verificar la identidad del conductor durante la conducción, ¿con qué frecuencia se debe realizar? En nuestras encuestas, los conductores de larga distancia nos han indicado que en algunos casos conducen durante el máximo de, horas seguidas y, en algunos casos, hacen ocho paradas en un trayecto de dos horas. El tiempo o distancia conducidos entre las paradas se debe tener en cuenta contrapesando la protección con la comodidad.

35 Se sugiere que la demanda de verificación no se debe presentar demasiado frecuentemente, dado que ello podría ser un estorbo para el conductor. Además, si el conductor se detiene a cargar/descargar, es muy probable que salga del vehículo y, por lo tanto, la verificación debe tener lugar antes de partir nuevamente.

40 Lo ideal sería si la verificación durante la conducción pudiera ser llevada a cabo sin acciones a tomar por parte del conductor, tal como en el caso de reconocimiento facial automático. Pero, también en este caso, la verificación no debe ser realizada demasiado frecuentemente debido al hecho de que si la verificación automática falla, el conductor debe ser verificado de alguna otra manera.

POSIBILIDADES ADICIONALES

45 Es posible tener, incluso, más niveles de seguridad que los realizados para este prototipo. Si el sistema de verificación tiene información sobre la carga y en qué área está operando el vehículo, el sistema puede ajustar el nivel de protección automáticamente. Por ejemplo, un transporte de oro en Cape Town requiere un nivel de protección más elevado que cuando se suministra hormigón a un lugar de construcción en el bosque de Laplander.

50 Tal como se ha sugerido en los casos de utilización, un sistema multimodal puede requerir solamente un método biométrico para la verificación. El método requerido es seleccionado al azar, de manera que el conductor necesita haber practicado todos ellos, pero utilizar solamente uno a la vez. Con este método al azar, un impostor no puede estar seguro de lo que necesita para la verificación, y tendrá muchas más dificultades en preparar una muestra falsa de todas las características distintas.

55 Otra ventaja cuando se prueban distintos métodos al azar, es que la habituación del conductor será mejor que si utiliza solamente un método todo el tiempo y, a continuación, tiene que cambiar debido a la pérdida de un dedo o algo menos drástico.

60 Esto daría también la posibilidad de actualizar un modelo en la base de datos si la verificación era un éxito total. Para mostrar un ejemplo: imaginad que el conductor recientemente ha sido verificado utilizando su tarjeta, el PIN y huellas dactilares. Si a continuación estos métodos tienen éxito, el sistema podría tomar una nueva foto de la cara para actualizar el registro. Esto puede facilitar la verificación si el conductor se está dejando crecer la barba o se ha afeitado recientemente o si el conductor ha aumentado o disminuido de peso desde el inicio.

65 Una idea que se consideró en esta etapa era la de combinar la geometría de la mano con el escaneado de las huellas dactilares. La resolución de las cámaras digitales actuales es suficientemente elevada para tomar una

imagen suficientemente detallada de la palma de la mano a efectos de analizar, tanto las medidas de los dedos como las huellas dactilares.

COLOCACIÓN DE LA BASE DE DATOS Y ADMINISTRACIÓN DEL SISTEMA

5 Dado que todos los métodos descritos requieren una base de datos para almacenar los modelos originales cerrados durante el proceso de inicio, se deben llevar a cabo estudios con respecto a la colocación de la base de datos. Esta base de datos es necesaria para la comparación durante la verificación. En el prototipo, la base de datos fue almacenada en un ordenador próximo a la cabina; en realidad, hay básicamente tres colocaciones
10 diferentes a tener en cuenta; oficina principal; en el vehículo; y tarjeta inteligente.

Cual es la mejor colocación depende de varios parámetros y se tiene que considerar caso a caso. Algo es evidente, si el sistema es utilizado para impedir que personas no autorizadas pongan en marcha el vehículo, la comunicación entre el dispositivo biométrico y la base de datos no debe fallar nunca. Esto se justifica porque, de
15 otro modo, un conductor autorizado puede quedar parado en cualquier lugar debido a problemas de comunicación entre el vehículo y la base de datos.

COLOCACIÓN EN LA OFICINA PRINCIPAL

20 La colocación en la oficina principal significa que la base de datos de modelos está situada en un ordenador, por ejemplo, en la oficina del contratista de transporte.

Un sistema de verificación puede requerir actualización en tiempo real y, por lo tanto, es necesario un enlace entre el vehículo y la base de datos. Si un conductor está enfermo y otro lleva a cabo su función, el sistema debe ser
25 actualizado para aceptar el nuevo conductor como conductor apropiado. Tal como se ha mencionado anteriormente, el gobierno de Estados Unidos desea evitar que las personas que se encuentran en las bases de datos del FBI conduzcan vehículos con mercancías peligrosas. La base de datos del FBI cambia, por lo que sería deseable la actualización en tiempo real para el sistema de verificación.

COLOCACIÓN EN EL VEHÍCULO

30 La colocación en el vehículo tiene lugar cuando los modelos son situados en un ordenador en el camión. Esto limita los problemas provocados por la comunicación inalámbrica pero, por el contrario, la protección contra robo o ataque al sistema, no sería tan considerable como en el caso de colocación en la oficina principal. Es la solución
35 más simple pero, asimismo, es probablemente la más cara dado que requiere una base de datos en cada vehículo.

COLOCACIÓN EN TARJETA INTELIGENTE

40 La colocación en la tarjeta inteligente se refiere al caso en el que los modelos son almacenados en una tarjeta inteligente que el conductor puede llevarse cuando sale del vehículo. Esto aumenta la protección dado que el conductor necesita también llevar la tarjeta inteligente para superar el sistema. Además, el hecho de que el propio conductor lleve sus propios modelos biométricos puede incrementar su sentimiento de privacidad.

45 Una ventaja en caso de que la base de datos se mantenga en una tarjeta o en la oficina principal, es que no está limitada a un vehículo determinado. Si un conductor necesita cambiar de vehículo debido a un fallo del motor, etcétera, ello no será problema alguno dado que todos los conductores pueden conducir todos los vehículos siempre que lleven su propia tarjeta inteligente y estén registrados en la base de datos. Se debe observar que la actualización dinámica de la base de datos será muy importante.

50 Desde el 5 de Agosto de 2005, todos los vehículos nuevos en toda la Unión Europea deben estar dotados de un tacógrafo digital. Los tacógrafos actuales son simples discos de papel y no es inhabitual que los datos sean manipulados. El tacógrafo digital es una tarjeta inteligente que registra automáticamente datos, tales como la velocidad y tiempo de conducción entre paradas. La tarjeta inteligente hace mucho más complicado que los conductores puedan manipular los datos registrados y, a largo plazo, el tacógrafo digital está destinado a ser
55 normal para todos los vehículos. El tacógrafo digital abre posibilidades para integración con la tarjeta inteligente biométrica que puede ser utilizada para los modelos. De esta manera, el conductor necesita solamente una tarjeta, pero tanto los parámetros del vehículo como los modelos para la verificación serán almacenados conjuntamente. Esto puede ser una forma de incrementar la seguridad adicionalmente, dado que se asegura que los datos del tacógrafo pertenecen al conductor (suponiendo que éste haya sido verificado).

60 Si el conductor pierde su tarjeta, se abre la posibilidad de que se introduzca un impostor y se apropie de los modelos de la tarjeta. No obstante, esto será difícil dado que necesitará no solamente conocer los métodos utilizados. Debe conocer también la estructura de los modelos y debe ser capaz de superar el encriptado incorporado en la tarjeta. Para almacenar algo en la tarjeta, debe tener también conocimientos del sistema operativo de la tarjeta específica. Los sistemas operativos varían notablemente de un fabricante a otro.
65

ADMINISTRACIÓN DEL SISTEMA

5 Con respecto a la discusión de la colocación de la base de datos, se pueden hacer reflexiones en la forma de administrar el sistema. Algunos contratistas de transporte tienen un gran número de vehículos y conductores y, si el sistema es difícil de administrar, pueden verse forzados a reclutar plantilla adicional solo para administrar el sistema de verificación. En este sentido, no se sigue la colocación de la base de datos en el vehículo. Ello, dado que cada conductor debe estar alistado en cada vehículo que deba conducir o que sus modelos deben ser descargados a la base de datos de estos vehículos.

10 Con la colocación de la base de datos de modelos en la oficina principal, una alternativa podría consistir en descargar los modelos temporalmente a una memoria del vehículo a efectos de llevar a cabo la correspondencia. La otra alternativa consiste en enviar los modelos escaneados durante la verificación a la oficina principal para verificar la correspondencia. No se sugiere esa forma de proceder debido al riesgo de que el vehículo entre en un área con insuficiente captación o posibilidad de que la conexión inalámbrica haya sido alterada. Aunque se diga que debería ser imposible crear nuevamente las características reales a partir del modelo, puede ser poco cómodo para el usuario conocer que los modelos biométricos se han enviado a otro lugar.

20 Si los modelos están almacenados en una tarjeta, por ejemplo, la tarjeta del tacógrafo digital, estos problemas no ocurren. Por el contrario, existe el riesgo de que el conductor pierda su tarjeta. No obstante, está prohibido conducir el vehículo sin que la tarjeta del tacógrafo esté introducida y, por lo tanto, es probable que los conductores cuiden adecuadamente sus tarjetas.

TELEMÁTICA

25 Para posibilitar que el sistema comunique con la oficina principal, se requiere telemática. La mayor parte de los camiones actuales están dotados de algún tipo de sistema de comunicación. Puede tratarse desde un sistema básico de comunicación por radio de tipo analógico hasta el sistema DynaFleet de tipo avanzado de Volvo. Dado que lo principal en estos sistemas es la propia verificación, se supone simplemente que es posible transferir datos entre el camión y la oficina.

30 Se sugiere enviar el nombre, ID de empleo e información del resultado de las diferentes verificaciones a la oficina principal. El riesgo de que la conexión haya sido manipulada sugiere que ni los modelos ni una información excesiva con respecto al conductor (por ejemplo, el número de la Seguridad Social) deban ser enviados.

35 Otra recomendación, debido al riesgo de que la conexión haya sido manipulada, consiste en enviar la información en forma encriptada para reducir el riesgo de que la información pueda pasar a manos no adecuadas. Hay numerosos productos en el mercado para el encriptado de datos. La mayor parte de sistemas procesan los datos de acuerdo con una clave de encriptado. Los datos son enviados a continuación al receptor, que tiene una clave de encriptado idéntica para decodificar la información.

DISTRIBUCIÓN DE LA INFORMACIÓN

45 ¿Dónde se deben enviar los datos y a quién se deben enviar? El propietario del camión posee la información, pero hay otros entes que podrían desear poseer una parte de la misma. Estos entes pueden ser, por ejemplo, las compañías de seguros, la asociación nacional de carreteras, la policía y los servicios de incendios y de rescate. Se debe tomar en consideración quién debe tener la responsabilidad de actualizar, almacenar, y distribuir la información.

ASPECTOS IMPORTANTES DE LA AUTOMOCIÓN

50 Hay una serie de escenarios que pueden crear complicaciones, que puede tener lugar a la perspectiva de la automoción, por ejemplo:

- 55 • Si el vehículo es utilizado para alquiler, debe ser fácil introducir y quitar personas del sistema. Una ventaja puede ser que la empresa de alquiler pueda asegurar que el vehículo es conducido solamente por la persona que lo ha contratado en la oficina comercial.
- 60 • Si el vehículo es prestado a alguien, se requiere un proceso fácil de traspaso o de alistamiento/eliminación.
- 65 • Si el vehículo necesita los servicios de un taller, debe haber una forma simple de superar el sistema en vez de alistar al mecánico en el taller. Una posible solución puede ser permitir que el camión se desplace, por ejemplo, a una velocidad de 5km/hora sin la tarjeta del tacógrafo o cualquier otra verificación.

- Si el conductor sufre daños o se encuentra, por cualquier otra razón, incapaz de conducir el vehículo, debe haber una manera de desplazarlo en caso de emergencia. La solución puede ser la sugerida en el párrafo anterior.
- Si el vehículo es vendido a alguien que no tiene necesidad de un sistema de verificación, debe ser posible eliminarlo.
- La manipulación del vehículo durante la fabricación o transporte es también un problema a tomar en consideración. Esto puede ser solucionado de manera similar a la del servicio en taller.

Estos aspectos deben ser considerados a fondo antes de que el sistema se introduzca en el mercado. También, en el caso de que el sistema biométrico deba sustituir la llave de encendido para poner en marcha el motor, la forma de manipular el suministro eléctrico, arrancar el motor y controlar el bloqueo de dirección, deben ser tenidos en cuenta.

CRÍTICA DEL MÉTODO

En la primera encuesta de conductores, los documentos fueron distribuidos en una parada del camión. Se pidió a los conductores si podrían contestar a algunas preguntas con respecto a su trabajo y las posibilidades de un sistema de verificación del conductor. Existe el riesgo de que solamente los que son fuertemente contrarios al mismo o muy positivos desearan contestar, mientras que el resto no se preocupó lo suficiente para perder el tiempo en contestar las preguntas.

Lo mismo es cierto para los documentos que fueron distribuidos en un contratista de transportes en Gothenburg. Solamente la mitad de los documentos distribuidos fueron devueltos, lo que lleva a las preguntas: ¿Quién decidió contestar/no contestar, y por qué?. Estos documentos se dejaron con instrucciones a un empleado en la oficina. Si aparecían preguntas, los conductores no tenían a nadie a quién preguntar para conseguir información/explicaciones.

La selección de los métodos y el equipo estuvieron limitados por falta de tiempo y también de fondos, por lo que es incierto si el equipo utilizado es el mejor de los sistemas disponibles. Además, el software se implementó por un programador relativamente inexperto, y esto puede haber afectado el rendimiento del sistema.

Tal como se ha indicado anteriormente, el simulador no era perfectamente adecuado para el escenario escogido y, debido a la falta de tiempo, no era posible hacer ajuste alguno. Algunos de los participantes tenían comentarios que hacer con respecto a su comportamiento. Esto puede haber afectado a sus opiniones con respecto al sistema de verificación. El resultado de las pruebas habría sido, probablemente, más correcto si el simulador hubiera sido más auténtico.

El escenario fue bastante intenso, con seis verificaciones en unos 30 minutos. Habría sido mejor una prueba más larga, pero esto no era posible debido a las limitaciones de tiempo.

Es posible que los conductores que decidieron participar en la prueba estén particularmente interesados en nuevas tecnologías y, por lo tanto, que sean más positivos que el promedio de los conductores de camión.

Es posible que no todos los participantes consiguieran exactamente la misma información durante la fase de alistamiento y esto puede haber afectado su comportamiento.

Durante el alistamiento, se pidió a los participantes que bajaran el volante para tener una visión clara por la cámara de reconocimiento facial. Durante la prueba, algunos de ellos levantaron el volante nuevamente durante la conducción. No fue posible suspender la prueba en aquel momento. Esto podría haber afectado al comportamiento del sistema de verificación facial.

Muchas palabras y abreviaturas utilizadas en esta invención pueden ser desconocidas para el lector y, por lo tanto, las indicamos en su acepción más habitual.

Antropometría	Estudio de medición del cuerpo humano para utilización (antropológica) en la clasificación y comparación.
Automoción	Término genérico de la tecnología relacionada con la industria de vehículos.
Biométrica	Término general para los métodos que utilizan análisis de las características corporales exclusivas de un sujeto.
Dieléctrico	Dieléctricos son materiales aislantes con diferentes propiedades.

	ECG	Abreviatura de Electrocardiograma. Medición de señales eléctricas del corazón.
5	FAR	Abreviatura de Tasa de Autenticación Falsa (False Authentication Rate). Indica la frecuencia en la que el sistema interpreta un impostor como usuario autorizado. FAR y FRR (ver más adelante) están muy correlacionados; un FAR elevado implica un FRR bajo, y viceversa,
10	Forense	Término genérico utilizado para elementos asociados con investigaciones de delitos y de la justicia.
15	FRR	Abreviatura de Tasa de Rechazo Falso (False Rejection Rate). Indica la frecuencia en la que el sistema rechaza un usuario autorizado. FRR y FAR (ver anterior) están muy correlacionados; un FRR elevado implica un FAR bajo, y viceversa.
	IR	Abreviatura de Infrarrojos. Luz con longitud de onda más larga que la luz roja visible, por lo tanto, es invisible para el ojo humano.
20	Indicios (“Minutiae”)	Características especiales de una huella dactilar, por ejemplo, el lugar en el que las crestas terminan o se dividen en dos.
	Imitación (“Mock-up”)	Partes, típicamente del entorno del conductor, de un vehículo dispuesto en un laboratorio para objetivos de simulación y pruebas.
25	NIR	Abreviatura de Próximo a Infrarrojos (“Near Infrared”)
	Oximetría	La oximetría del pulso es un método simple no invasivo de controlar el porcentaje de hemoglobina (Hb) saturada con oxígeno.
30	Permisividad	Medición de la magnitud en la que un medio cambia para absorber energía cuando es sometido a un campo eléctrico.
35	PIN	Abreviatura de Número de Identificación Personal (“Personal Identification Number”).
	Cresta	Líneas salientes de una huella dactilar.
40	Tarjeta inteligente	Un minúsculo criptoprocador de seguridad incorporado dentro de una tarjeta del tamaño de una tarjeta de crédito o menor. Un ejemplo son las tarjetas SIM para teléfonos móviles GSM.
	TER	Abreviatura de Tasa Total de Error (“Total Error Rate”), suma de FAR y FRR.
45	Termografía	Medición de diferencias de calor utilizando una cámara IR.
	Valle	Las partes más bajas entre las crestas de una huella dactilar.

TABLAS DE ANÁLISIS SWOT

- 50 Figura 20 - Huellas dactilares como método de verificación
- Figura 21 - Escaneado del iris como método de verificación
- Figura 22 - Verificación de voz como método de verificación
- Figura 23 - Reconocimiento facial como método de verificación
- Figura 24 - Termografía facial como método de verificación
- 55 Figura 25 - Escaneado de retina como método de verificación
- Figura 26 - Movimiento de labios como método de verificación
- Figura 27 - Reconocimiento de geometría de la mano como método de verificación
- Figura 28 - Escaneado de contraseñas y PIN como método de verificación
- Figura 29 - Tarjetas como método de verificación
- 60 Figura 30 - RFID como método de verificación
- Figura 31 - Estadísticas de la escala de aceptación van der Laans

VERIFICACIÓN MULTIMODAL UTILIZANDO TODOS LOS MÉTODOS BIOMÉTRICOS

- 65 **Caso de uso:** Verificación multimodal al nivel de protección más elevado (todos los métodos biométricos)

Referencia:

- 5 **Objetivo:** La verificación se lleva a cabo para asegurar que el conductor es el conductor apropiado. El conductor utiliza todos los métodos biométricos disponibles para la verificación porque el vehículo está clasificado al nivel de protección más elevado.
- 10 **Entes:** Sistema de verificación, conductor, oficina principal.
- 10 **Precondiciones:** El vehículo está bloqueado o recientemente desbloqueado.

TRANSCURSO PRINCIPAL DE EVENTOS

15 El conductor entra en el vehículo y acciona la llave de encendido, después de lo cual el sistema requiere la verificación utilizando varios métodos para asegurar que él es el conductor apropiado. El conductor empieza por su propia verificación con uno de los métodos y, a continuación, sigue con el siguiente, y el siguiente, hasta que se ha terminado la verificación. Cuando el conductor es verificado, la información es enviada, encriptada, a la oficina principal y el conductor puede salir con el vehículo.

20 **TRASNCURSO DE EVENTOS ALTERNATIVO**

25 El conductor entra en el vehículo y acciona la llave de encendido, después de lo cual el sistema requiere la verificación utilizando varios métodos para asegurar que él es el conductor apropiado. El conductor no tiene éxito con uno o varios de los métodos de verificación. Después de tres fallos con un método, la verificación continúa con los otros métodos (o termina sin el último si éste es el que falla). Como mínimo, uno de los métodos tiene éxito y la información se envía, encriptada, a la oficina principal y el conductor puede marcharse con el vehículo. Junto con la información verificada sobre el conductor, la oficina principal recibe también información con respecto a la verificación que ha fallado.

30 **TRANSCURSO DE EVENTOS ALTERNATIVO**

35 El conductor entra en el vehículo y acciona la llave de encendido, después de lo cual el sistema requiere la verificación utilizando varios métodos para asegurar que él es el conductor apropiado. El conductor no tiene éxito con el primer método de verificación, después de tres fallos, el sistema continúa con el método siguiente. Ninguno de los métodos tiene éxito, con lo que se envía inmediatamente un aviso a la oficina central.

REQUERIMIENTO ESPECIAL

40 El sistema debería recibir información cuando una persona desbloquee las puertas. El sistema requiere medios telemáticos para poder enviar la información entre el vehículo y la oficina central.

Ejemplo 1

45 El conductor ha llegado a la base para empezar el día de trabajo. Al entrar en el vehículo inserta su tarjeta inteligente (integrada en la tarjeta para el tacógrafo) en el dispositivo lector, marca su código PIN y, a continuación, pone un dedo en el escáner. El PIN es correcto y la huella dactilar es verificada con respecto a la tarjeta, de manera que el sistema pide una muestra de la voz. El conductor dice su contraseña frente al micrófono. Aparece un mensaje del sistema indicando al conductor que se siente en posición normal de conducción para llevar a cabo la verificación facial. Los datos registrados son analizados y comparados con los datos del modelo, almacenados en la tarjeta inteligente - la verificación ha sido satisfactoria. Se envían el nombre y el número de identificación de empleo a la oficina principal.

55 **Ejemplo 2**

60 El conductor ha llegado a la base para empezar el día de trabajo. Al entrar en el vehículo inserta su tarjeta inteligente (integrada en la tarjeta del tacógrafo) en el dispositivo lector, marca su código PIN y pone el dedo en el escáner. Intenta verificar su identidad mediante su voz, pero falla dado que este día tiene un resfriado. Una señal informa al conductor de que ha fallado la verificación. El proceso continúa con la verificación facial, con éxito. El nombre y número de identificación de empleo son enviados, encriptados, a la oficina principal, junto con información sobre la verificación de voz que ha fallado.

Ejemplo 3

65 En un viaje de largo recorrido, el conductor hace una siesta en la cabina. Al despertar, sale para estirar las piernas antes de continuar el viaje. La puerta del pasajero se abre y un impostor sube y se sienta en el asiento del

conductor. El impostor intenta poner en marcha el vehículo pero no tiene éxito con la verificación, por lo que el vehículo queda inmovilizado. Se envía inmediatamente un aviso a la oficina central, y el sistema toma una imagen de la persona que se encuentra detrás del volante. Esta imagen es enviada también a la oficina principal.

5 **VERIFICACIÓN MULTIMODAL UTILIZANDO DOS MÉTODOS BIOMÉTRICOS**

Caso de uso: Verificación multimodal con un nivel de protección medio (dos características biométricas).

10 **Referencia:**

Objetivo: Se lleva a cabo la verificación para asegurar que el conductor es el conductor apropiado. Para adaptarse a la clasificación del vehículo, nivel de seguridad medio, el conductor verifica su identidad utilizando dos características biométricas.

Participantes: Sistema de verificación, conductor, oficina principal.

Condiciones previas: El vehículo está bloqueado, o recientemente desbloqueado.

20 **TRANSCURSO PRINCIPAL DE EVENTOS**

25 El conductor entra en el vehículo y acciona la llave de contacto, después de lo cual el sistema requiere la verificación utilizando varios métodos para asegurar que él es el conductor apropiado. El conductor empieza por su propia verificación con uno de los métodos y, a continuación, continúa con la siguiente, y la siguiente, hasta que la verificación se ha terminado. Cuando el conductor ha sido verificado, la información es enviada, encriptada, a la oficina principal y el conductor puede salir con el vehículo.

30 **TRANSCURSO DE EVENTOS ALTERNATIVO**

35 El conductor entra en el vehículo y acciona la llave de contacto, después de lo cual el sistema requiere la verificación utilizando varios métodos para asegurar que él es el conductor apropiado. El conductor no tiene éxito con uno o varios de los métodos de verificación. Después de tres fallos con un método, la verificación continúa con los otros métodos (o termina con el último si es que falla). Por lo menos, uno de los métodos tiene éxito y la información es enviada, encriptada, a la oficina principal y el conductor puede salir con el vehículo. Junto con la información verificada sobre el conductor, la oficina principal recibe también información con respecto a la verificación que ha fallado.

40 **TRANSCURSO DE EVENTOS ALTERNATIVO**

45 El conductor entra en el vehículo y acciona la llave de contacto, después de lo cual el sistema requiere la verificación utilizando varios métodos para asegurar que él es el conductor apropiado. El conductor no tiene éxito con el primer método de verificación, después de tres fallos, el sistema continúa con el método siguiente. Ninguno de los métodos tiene éxito, con lo que se envía inmediatamente un aviso a la oficina central.

REQUERIMIENTO ESPECIAL

50 El sistema debería recibir información cuando una persona desbloquee las puertas. El sistema requiere medios telemáticos para poder enviar la información entre el vehículo y la oficina central.

Ejemplo 1

55 El conductor ha llegado a la base para empezar el día de trabajo. Al entrar en el vehículo inserta su tarjeta inteligente (integrada en la tarjeta para el tacógrafo) en el dispositivo lector, marca su código PIN y, a continuación, coloca el dedo en el escáner. El PIN es correcto y el dedo es verificado con respecto a la tarjeta. El sistema requiere una muestra de voz, de manera que el conductor indica su contraseña delante del micrófono. Los datos registrados son analizados y comparados con los datos modelo, almacenados en la tarjeta inteligente - la verificación fue satisfactoria. El nombre y el número de identificación de empleo son enviados, encriptados, a la oficina principal.

60 Ejemplo 2

65 El conductor ha llegado a la base para empezar el día de trabajo. Al entrar en el vehículo, inserta su tarjeta inteligente (integrada en la tarjeta para el tacógrafo) en el dispositivo lector, marca su código PIN y, a continuación, coloca el dedo sobre el escáner. El PIN es correcto y el dedo es verificado con respecto a la tarjeta. Aparece un mensaje del sistema indicando al conductor que se siente en posición normal de conducción a efectos de llevar a

cabo la verificación facial. Los datos registrados son analizados y comparados con los datos modelo almacenados en la tarjeta inteligente – la verificación tuvo éxito. El nombre y el número de identificación de empleado se envían, encriptados, a la oficina principal.

5 **Ejemplo 3**

El conductor ha llegado a la base para empezar el día de trabajo. Al entrar en el vehículo, inserta su tarjeta inteligente (integrada en la tarjeta para el tacógrafo) en el dispositivo lector, marca su código PIN y, a continuación, coloca el dedo sobre el escáner. Intenta verificar su identidad por su voz, pero falla dado que este día está resfriado.

10 El nombre y número de identificación de empleado son enviados, encriptados, a la oficina principal, junto con información sobre el fallo de la verificación de voz.

Ejemplo 4

15 El conductor ha llegado a la base para empezar el día de trabajo. Al entrar en el vehículo, inserta su tarjeta inteligente (integrada en la tarjeta para el tacógrafo) en el dispositivo lector, marca su código PIN y, a continuación, coloca el dedo sobre el escáner. Se toma una imagen de la cara del conductor, pero se ha dejado crecer la barba durante sus vacaciones, por lo que la verificación falla. Se envían el nombre y número de identificación de empleo, encriptados, a la oficina principal, junto con información sobre la verificación facial que ha fallado.

20 A continuación, se describen implementaciones a título de ejemplo de la invención o invenciones que se dan a conocer en la actualidad. Estas características, para la que se pide la protección de patente, se indican en las reivindicaciones siguientes.

REIVINDICACIONES

1. Método para asegurar que el conductor de un vehículo es un conductor autorizado, cuyo método comprende:

5 utilizar un sistema de verificación multimodal del conductor, a bordo del vehículo, para asegurar si el conductor es un conductor autorizado;

llevar a cabo un primer proceso de verificación del conductor en el operador presente del vehículo y determinar si el operador presente es un conductor autorizado o no autorizado del vehículo.

10 llevar a cabo un segundo proceso de verificación del conductor del operador presente del vehículo y determinar si el operador presente es un conductor autorizado o no autorizado del vehículo, de manera que dichos primer y segundo procedimientos de verificación del conductor son llevados a cabo con un intervalo de tiempo entre ellos, dependiendo dicho intervalo de tiempo de la naturaleza del trabajo llevado a cabo por el conductor;

15 llevar a cabo una medida correctiva para evitar un impacto potencialmente negativo cuando el operador presente del vehículo se ha determinado que es un conductor no autorizado, basándose en, como mínimo, uno de los procedimientos de verificación llevados a cabo; y en el que, como mínimo, uno de los procedimientos de verificación comprende la utilización de datos biométricos que pueden cambiar a lo largo del tiempo para una persona determinada, permitiendo potencialmente un fallo de verificación de dicha persona basado en la comparación de las mediciones biométricas actuales con respecto a un modelo conseguido previamente de las mismas características, y actualizando automáticamente el modelo previamente conseguido.

20 en el que se utilizan uno o más procedimientos de verificación para verificar el conductor, mientras que uno de los procedimientos de verificación no es utilizado para la verificación, sino que, alternativamente, actualiza su modelo previamente conseguido si el proceso de verificación ha tenido éxito, o

25 en el que un modelo previamente conseguido es actualizado si el proceso de verificación ha tenido un completo éxito, ya que han tenido éxito todos los procedimientos de verificación utilizados para la verificación del conductor.

30 2. Método, según la reivindicación 1, en el que dicha actualización automática es conseguida en un sistema de verificación multimodal, en el que el sistema de verificación utiliza más de uno de: técnicas biométricas/código PIN/tarjeta inteligente y el segundo proceso de configuración del conductor es distinto de dicho primer procedimiento de verificación del conductor.

35 3. Método, según la reivindicación 1, en el que, como mínimo, un procedimiento de verificación utiliza datos biométricos de reconocimiento facial actualizados que han cambiado a lo largo del tiempo.

40 4. Método, según la reivindicación 1, en el que al entrar el conductor en el vehículo, se genera una petición requiriendo la verificación de identidad utilizando un código PIN, las huellas dactilares y el reconocimiento facial, y después de lo cual el sistema verifica la identidad del conductor utilizando el código PIN y el reconocimiento facial, y utiliza los datos biométricos de las huellas dactilares para actualizar el modelo de huellas dactilares en la base de datos.

45 5. Método, según la reivindicación 1, en el que se llevan a cabo múltiples procedimientos de verificación del conductor durante un solo turno de conducción del conductor, extendiéndose dicho turno de conducción único desde el momento en el que el conductor entra en el vehículo por primera vez cuando llega al trabajo, hasta que el conductor deja finalmente el vehículo cuando sale del trabajo.

50 6. Método, según la reivindicación 1, en el que dicho segundo procedimiento de verificación del conductor es llevado a cabo solamente cuando el conductor del vehículo no se ha determinado que sea un conductor autorizado, basándose en la realización del primer procedimiento de verificación del conductor.

55 7. Método, según la reivindicación 1, en el que, como mínimo, uno de dichos primer y segundo procedimientos de verificación del conductor es una prueba de verificación pasiva que no requiere interacción consciente por parte del conductor, en asociación con la realización del, como mínimo, uno de dichos procedimientos de verificación del conductor.

60 8. Método, según la reivindicación 7, en el que dicha prueba de verificación pasiva comprende la exploración de una característica física del operador, de la que se compara una imagen con un conjunto de imágenes de control representativas de los conductores autorizados del vehículo.

65 9. Método, según la reivindicación 8, en el que dicha característica física escaneada del conductor es el iris de, como mínimo, uno de los ojos del conductor.

10. Método, según la reivindicación 8, en el que dicha característica física escaneada del conductor es la retina de, como mínimo, uno de los ojos del conductor.
- 5 11. Método, según la reivindicación 8, en el que dicha característica física escaneada es un termograma facial del conductor.
12. Método, según la reivindicación 8, en el que dicha prueba de verificación pasiva tiene una tasa de fallo debido a, como mínimo, una situación ambiental que impide la obtención del escaneado adecuado de la característica física del conductor.
- 10 13. Método, según la reivindicación 12, en el que, como mínimo, una situación ambiental es de iluminación insuficiente.
- 15 14. Método, según la reivindicación 1, en el que, al menos, uno de dichos primer y segundo procedimientos de verificación del conductor es una prueba de verificación activa que requiere interacción conciente por parte del conductor, en asociación con la realización de, como mínimo, uno de dichos procedimientos de verificación del conductor.
- 20 15. Método, según la reivindicación 14, en el que dicha prueba de verificación activa comprende un escaneado de una característica física del conductor, del que se compara una imagen con un conjunto de imágenes de control representativas de los conductores autorizados del vehículo, requiriendo dicho escaneado, que el operador coloque una parte del cuerpo sobre un escáner.
- 25 16. Método, según la reivindicación 15, en el que dicha característica física escaneada del conductor es la forma de la marca de, como mínimo, uno de los dedos del conductor.
- 30 17. Método, según la reivindicación 15, en el que dicha característica física escaneada es la geometría de la mano del conductor.
- 35 18. Método, según la reivindicación 14, en el que dicha prueba de verificación activa comprende la emisión de una petición al conductor de que introduzca un número de identificación personal en el sistema, identificando al conductor como conductor autorizado.
- 40 19. Método, según la reivindicación 14, en el que dicha prueba de verificación activa comprende la lectura de la información de verificación codificada en una tarjeta de verificación presentada por el conductor, y requiriendo que el conductor introduzca un número de identificación personal en el sistema que corresponde a un número desde verificación codificado leído de la tarjeta de verificación.
- 45 20. Método, según la reivindicación 14, en el que dicha prueba de verificación activa comprende la emisión de una instrucción al conductor que emita una frase predeterminada y registrar dicha frase hablada como modelo de voz y comparar dicho modelo con un conjunto de modelos de voz de control de los conductores autorizados del vehículo.
- 50 21. Método, según la reivindicación 1, en el que dicho segundo proceso de verificación del conductor es el mismo que dicho primer procedimiento de verificación del conductor.
- 55 22. Método, según la reivindicación 1, que comprende, además, el inicio de dicha segunda verificación del conductor siguiendo inmediatamente la determinación de que el presente conductor es un conductor no autorizado en dicho primer proceso de verificación del conductor.
23. Método, según cualquiera de las reivindicaciones 1 a 22, en el que el sistema o sistemas de verificación, el procedimiento o procedimientos de verificación, la prueba o pruebas de verificación, el número o números de verificaciones, la tarjeta o tarjetas de verificación, el fallo o fallos de verificación, o información de verificación, son sustituidos por un correspondiente sistema o sistemas de identificación, procedimiento o procedimientos de identificación, prueba o pruebas de identificación, número o números de identificación, tarjeta o tarjetas de identificación, fallo o fallos de identificación, o información de identificación, según sea el caso, o por cualquier combinación de sistemas de verificación y de identificación, procedimiento o procedimientos, prueba o pruebas, número o números, tarjeta o tarjetas, fallo o fallos, o información, según sea el caso.



Figura 1



Figura 2

	Cresta	Definido por tener una distancia doble desde el inicio al final, dado que las crestas adyacentes son anchas
	Cresta	
	Extremos divergentes	Dos crestas con diferentes direcciones discurren paralelamente entre si en más de 3 mm
	Bifurcación	Una cresta se divide, ambas crestas mantienen la misma dirección y tienen una longitud superior a 3 mm
	Bifurcación	
	Gancho	Una cresta se divide, una cresta tiene una longitud no superior a 3 mm
	Gancho	
	Horquilla	Dos crestas están conectadas por una tercera cresta con una longitud no superior a 3 mm
	Horquilla	
	Punto	La sección de crestas no es más larga que la anchura de las crestas adyacentes
	Punto	
	Ojo	La cresta se divide y se vuelve a unir dentro de 3 mm
	Ojo / Isla	
	Isla	Una cresta se divide y se reune nuevamente dentro de no menos de 3 mm y no más de 6 mm. El área encerrada no tiene crestas
	Ojo / Isla	
	Cresta cerrada	Una cresta no superior a 6 mm entre otras dos crestas
	Cresta cerrada	
	Bucle cerrado	Bucle que no determina modelo entre dos o más crestas paralelas
	Bucle cerrado	
	Especialidad	Formas raras de las crestas tales como marcas de interrogante y ganchos de carnicero
	Especialidad	

Figura 3

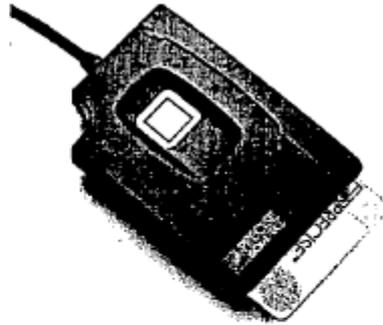


Figura 4

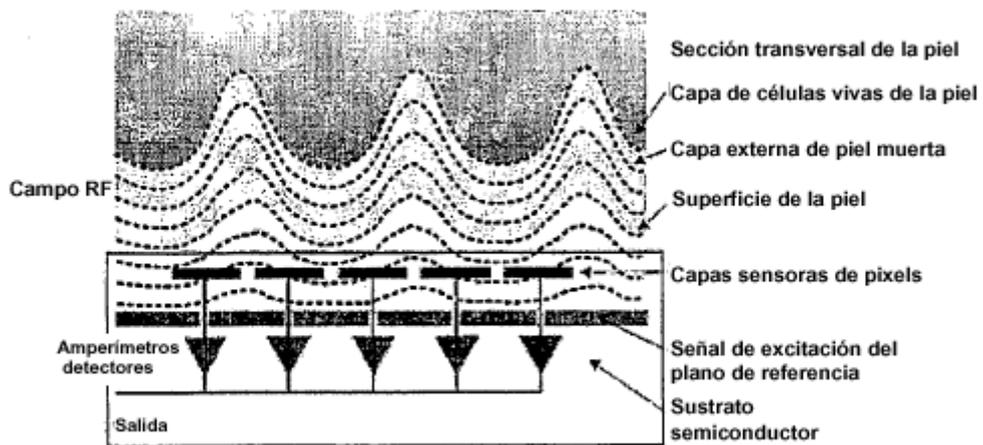


Figura 5

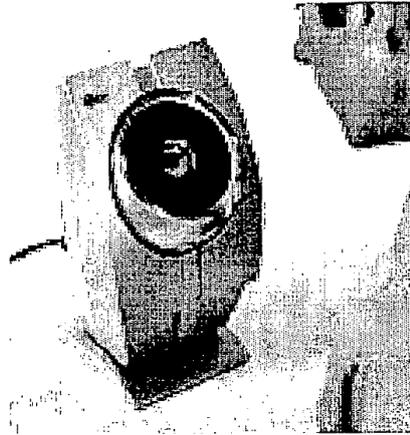


Figura 6

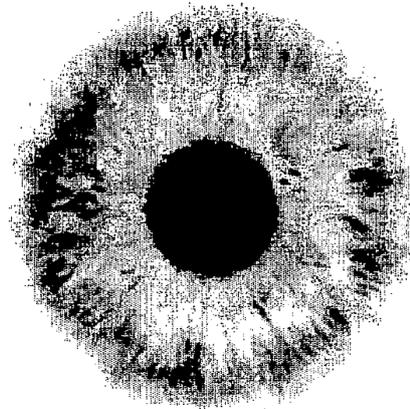


Figura 7

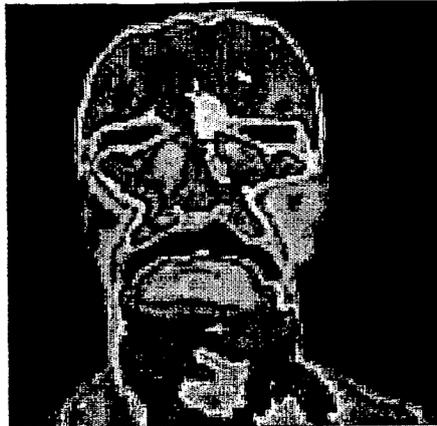


Figura 8

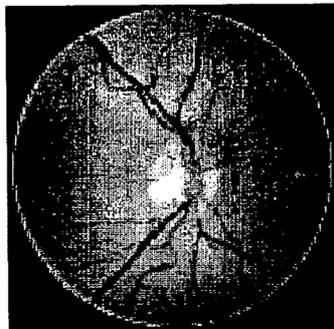


Figura 9



Figura 10

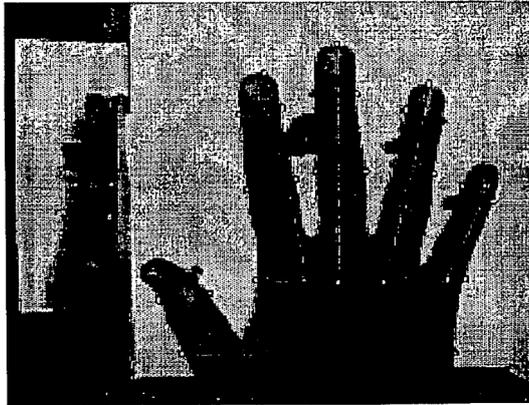


Figura 11

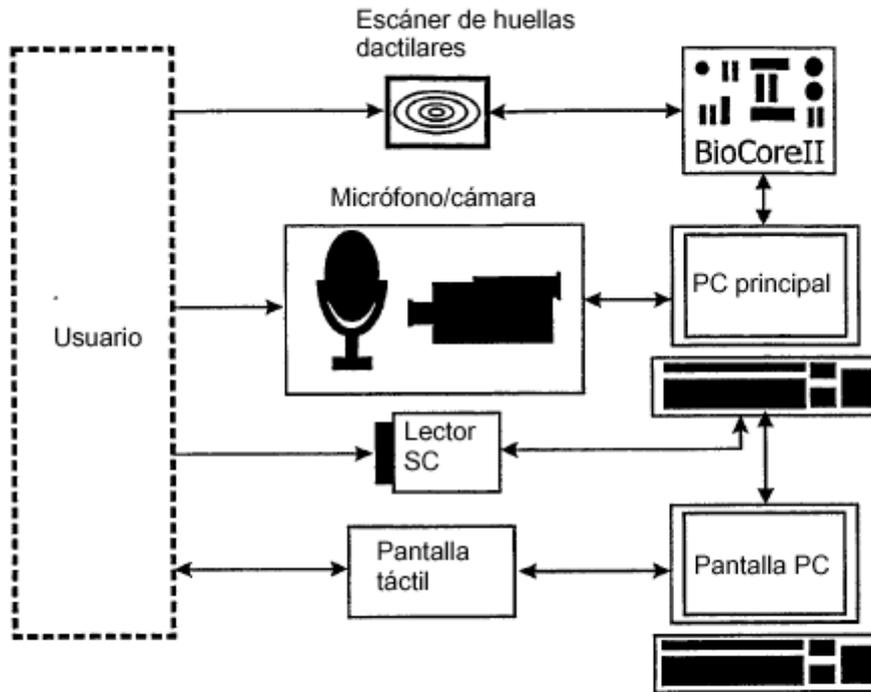


Figura 12

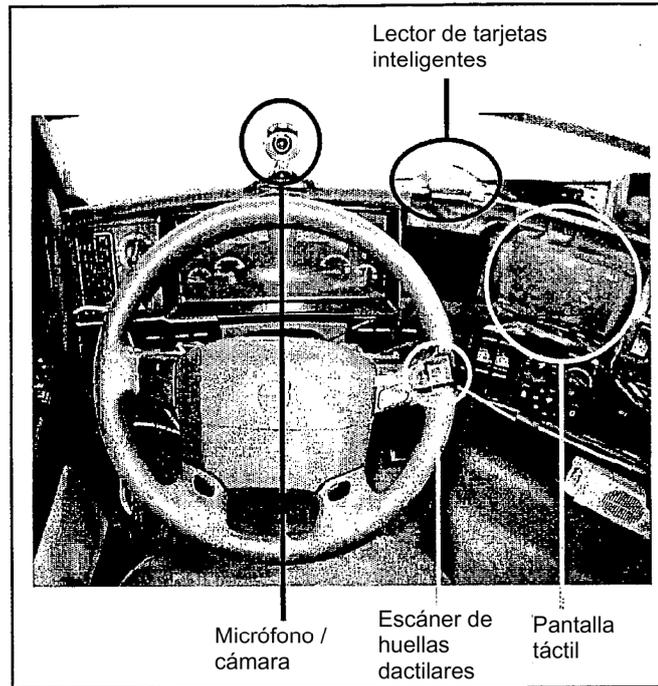


Figura 13

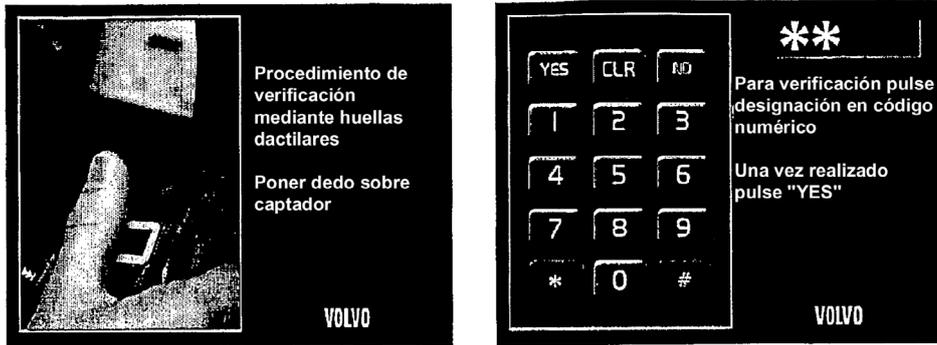


Figura 14

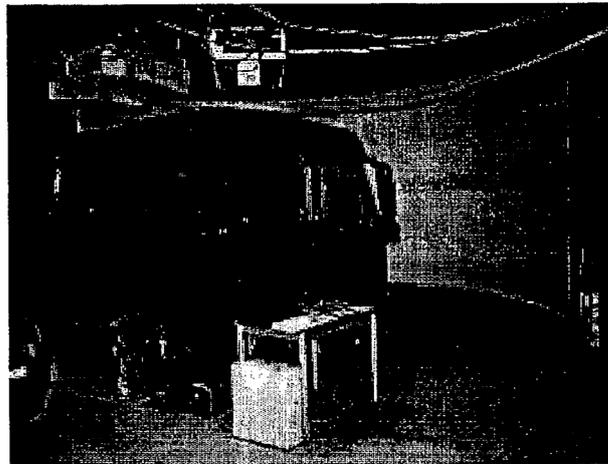


Figura 15



Figura 16

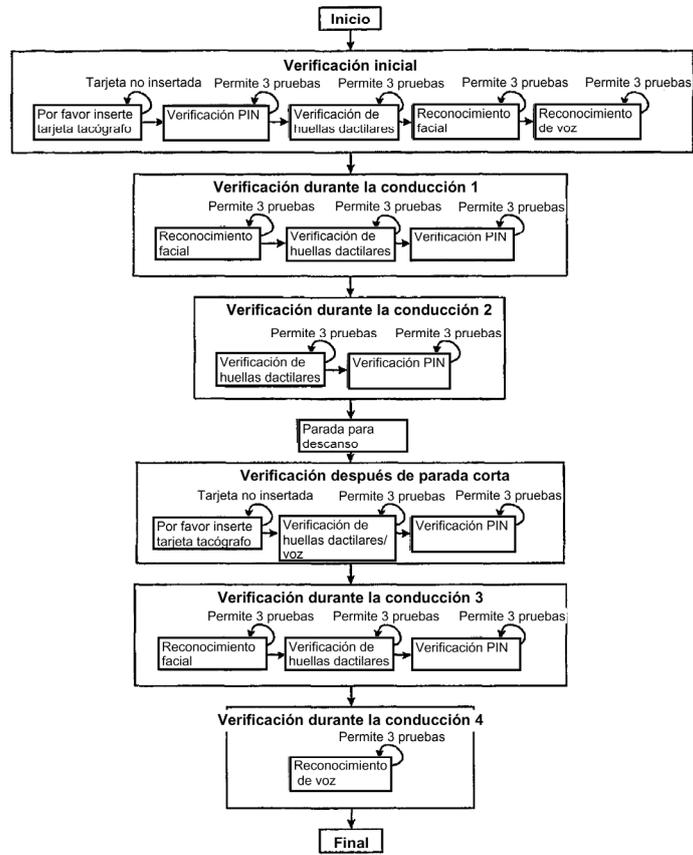


Figura 17

Fortalezas	Debilidades	Oportunidades	Amenazas
Económico	No todo el mundo puede utilizar este método	Puede ser utilizado durante la conducción	El sensor se avería por suciedad, etc.
Bien comprobado	Puede ser burlado por la suciedad	Equipo pequeño, puede ser fácilmente integrado en el entorno del conductor	Algunos pueden rechazar su utilización, dado que el método se asocia con la identificación de delincuentes
Fácil de utilizar	Puede tener problemas con suciedad o daños en las manos	Con más de un modelo en la memoria, el sistema puede indicar al azar qué dedo se debe escanear para la identificación	Si el conductor se encuentra en un lugar apartado y sus huellas dactilares se han destruido, por ejemplo, por quemaduras en las manos
Rápido		Se dispone de varios modelos, dado que diferentes empresas fabrican el equipo	

Figura 20

Fortalezas	Debilidades	Oportunidades	Amenazas
Muy exacto	Caro	Se podría integrar con el espejo retrovisor	Los usuarios pueden rechazar el análisis de los ojos si creen que es peligroso
Rápido	Una empresa, Iridian, tiene todas las patentes. Todos los otros fabricantes deben adquirir licencias de ella	Puede ser posible su utilización durante la conducción	El fabricante deja de fabricarlo por alguna razón
El iris no cambia a lo largo del tiempo			Puede ser imposible de utilizar en un vehículo debido a las condiciones de iluminación
Difícil de burlar			

Figura 21

Fortalezas	Debilidades	Oportunidades	Amenazas
Rápido, a lo largo de la verificación. (Y si no pide que se diga una frase larga.)	Cambios de voz a lo largo del tiempo	Se puede integrar en un teléfono móvil u otros equipos controlados por voz	La voz de los conductores cambia debido a condiciones de salud y condiciones emocionales
Económico	Algunos usuarios no confían en esta tecnología	El sistema puede escoger al azar la frase deseada	Pueden haber problemas con un ambiente ruidoso dentro de la cabina
Fácil de utilizar		El conductor puede tener una única contraseña, haciendo innecesaria la solicitud de otro método de verificación	
No intrusivo		Se puede utilizar durante la conducción	
La frase hablada se puede cambiar en caso, por ejemplo, de robo			

Figura 22

Fortalezas	Debilidades	Oportunidades	Amenazas
No intrusivo	Pueden haber problemas con la barba, gafas, cosmética, etc.	La cámara puede estar integrada en el espejo retrovisor	Las condiciones de iluminación en la cabina pueden hacer imposible tomar una imagen satisfactoria
Económico	La cara de las personas cambia a lo largo del tiempo	Puede ser posible utilizarlo durante la conducción	La cara del conductor se hincha o presenta daños por alguna razón
Fácil de utilizar			

Figura 23

Fortalezas	Debilidades	Oportunidades	Amenazas
Rápido	Caro	La cámara puede ser integrada en el espejo retrovisor	Nuevo método, no está clara la magnitud de la investigación y desarrollo que se realizará
Independiente de las condiciones de luz	Nuevo y, por lo tanto, no comprobado	Puede ser utilizado durante la conducción	
Difícil de burlar			
No intrusivo			

Figura 24

Fortalezas	Debilidades	Oportunidades	Amenazas
Muy exacto	No puede ser utilizado durante la conducción	Utiliza láser, lo que significa que es independiente de las condiciones de iluminación de la cabina	Los usuarios pueden rechazar utilizar este método dado que pueden desconfiar de la radiación láser
Difícil de burlar	Necesita una alineación casi perfecta de los ojos		
El modelo de vasos de la retina cambia poco a lo largo del tiempo	Caro		
Rápido			

Figura 25

Fortalezas	Debilidades	Oportunidades	Amenazas
No intrusivo	Debe ser utilizado conjuntamente con otros medios de verificación	Puede ser utilizado durante la conducción	No hay certidumbre de la magnitud de la investigación y desarrollo del método que se realizará
Rápido	Comprobado solamente dentro de un cierto contexto	La cámara puede ser integrada en el retrovisor	Los conductores se han hecho daño en el area alrededor de la boca por una razón u otra
Fácil de utilizar	No se sabe cuántas empresas, en caso de que existan, fabrican este equipo	Puede ser utilizado conjuntamente, por ejemplo, con verificación facial o de voz	

Figura 26

Fortalezas	Debilidades	Oportunidades	Amenazas
Rápido	Equipo voluminoso	Se puede utilizar durante la conducción	Solamente un fabricante del equipo
Funciona con manos (razonablemente) sucias	Las manos no son únicas, se necesitan otros medios de verificación		
No intrusivo			
Fácil de utilizar			
Económico			

Figura 27

Fortalezas	Debilidades	Oportunidades	Amenazas
Rápido	Si alguien encuentra la contraseña o el PIN, no habrá impedimento para que lo pueda utilizar	La mayor parte de los equipos necesarios se encuentran ya en los vehículos en la actualidad	Se pueden olvidar la contraseña o el PIN
Fácil de utilizar, siempre que tenga buena memoria	Funciona mejor cuando se utiliza conjuntamente con otros métodos	No es difícil de utilizar durante la conducción	La contraseña o el PIN se pueden dar a conocer y pueden ser utilizados por otros
No tiene costes importantes para integrar/utilizar el método			

Figura 28

Fortalezas	Debilidades	Oportunidades	Amenazas
Fácil de utilizar dado que es un método bien conocido que muchas personas han utilizado antes	La tarjeta se puede desgastar o puede ser robada	Todo el equipo necesario se encuentra ya en los vehículos, en la actualidad	La tarjeta es fácil de perder o de olvidar en casa
Rápido	Se puede utilizar una tarjeta por varias personas distintas	La protección se puede incrementar al añadir datos biométricos a la tarjeta, haciendo difícil utilizar la tarjeta de otra persona	La tarjeta puede ser robada
No intrusivo	Funciona mejor cuando se utiliza conjuntamente con otros métodos		Más fácil de burlar que, por ejemplo, otros métodos biométricos
Económico			

Figura 29

Fortalezas	Debilidades	Oportunidades	Amenazas
Muy rápido	Una etiqueta RFID puede ser utilizada por varias personas distintas	El equipo no necesita mucho espacio y no sería difícil integrarlo en el vehículo	Una etiqueta RFID es fácil de perder o de olvidar en casa
Independiente de las condiciones de iluminación	Funciona mejor cuando se utiliza conjuntamente con otros métodos	Puede ser utilizado durante la conducción	La etiqueta RFID puede ser robada
No intrusivo			
Fácil de utilizar			

Figura 30

Estadística descriptiva

	N	Mínimo	Máximo	Media	Desviación estándar
Útil / Inútil	18	,00	2,00	1,2778	,82644
Agradable / Desagradable	18	-2,00	2,00	,4444	,98352
Malo / Bueno	18	-1,00	2,00	,8333	1,09813
Simpático / Antipático	18	-2,00	2,00	,3333	1,32642
Efectivo / Superfluo	18	-2,00	2,00	1,0000	1,13759
Irritante / Agradable	18	-2,00	2,00	-,0556	1,21133
Colaborador / Inútil	18	-2,00	2,00	,7222	1,22741
No deseable / Deseable	18	-2,00	2,00	,2222	1,35280
Produce alerta / Produce sueño	18	,00	1,00	,1667	,38348
Utilidad	18	-1,00	1,60	,8000	,72274
Satisfacción	18	-2,00	1,50	,2361	,88895
Válido N (listado)	18				

Figura 31