



República Federativa do Brasil
Ministério do Desenvolvimento, Indústria
e do Comércio Exterior
Instituto Nacional da Propriedade Industrial.

(21) **PI0613023-2 A2**



* B R P I O 6 1 3 0 2 3 A 2 *

(22) Data de Depósito: 11/07/2006
(43) Data da Publicação: 14/12/2010
(RPI 2084)

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

(54) Título: **MÉTODOS E DISPOSIÇÃO PARA EXECUÇÃO DE VERIFICAÇÃO DE IDENTIDADE DE MOTORISTA**

(30) Prioridade Unionista: 11/07/2005 US 60/697,564

(73) Titular(es): VOLVO TECHNOLOGY CORPORATION

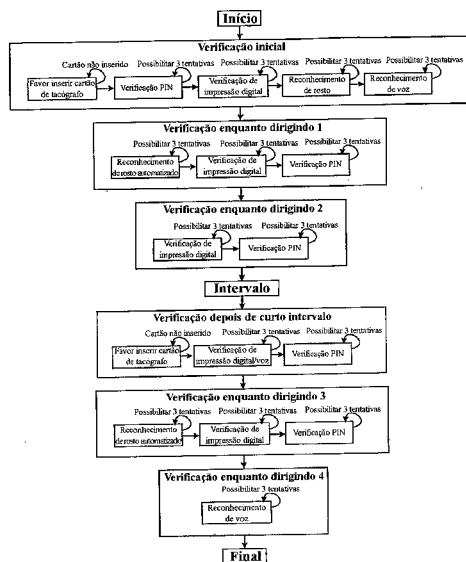
(72) Inventor(es): Björk, Hanna, Hagermann, Andreas, Larsson, Petter

(74) Procurador(es): MAGNUS ASPEBY E CLAUDIO SZABAS

(86) Pedido Internacional: PCT SE2006000869 de 11/07/2006

(87) Publicação Internacional: WO 2007/008159 de 18/01/2007

(57) **Resumo:** MÉTODOS E DISPOSIÇÃO PARA EXECUÇÃO DE VERIFICAÇÃO DE IDENTIDADE DE MOTORISTA. A presente invenção se refere a um método para assegurar que o operador de um veículo é um motorista autorizado. Em concordância com a presente invenção, o referido método está caracterizado pelo fato de que compreende: utilização de um sistema de verificação de motorista de modo múltiplo, embarcado, para verificar se um operador é um motorista autorizado; execução de um primeiro procedimento de verificação de motorista sobre um operador presente do veículo e determinar se o operador presente é um motorista autorizado ou não autorizado do veículo; execução de um segundo procedimento de verificação de motorista sobre o operador presente do veículo e determinar se o operador presente é um motorista autorizado ou não autorizado do veículo, em que referidos primeiro e segundo procedimentos de verificação de motorista são executados com um intervalo de tempo dentre eles, referido intervalo de tempo sendo dependente da natureza de trabalho sendo executado pelo operador; exercício de uma mensuração remediadora para impedir impacto potencialmente negativo quando o operador presente do veículo é determinado ser um motorista não autorizado fundamentado sobre pelo menos um dos procedimentos de verificação executados.



" MÉTODOS E DISPOSIÇÃO PARA EXECUÇÃO DE VERIFICAÇÃO
DE IDENTIDADE DE MOTORISTA "

CAMPO TÉCNICO DA PRESENTE INVENÇÃO

5 A presente invenção se refere a métodos e a uma
disposição para execução de verificação de identidade de
motorista.

PANORAMA DO ESTADO DA TÉCNICA DA PRESENTE INVENÇÃO

10 A indústria de transporte sofre de problemas com
contrabando e roubo de mercadorias valiosas. Diferentes
salvaguardas de segurança são um assunto principal em todo
o mundo, especialmente na mensurada em que ameaças
terroristas têm se intensificado. Uma maneira de aumentar o
15 nível de segurança poderia ser a de possuir um sistema de
verificação instalado em caminhões comerciais, de maneira a
assegurar que o motorista é aquele apropriado.

A patente alemã número **DE 43 26 514 A1** apresenta um
dispositivo eletrônico anti-roubo para veículos que
20 gradualmente torna um veículo a motor com controle
eletrônico de motor inoperante se um roubo, saque ou ataque
acontecer, se o motorista não puder provar sua autorização
de utilização pela inserção (codificação) de um número de
identificação pessoal (**PIN**). A investigação controlada pelo
25 sistema eletrônico de segurança de maneira a provar
identificação acontece em determinados intervalos adequados
no tempo de viagem ou ao longo da rota enquanto o veículo
está sendo utilizado. Se o motorista não é capaz de
proporcionar sua identidade dentro de uma janela de tempo
30 de resposta, a velocidade do veículo é incrementadamente

enforcada até que este venha a parar sem comprometer o tráfego pela intervenção no controle eletrônico de motor e após isso tão prontamente quanto possível este fica estacionário (imóvel) o veículo sendo bloqueado contra ser 5 dirigido para longe ou rebocado para longe pela intervenção no sistema de frenagem, e adicionalmente nos sistemas eletrônicos de trem de tração se eles estiverem presentes.

A patente alemã número **DE 101 56 731 A1** apresenta um método e um aparelho para verificação de operadores 10 autorizados de um veículo. Dados biométricos do operador a serem verificados são determinados antes e/ou durante direção (tração) do veículo e comparados com dados de referência. Se nenhuma igualdade (emparelhamento) é encontrada entre os dados biométricos mensurados e os dados 15 de referência, um sistema de controle operando automaticamente toma para si (assume) o controle do veículo.

A patente norte americana número **US 2004/078118 A1** se refere a um dispositivo para controlar um instrumento, que 20 coopera com um operador humano, em que o instrumento compreende um dispositivo de segurança paralelo ao instrumento, que pode interagir com um elemento habilitado proporcionado com recursos de memória e associado com um operador humano, particular, autorizado, o instrumento 25 sendo operável somente depois de interação com o elemento habilitado.

Em uma aplicação a ocorrência a ser observada pode ser armazenada no recurso de memória do elemento habilitado, por exemplo, para observação de veículos a motor levando-se 30 em consideração tempos de direção inaceitavelmente longos

de um motorista particular. Em uma outra aplicação, os recursos de controle de aeronaves são observados para assegurar que a aeronave possa ser pilotada somente por um piloto autorizado. Características corporais invariáveis do
5 motorista ou piloto, por exemplo, uma impressão digital, são armazenadas no elemento habilitado. As características corporais reais são detectadas por sensores e são comparadas com aquelas armazenadas. O veículo ou aeronave pode somente ser utilizado, se características corporais
10 detectadas e armazenadas forem idênticas.

A patente norte americana número **US 5.686.765 A1** proporciona um sistema para utilização com um veículo automotivo possuindo um sistema de ignição normalmente desabilitado. O sistema inclui um leitor, tal como um
15 leitor de impressão digital ou leitor de retina, para identificar o motorista. A saída a partir do leitor é comparada com correspondentes dados fisiológicos armazenados em memória para determinar se o motorista está autorizado a operar o veículo. Opcionalmente, um marcador
20 de tempo (*timer*) é empregado para permitir operação do veículo somente durante períodos de tempo prescritos pré-ajustados.

Um objetivo da presente invenção é o de proporcionar métodos e sistemas flexíveis, de fácil utilização, não
25 intrusivos, seguros contra enganos (falsificação) para verificação de motorista de caminhão. Um objetivo adicional da presente invenção é o de proporcionar métodos e sistemas de verificação e/ou de identificação similares.

O objetivo da presente invenção é conseguido pelas
30 características das **reivindicações de patente independentes**

posteriormente.

O pedido de patente possui **dois** propósitos. Um é o de encontrar métodos apropriados para verificação de motorista e construção de um protótipo de um sistema de verificação
5 que pode ser utilizado para testagem e adicional desenvolvimento. O outro é o de estudar como motoristas de caminhão percebem um tal sistema e como sua concepção vai ao encontro da crescente demanda para segurança mais alta. A aplicação está centralizada sobre a indústria de
10 transporte.

Onze métodos de verificação disponíveis foram estudados. Para possibilitar uma seleção bem fundamentada de métodos para implementação em um protótipo, perguntas e entrevistas com motoristas de caminhão e com contratantes
15 de transporte foram realizadas para complementar o estudo teórico.

Um regular e **três** métodos de verificação biométrica foram escolhidos para um teste; verificação de impressão digital, reconhecimento de rosto, reconhecimento de voz e
20 código **PIN**. Estes métodos foram colocados juntamente em um sistema que foi implementado em um simulador de direção de caminhão. Uma interface gráfica de usuário foi desenvolvida de maneira a tornar o sistema amigável ao usuário. **Dezoito** motoristas de caminhão testaram o sistema de verificação.
25 Eles foram exaustivamente entrevistados antes e depois do teste de maneira a recuperar suas experiências, expectativas e opiniões.

A maioria dos participantes de teste foi positiva para o sistema. Ainda que eles não sentissem uma necessidade
30 deste de imediato, eles acreditaram que este venha a ser

"para o futuro". Entretanto, alguns participantes se sentiram desconfortáveis com o sistema na mensurada em que eles se sentiram controlados por ele. Isto torna claro o quanto é importante possuir um sistema que respeite a privacidade dos usuários e assegurar que os usuários sejam bem informados acerca de como o sistema é utilizado. Alguma da tecnologia utilizada para o sistema de verificação requer mais desenvolvimento para adaptação (montagem) no contexto automotivo, mas é considerado ser possível conseguir um sistema seguro e robusto.

RESUMO DA PRESENTE INVENÇÃO

Como irá ser descrito em maiores detalhes aqui posteriormente, um número de invenções foram feitas no transcorrer da pesquisa e análise descritas levando-se em consideração sistemas de verificação de motorista.

Em pelo menos uma concretização, a presente invenção adota a forma de um método para assegurar que o operador de um veículo é um motorista autorizado. Isto é consumado através da utilização de um sistema de verificação de motorista de modo múltiplo, embarcado, utilizado para verificar se um operador é um motorista autorizado. Um primeiro procedimento de identificação de motorista é executado sobre o operador no veículo e é determinado se sim ou não ele ou ela é um motorista autorizado ou não autorizado do veículo. Normalmente, o teste irá somente ser para confirmar se a pessoa sendo avaliada é um motorista autorizado. Se o procedimento de identificação falha em confirmar que ele ou ela é autorizado, irá ser assumido e acionado como tal se for confirmado que eles não são

autorizados. Levando-se em consideração o efeito do primeiro procedimento de identificação, um segundo procedimento de identificação é subseqüentemente executado sobre o operador e é novamente tentado determinar se ele ou
5 ela é um motorista autorizado ou não autorizado. O primeiro e segundo procedimentos de identificação são executados com um intervalo de tempo dentre eles, e este intervalo de tempo é dependente da natureza do trabalho sendo executado pelo operador. Como um exemplo, o intervalo entre
10 confirmações de identificação irá ser diferente para motoristas de entrega urbana fazendo paradas freqüentes e entradas/saídas para o e a partir do veículo quando comparado com motoristas de transporte de longa duração fazendo somente umas poucas paradas durante o dia e
15 apresentando pouquíssimas oportunidades para operadores não autorizados furtarem o veículo. Finalmente, mensurações remediadoras (corretivas) irão ser exercidas de maneira a impedir impacto potencialmente negativo quando o operador presente do veículo é determinado ser um motorista não
20 autorizado fundamentado sobre pelo menos um dos procedimentos de identificação executados. Enquanto o caminhão normalmente não irá ser induzido a uma parada imediata fundamentada sobre uma falha de **ID** do operador como um motorista autorizado, coisas tais como notificações
25 para o escritório principal podem ser telematicamente afetadas ou se prevenir que ao veículo seja dada partida novamente depois da próxima parada feita pelo motorista.

É contemplado que os procedimentos de identificação de motorista podem ser diferentes uns a partir dos outros, ou
30 os assemelhados.

A segunda identificação de motorista pode ser iniciada imediatamente seguindo uma determinação de que o operador é um motorista não autorizado no primeiro procedimento de identificação de motorista.

5 Alternativamente, o segundo procedimento de identificação de motorista pode ser executado somente quando não pode ser determinado que o operador é um motorista autorizado fundamentado sobre execução do primeiro procedimento de identificação de motorista.

10 Em pelo menos uma concretização da presente invenção, um dos procedimentos de identificação é um teste de identificação passivo que não requer interação consciente pelo operador em associação com a execução dos procedimentos de identificação de motorista. Em um exemplo,
15 o teste de identificação passivo compreende um escaneamento de uma característica física do operador a partir da qual uma imagem é comparada com um conjunto de imagens de controle representativas de motoristas autorizados do veículo.

20 Pelo menos um dos primeiro e segundo procedimentos de identificação de motorista é um teste de identificação ativo que requer interação consciente pelo operador em associação com a execução do pelo menos um dos procedimentos de identificação de motorista. Um exemplo
25 deveria ser a colocação de um dedo ou da mão sobre um scanner. Alternativamente, o teste de identificação ativo pode incluir emissão de uma requisição para que o operador venha a inserir um número de identificação pessoal para o sistema identificando o operador como um motorista
30 autorizado. Uma outra forma de um teste de identificação

ativo compreende leitura de informação de identificação severamente codificada sobre um cartão de verificação apresentado pelo operador. O sistema após isso pode requerer que o operador venha a inserir um número de 5 identificação pessoal para o sistema que venha a corresponder a um número de identificação severamente codificado lido a partir do cartão de identificação. Similarmente, o teste de identificação ativo pode compreender emissão de um comando para que o operador venha 10 a falar uma sentença prescrita, registrando a sentença falada como um padrão de fala e comparando aquele padrão com um conjunto de padrões de fala de controle de motoristas autorizados do veículo.

Em uma variação ou desenvolvimento da presente 15 invenção, o primeiro e segundo procedimentos de identificação são de **dois** diferentes tipos um a partir do outro e eles são executados com intervalos de tempo randômicos dentre eles.

Em um outro aspecto inventivo da presente invenção, um 20 sistema de verificação automatizado é apresentado que avalia que uma das especialidades de fatores humanos de questões envolvidas com esta área é quando e como deveria um motorista ser verificado. Na medida em que a utilização de veículos comerciais difere dependendo da aplicação, 25 alguns motoristas deveriam deixar e adentrar seus veículos **vinte** vezes por dia enquanto que algum motorista faz a mesma coisa somente **duas** ou **três** vezes por dia. De maneira a manter um nível de segurança alto o suficiente sem que o sistema venha a se tornar irritante para o motorista, 30 diversas estratégias diferentes podem ser utilizadas. Uma

delas é executar verificação automática enquanto dirigindo. Por exemplo, um reconhecimento de rosto (verificação) pode ser executado durante direção (tração), sem que o motorista venha a ser informado disto. Se isto falha, o motorista
5 pode ser lembrado para inserir seu código **PIN** ou utilizar um outro método. A verificação pode ser executada com intervalos randômicos.

Em ainda um outro aspecto inventivo, um veículo é equipado com diversos métodos de verificação e o motorista
10 pode ser lembrado (alertado) com diferentes métodos em diferentes tempos. Se a escolha de método e tempo é randômica, o motorista não irá ter, de nenhuma maneira, conhecimento de quando ou de como verificar a si mesmo. Implementando esta espécie de não previsibilidade no
15 sistema, se aumenta o nível de segurança, na medida em que um impostor nunca deveria conhecer quando ou de que maneira ele deveria ter para se verificar a si mesmo.

Em ainda um outro aspecto inventivo, é avaliado que em sistemas biométricos não é o biométrico mensurado (imagem)
20 em si mesmo que é verificado (emparelhado), mas preferencialmente um gabarito (*template*) do biométrico; o que significa, um gabarito é extraído a partir do biométrico mensurado e comparado com um gabarito existente na base de dados. Um dos problemas com emparelhamento
25 contra um gabarito armazenado (ou o biométrica mensurado em si mesmo) é o fato de que uns biométricos da pessoa poderiam mudar ao longo do tempo, enquanto o gabarito armazenado não o faz. Por exemplo, uma impressão digital da pessoa poderia mudar devido a uma cicatriz ou uma senha
30 falada devido a doença ou idade. Uma solução para este

problema é atualizar o gabarito (manualmente ou automaticamente). Uma atualização automática pode ser conseguida em um sistema de verificação de modo múltiplo; o que significa, um sistema de verificação utilizando mais do que um biométrico/código **PIN**/cartão inteligente. Um ou mais métodos de verificação podem após isso ser utilizados para verificar o motorista enquanto um dos métodos não utilizado atualiza seu gabarito (se o processo de verificação foi bem sucedido). A propósito de exemplo, o motorista adentra seu veículo e é lembrado a verificar a si mesmo utilizando código **PIN**, impressão digital e reconhecimento de rosto. O sistema verifica o motorista utilizando código **PIN** e reconhecimento de rosto e utiliza o biométrico de impressão digital para atualizar o gabarito de impressão digital na base de dados.

Em um aspecto relacionado levando-se em consideração os gabaritos biométricos armazenados, uma questão crucial é onde se armazenar o gabarito. Fundamentalmente existem **três** alternativas; **(i)** uma base de dados no caminhão; **(ii)** uma base de dados no escritório de apoio (*back-office*) (requer comunicação em tempo real entre o veículo e o escritório de apoio); e/ou **(iii)** (interconexão) de uma base de dados que o motorista carrega com ele tal como um cartão inteligente. Uma opção é a de utilizar o cartão de motorista de *Tachograph* digital para armazenar gabaritos de verificação. O cartão é um cartão inteligente e, por conseqüência, adequado para esta espécie de armazenamento, mas de modo mais importante, isto é algo que o motorista é forçado a utilizar por lei (pelo menos na Europa) e é, por conseqüência, sempre carregado com o motorista.

Em um outro aspecto inventivo, redundância é instituída em apreciação da incerteza tipicamente relacionada para sistemas de verificação de identificação conhecidos. A execução de um método de reconhecimento de rosto poderia, por exemplo, ser afetada pelas condições de iluminação. Utilizando diversos métodos (por exemplo, reconhecimento de rosto e código **PIN**), redundância é conseguida no sistema. Por exemplo, um motorista está dirigindo na estrada e um reconhecimento de rosto agendado automaticamente é executado e este falha por alguma razão (condições de iluminação podem estar ruins ou os assemelhados). O motorista é conseqüentemente interpelado para verificar a si mesmo utilizando impressão digital e código **PIN**.

Finalmente, deveria ser apreciado que cada um dos aspectos descritos anteriormente, tanto sozinhos ou quanto em combinação, podem ser implementados em um contexto de telemática. Ou seja, o sistema de verificação pode reportar/receber informação e os assemelhados para um/a partir de um escritório de apoio ou de uma rede de segurança em um nível de companhia/nacional/internacional. Como um exemplo, ex-condenados podem ser impedidos de dirigir veículos de transporte de mercadorias perigosas pela verificação de seus dados biométricos detectados contra uma base de dados nacional/internacional a respeito de criminosos.

BREVE DESCRIÇÃO DOS DESENHOS DA PRESENTE INVENÇÃO

A presente invenção juntamente com os objetivos e vantagens anteriormente mencionados pode ser mais bem

compreendida a partir da descrição detalhada posteriormente das concretizações e com referência aos **desenhos** acompanhantes em que esquematicamente:

5 A **Figura 1** mostra etapas para inscrever/emparelhar usuários em métodos de verificação os mais comuns;

 A **Figura 2** mostra uma impressão digital com sulcos e vales formando um padrão, que está caracterizado por linhas irregulares e incoerentes;

10 A **Figura 3** mostra diversos tipos de características distintas de uma impressão digital para análise, por exemplo, *loops*, arcos e espirais;

 A **Figura 4** mostra um *scanner* capacitivo para escaneamento de um dedo;

15 A **Figura 5** mostra um método **RF** para escaneamento da impressão abaixo da superfície efetiva da ponta do dedo;

 A **Figura 6** mostra um scanner de íris;

 A **Figura 7** mostra uma íris escaneada;

20 A **Figura 8** mostra uma termografia de rosto para reconhecimento de rosto, com a utilização de um padrão de calor de uma câmara de infravermelho, fundamentado sobre um padrão do vaso sanguíneo de rosto de uma pessoa sendo único para cada pessoa;

 A **Figura 9** mostra uma fotografia de uma retina para
25 reconhecimento de retina;

 A **Figura 10** mostra a imagem da retina;

30 A **Figura 11** mostra um *scanner* de geometria de mão mensurando o comprimento, a largura, a espessura e a curvatura dos dedos;

A **Figura 12** mostra uma visão geral de um sistema de verificação implementado, as flechas mostrando como as diferentes partes se comunicam uma com a outra;

A **Figura 13** mostra uma fotografia de partes do sistema montado no coupê de caminhão;

A **Figura 14** mostra **dois** exemplos de uma interface gráfica de usuário;

A **Figura 15** mostra uma fotografia de um simulador;

A **Figura 16** mostra uma fotografia de um simulador;

10 A **Figura 17** mostra um cenário de teste com uma verificação inicial consumada com um intervalo (uma parada rápida) seguido por uma curta verificação, utilizando tanto impressão digital ou quanto voz e uma outra verificação enquanto dirigindo sendo requisitada;

15 A **Figura 18** mostra um diagrama de cada contagem média de participantes levando-se em consideração utilidade e satisfação;

A **Figura 19** mostra um diagrama com respostas de participantes antes e depois do teste;

20 A **Figura 20** mostra uma tabela levando-se em consideração impressões digitais como método de verificação;

A **Figura 21** mostra uma tabela levando-se em consideração escaneamento de íris como método de verificação;

A **Figura 22** mostra uma tabela levando-se em consideração verificação de voz como método de verificação;

30 A **Figura 23** mostra uma tabela levando-se em consideração reconhecimento de rosto como método de verificação;

A **Figura 24** mostra uma tabela levando-se em consideração termografia de rosto como método de verificação;

5 A **Figura 25** mostra uma tabela levando-se em consideração escaneamento de retina como método de verificação;

A **Figura 26** mostra uma tabela levando-se em consideração escaneamento de movimentação de lábios como método de verificação;

10 A **Figura 27** mostra uma tabela levando-se em consideração reconhecimento de geometria de mão como método de verificação;

A **Figura 28** mostra uma tabela levando-se em consideração senhas e escaneamento de **PIN** como método de verificação;

A **Figura 29** mostra uma tabela levando-se em consideração cartões como método de verificação;

A **Figura 30** mostra uma tabela levando-se em consideração **RFID** como método de verificação; e

20 A **Figura 31** mostra uma tabela levando-se em consideração estatísticas a partir de *van der Laans Acceptance Scale* (Escala de Aceitação de *van der Laans*).

As **Figuras** são somente representações esquemáticas e a presente invenção não está limitada para estas concretizações.

DESCRIÇÃO DETALHADA DA PRESENTE INVENÇÃO

30 Às questões de segurança são determinadas altas prioridades em todo o mundo. Isto tem também afetado a

industria automotiva, que tem elevado a questão de que se isto deveria ser possível aumentar a segurança por implementação de um sistema de verificação de motorista em veículos comerciais. Questões que irão ser exploradas aqui são, por exemplo, que tipo de verificação utilizar e a quem um tal sistema deveria beneficiar. Esta seção contém um panorama, um propósito e as restrições para o presente pedido de patente. Para determinar uma visão geral do pedido de patente esta seção é concluída com um guia de leitura.

Devido às crescentes ameaças terroristas, grandes investimentos em pesquisas e desenvolvimentos são feitos de maneira a aumentar a segurança na sociedade. O *Department of Homeland Security* (Estados Unidos da América) é um exemplo deste esforço. Independentemente de como é apresentada, segurança é um tópico que tem se tornado cada vez mais importante, especialmente depois dos ataques terroristas contra o *World Trade Center* em **2.001**. Muitas mudanças na legislação já foram feitas, especialmente nos Estados Unidos da América. Por exemplo, existe uma legislação proposta de que todos os caminhões que realizam transporte de mercadorias perigosas têm que possuir um sistema de verificação de motorista biométrico. Isto na medida em que o governo dos Estados Unidos da América deseja prevenir que criminosos (em registros do **FBI**) venham a realizar transporte de mercadorias perigosas. As demandas para um sistema de verificação flexível, seguro e confiável são, conseqüentemente altas, na medida em que existem cerca de **8 milhões** de motoristas de caminhão profissionais nos Estados Unidos da América. A **EU** (União Européia) juntamente

com outras associações e países tem também feito grandes investimentos em pesquisa de segurança e administração de crises.

Um exemplo das demandas por segurança crescentes é a de que diversos aeroportos, por exemplo, o *Amsterdam Airport Schiphol* e o aeroporto em *Umeå*, Suécia, têm testado a utilização de verificação biométrica de seus passageiros. Depois de um ano piloto em **2.001**, um sistema de passagem de fronteira automático, utilizando reconhecimento de íris, é agora permanente no *Amsterdam Airport Schiphol*.

Para cumprir com as demandas a partir do mercado e com as mudanças em legislação, novos produtos frequentemente possuem sistemas de segurança mais avançados do que aqueles mais antigos, utilizando técnicas de verificação e de identificação mais avançadas. Um exemplo são *notebooks* com *scanners* de impressão digital embutidos.

Contrabando, ataques terroristas e roubo de mercadorias valiosas são cenários que usualmente envolvem veículos roubados. A indústria de transporte é, por conseqüência, um segmento natural a ser focalizado para aperfeiçoar a segurança pública. Uma visão central quando se reforçando transporte seguro e segurança é verificar que o motorista é quem ele reivindica ser (ele diz que é).

Esta presente invenção combina **duas** diferentes competências e resultados em um teste de possíveis técnicas que poderiam ser adequadas para verificação de motorista, mas também em uma avaliação das opiniões dos motoristas sobre o sistema. Entrevistas e averiguações irão mapear as opiniões dos motoristas antes e depois de testagem de um protótipo. Uma comparação entre qual recurso de segurança

para o grupo interessado/os fabricantes e como isto se coaduna com a concepção dos motoristas de utilidade, segurança e privacidade irão também ser executados.

5 **BENEFÍCIOS DE UM SISTEMA DE VERIFICAÇÃO DE MOTORISTA**

Caminhões são utilizados para diversos propósitos. Por conseqüência, um sistema flexível, que pode se adaptar em diversificadas situações, é requerido. Conseqüentemente, muitos diferentes desafios aparecem quando se vem a
10 projetar um tal sistema. É desejável se satisfazer tantas demandas quanto possível, ainda que seja impossível se construir um sistema para todos os propósitos. Um poucas diversas situações quando um sistema de verificação de motorista poderia ser benéfico estão ilustradas
15 posteriormente.

Na América do Sul existem grandes problemas com veículos roubados. Isto tem conduzido para um procedimento rotineiro que, quando transportando mercadorias valiosas, o motorista liga para a companhia de seguros a cada **10**
20 **minutos** para assegurar que tudo está correndo bem. Se o veículo estiver equipado com um sistema de verificação, o sistema poderia continuamente assegurar para a companhia de seguros que o veículo está sendo dirigido pelo motorista apropriado, por conseqüência, possibilitando que o
25 motorista venha a se concentrar sobre sua função de direção.

Um sistema de verificação poderia possibilitar que um contratante de transporte pudesse ter certeza de que o motorista não foi anteriormente sentenciado por má conduta
30 relacionada ao tráfego. Para armazenar a informação acerca

dos motoristas uma base de dados deveria ser requerida. Se aquela base de dados estiver conectada para as autoridades, uma verificação de arquivo poderia ser feita quase que em tempo real.

5 Um contratante de transporte que possui tanto verificação de motorista e quanto um dispositivo de consumo de álcool montado em veículo poderia receber um "sinal de motorista confiável". Clientes poderiam após isso ser assegurados de que suas mercadorias são transportadas por
10 um motorista "confiável". Cooperação com a associação nacional de estradas e as companhias de seguros poderia resultar em custos reduzidos com seguros de veículos.

Um bônus para a utilização de um sistema de verificação poderia ser o de que, motoristas confiáveis,
15 verificados poderiam ser privilegiados para passar estações de avaliação ou instrumentos de estrada. Isto deveria facilitar o trabalho para os motoristas e tornar o transporte mais eficiente.

Uma verificação que associa os parâmetros registrados
20 para um motorista específico poderiam controlar se alguém dirige por mais tempo do que as **4,5 horas** estabelecidas por lei (Legislação Européia) sem uma parada (um intervalo). Neste caso, um alerta poderia ser enviado para o motorista e bem como para o contratante de transporte.

25 Na Suécia, casos de demissão ocorreram devido para o fato de que os processados responsabilizaram um ao outro. Em caso de acidente ou crime, um sistema de verificação poderia assegurar aos investigadores quem efetivamente dirigiu o veículo naquele tempo específico.

30 Se um veículo é roubado e existe uma demanda para

verificação de que o impostor não irá ir para muito longe antes que o sistema venha a revelar o roubo. Isto garante mensurações mais rápidas se o veículo foi exposto ao crime.

As aduaneiras suecas possuem um processo chamado "Servicetrappan" (a escada de serviço) de maneira a simplificar o procedimento de aduaneira para companhias confiáveis. O processo consiste de um número de etapas de classificação (*ranking*). Quanto mais elevada a classificação da companhia, tanto mais tranqüila a passagem através das aduaneiras. Um sistema de verificação de motorista poderia ser uma parte deste processo, oferecendo aos contratantes de transporte com motoristas verificados e confiáveis uma classificação mais elevada e, por conseqüência, liberações de aduaneiras mais eficientes.

Adicionalmente, se existe um sistema de verificação no caminhão, o motorista poderia se beneficiar a partir dele, na medida em que deveria ser possível automaticamente ajustar os ajustamentos no ambiente de motorista em concordância com as preferências pessoais do motorista. Como exemplo, ajustamentos para o assento de motorista, controle de climatização e de equipamento de som poderiam ser automaticamente ajustados. Isto está, entretanto, além do enfoque deste pedido de patente.

Existem **dois** propósitos principais com este pedido de patente. Um é o de encontrar métodos apropriados para verificação de motorista e construir um protótipo de um sistema de verificação que pode ser utilizado para testagem e desenvolvimento adicional. O outro propósito é o de estudar como os motoristas percebem um tal sistema e como sua concepção vai de encontro com a demanda crescente para

segurança mais elevada.

Estes **dois** propósitos podem ser resumidos como:
"Estudar as possibilidades para utilização de métodos de
verificação disponíveis para projetar um sistema flexível,
5 de fácil utilização, não intrusivo, seguro contra enganos
para verificação de motorista de caminhão".

Embora os métodos de verificação descritos aqui possam
ser utilizados em quase qualquer tipo de veículo, o enfoque
deste pedido de patente irá ser para caminhões comerciais e
10 para a indústria de transporte.

Três métodos biométricos irão ser implementados e
testados no protótipo. A seleção de método irá
principalmente contar com a teoria que foi lida durante o
trabalho, mas preço e tempo de entrega podem também afetar
15 as decisões.

Uma **GUI** (**Graphical User Interface** - Interface Gráfica
de Usuário) foi desenvolvida para facilitar a comunicação
entre o sistema de verificação e o usuário. Entretanto,
nenhuma teoria acerca de habilidade de usuário e projeto
20 irá ser mencionada na medida em que o autor que desenvolveu
a **GUI** já é possuidor deste conhecimento antecipadamente.
Além disto, é o sistema, e não a **GUI** que está sendo
enfocada para este pedido de patente.

Um sistema de verificação em um veículo abre muitas
25 possibilidades para reforçar a segurança. Algumas das
questões que irão ser enfocadas são que tipo de verificação
se utilizar e a quem um tal sistema deveria beneficiar.
Entretanto, o assunto de segurança não é somente assunto
para ser levado consideração quando se constrói um tal
30 sistema de verificação. A privacidade do motorista e

concepções de segurança deveriam também ser levadas em consideração. Estas diferentes visões conduzem para abordagens separadas para o problema, as diversas perspectivas de proteção (seguridade), segurança e 5 privacidade são conseqüentemente aqui explanadas. Isto é também para esclarecer o que estas expressões aqui estabelecidas e para mostrar porque elas são importantes para este pedido de patente.

10 **PROTEÇÃO (SEGURIDADE)**

Existem tipos diferentes de proteção, tais como pessoal, privada, pública e de segurança nacional. Todos estes aspectos tornam difícil proporcionar uma definição única. Um pensamento de concepção rotineiramente aceita, é 15 o de que proteção (seguridade) significa qualidades ou mensurações tomadas para reduzir a probabilidade de que incidentes indesejados venham a acontecer.

As salvaguardas de proteção dentro desta tese incluem todas as aplicações referidas anteriormente. Segurança 20 pública e segurança nacional são questões para considerar quando se levando em consideração os riscos de ataques terroristas. Os riscos em conjunção com transporte de mercadorias perigosas também afetam a segurança pública. Os riscos de veículos roubados são endereçados às companhias 25 de seguro. Finalmente, segurança pessoal é endereçada pelos riscos, bem como benefícios, que poderiam chegar levando-se em consideração a implementação de um sistema de verificação de motorista. Estes diversos assuntos irão ser apresentados aqui posteriormente.

PRIVACIDADE

O propósito principal como o sistema de verificação é o de aumentar o nível de segurança. Uma maneira de se fazer isto é a de utilizar métodos biométricos. O problema é o de que eles em si mesmos são uma ameaça, na medida em que eles poderiam se intrometer com uma privacidade pessoal. Portanto, a privacidade do usuário é uma outra questão que irá ser aqui considerada.

Privacidade pode ser descrita como o direito de se possuir uma esfera pessoal de proteção da individualidade de alguém e de se ter capacidade de manter algumas coisas de alguém em si mesmas, sem qualquer discriminação a partir de autoridades públicas, empregadores ou outros. Métodos biométricos podem proporcionar a sensação da observação global (integral) "*Big Brother*" (como em "**1984**" de *George Orwell*). Em assim sendo, os métodos podem ser percebidos como se eles fossem violações de uma privacidade pessoais.

SEGURANÇA

Segurança e proteção não são exatamente a mesma coisa, ainda que elas estejam intimamente relacionadas. Segurança pode ser definida como quando, ou onde, uma pessoa pode fazer alguma coisa, sem estar amedrontada que alguma coisa indevida (ilegal) está para acontecer. Boa proteção pode, por consequência, resultar em segurança percebida.

Ainda que todos os métodos sejam seguros para utilizar, uma pessoa poderia não desejar utilizá-los se vem a perceber estes como intrusos ou se vem a pensar que estes poderiam prejudicar esta pessoa de qualquer forma. A concepção do usuário de um sistema tem que consequentemente

ser considerada, porque não importa quão seguro um método é; uma pessoa que não confia nele não irá utilizá-lo. Não faz nenhuma diferença se o motorista utilizou um método ou não, ele irá sempre possuir opiniões sobre este método.

5 Entretanto, sua concepção não está sempre em concordância com fatos e realidade. Escaneamento de íris, por exemplo, é considerado um dos métodos mais precisos e também um método seguro de utilizar, mas muitas pessoas não gostam da idéia de utilização de um sistema que escaneia os olhos. Uma

10 pessoa que tem medo de que este escaneamento poderia fazer mal aos olhos não irá perceber um tal sistema como seguro.

Coisas que são desconhecidas freqüentemente fazem as pessoas se espantarem (se intimidarem), e informação é, por consequência, importante na medida em que conhecimento

15 poderia diminuir sentimentos negativos. Como anteriormente estabelecido, pessoas tendem a acreditar que escaneamento de íris é um método de verificação desconfortável, mas um teste realizado pela **SAS** se provou diferentemente. Eles avaliaram **dois** diferentes sistemas de verificação no

20 aeroporto de Umeå; impressão digital e escaneamento de íris. Passageiros freqüentes participaram do teste e utilizaram verificação de impressão digital metade do tempo e escaneamento de íris metade do tempo. A maior parte dos participantes foi positiva para a utilização de biométricos

25 (**78 %** acreditavam que a **SAS** deveria introduzir verificação biométrica dos passageiros) e neste caso o escaneamento de íris foi graduado ligeiramente mais alto do que verificação de impressão digital. Isto significa que os usuários foram convencidos de que o sistema é um benefício para eles e seu

30 trabalho; por outro lado eles não concordaram em utilizar o

sistema.

VERIFICAÇÃO DE MOTORISTA APROPRIADO DE VEÍCULO

Existem muitos diferentes métodos de verificação no
5 mercado atualmente, alguns deles já em utilização, outros
brevemente chegando. A despeito disto, não existe nenhuma
verificação atualmente de quem está efetivamente dirigindo
um veículo. A intenção com isto é a de introduzir alguns
dos diversos métodos para verificação e listar suas
10 vantagens e desvantagens, a partir tanto de uma perspectiva
automotiva e quanto de uma perspectiva de usuário. A seção
inclui uma introdução para biométricos e descrições de
diferentes métodos biométricos. **PINs** (*Personal*
Identification Numbers - Números de Identificação Pessoal),
15 senhas e diversos tipos de cartões são também métodos para
verificação. Na medida em que eles são utilizados
freqüentemente hoje em dia, eles são assumidos serem bem
conhecidos para o leitor e são somente brevemente aqui
mencionados.

20 Uma vantagem universal para todos estes métodos é a de
que o usuário deve dar uma pausa em sua tarefa presente de
maneira a realizar a verificação. Isto aumenta sua
consciência de risco e pode influenciá-lo a ser mais atento
e cuidadoso.

25

UMA INTRODUÇÃO PARA MÉTODOS BIOMÉTRICOS

A palavra biometria tem sua origem no latim e pode ser
traduzida para "vida mensurada". Biometria usualmente se
refere a estudos estatísticos das características, de
30 organismos vivos, que podem ser mensuradas. Biometria por

outro lado, é de preferência utilizada para análise para identificar humanos pela mensuração de suas características. Métodos biométricos foram utilizados para propósitos de identificação e de verificação na medida em
5 os últimos anos do século **XIX**. Quando se referindo a métodos biométricos de verificação/identificação neste pedido De patente, se quer significar métodos que analisam uma ou mais das características corporais únicas de uma pessoa, tais como mãos, rosto ou olhos.

10 O método de verificação o mais apropriado varia dependendo de onde e por qual razão, ele irá ser utilizado. Entretanto, existem **três** demandas fundamentais, que alguém deveria se esforçar para satisfazer quando decidindo que método utilizar. Para conseguir o método ideal para
15 verificação, a característica a ser mensurada deveria ser única, o que significa alguma característica para aquele indivíduo, permanente, o que significa que ela não deveria mudar ao longo do tempo e finalmente ela deveria também ser universal, o que significa que todo mundo deveria possuí-
20 la. A aceitabilidade e bem como a acessibilidade das características analisadas por um método deveriam também ser consideradas. Uma característica biométrica é aceitável se ela não é percebido como intrusiva pelo usuário para mensurá-la. Se uma característica é fácil para apresentar
25 para um sensor, aquela característica é referida como acessível.

Basicamente existem **três** maneiras para uma pessoa identificar a si mesmo; possuir alguma coisa, um cartão de acesso, por exemplo; conhecer alguma coisa, por exemplo,
30 uma senha ou um código **PIN**; ser alguém, utilizando métodos

biométricos para identificação.

A maior parte dos métodos biométricos aqui descritos podem ser utilizados tanto para verificação e quanto para identificação, mas a distinção entre as **duas** expressões, 5 deveria ser observada.

Identificação: Quando um método é utilizado para encontrar quem é uma pessoa em um grande grupo, este é chamado 10 identificação. Isto é algumas vezes referido como "uma para muita comparação". Isto significa pesquisa através do grande grupo para encontrar um indivíduo que combine com a 15 característica que é utilizada para a identificação.

Verificação: Quando um método é utilizado para analisar se uma pessoa é quem ela reivindica ser, este método é chamado 20 verificação. Isto é algumas vezes referido como "uma para uma comparação". Neste caso isto é somente necessário comparar a característica de uma pessoa contra os dados que foram 25 registrados naquele nome da pessoa.

Este pedido de patente irá ser focado sobre verificação na medida em que o motorista é suposto ser conhecido para a companhia. O sistema é, por consequência, somente utilizado para verificar que aquele é realmente o 30 motorista quem se espera estar atrás do volante de direção.

Existe um número de vantagens que torna a utilização de métodos biométricos para verificação digna de ser levada em consideração; características biométricas não podem ser esquecidas; atributos físicos não podem ser confundidos; atributos físicos são mais difíceis de falsificação do que 5 cartões de identidade; padrões de impressão digital e outras características biométricas não podem ser adivinhadas ou reveladas tão facilmente quanto, por exemplo, uma senha.

10 Um problema com sistemas biométricos de proteção é o da extensão do dano que ele pode provocar no caso de alguém eventualmente manipular para roubar a informação de identidade. Se uma pessoa perde um cartão de crédito, ou se outra pessoa qualquer descobre o código secreto **PIN** para 15 desligar o alarme de arrombamento, é sempre possível adquirir um novo cartão, ou mudar o código. Entretanto, se impressões digitais de uma pessoa são copiadas é impossível adquirir umas novas. A pessoa deveria não demoradamente ter a capacidade para utilizar as impressões para verificação 20 na medida em que existiria sempre um risco de que outra pessoa qualquer viesse a reivindicar ser esta pessoa.

No caso de roubo é importante atualizar bases de dados de interesse e registrar itens de identidade roubados de maneira que um possível impostor não pode utilizá-los. Um 25 dos terroristas em **11** de setembro de **2.001** utilizou um passaporte que foi roubado de um saudita, nos Estados Unidos da América, **cinco** anos antes. Com uma base de dados atualizada isto poderia talvez ter sido evitado. Se os passageiros antes de **2.001** também tivessem tido necessidade 30 de identificar a si mesmos biometricamente, deveria ter

sido mais difícil para os terroristas serem bem sucedidos em sua missão. Ainda, métodos de verificação biométricos não são uma solução perfeita. Um impostor pode atacar a base de dados, ou a conexão entre a base de dados e o scanner, de maneira a burlar ou manipular o sistema. Por conseqüência, mesmo se o propósito for encontrar uma solução suficientemente segura, é impossível eliminar completamente todos os riscos.

10 **O PROCESSO DE VERIFICAÇÃO**

Esta seção irá determinar uma visão global dos métodos de verificação os mais comuns. A maior parte deles utiliza as seguintes etapas para listar/emparelhar (registrar/comparar) usuários de acordo com a **Figura 1**:

15

Aquisição de Dados: O sensor escaneia o sujeito.

Sinal de Pré-processamento: Por exemplo, removendo ruído de ambiente em um sistema de reconhecimento de voz.

20

Extração de Característica: Analisando as diferentes características e criando um gabarito fundamentado sobre um sub-conjunto dos dados adquiridos.

25

Protocolo/Emparelhamento: Tanto adicionando o gabarito para a base de dados (protocolo) ou comparando este com gabaritos já na base de dados (emparelhamento).

30

Decisão: Um emparelhamento bem sucedido autoriza o sujeito, uma falha rejeita autorização.

Gabaritos são primordialmente feitos por **duas** razões. Uma é reduzir a quantidade de dados armazenados e a outra é reduzir a complexidade da fase de emparelhamento seguinte. Um outro benefício com gabaritos é o de que, por exemplo, se utilizando um *scanner* de impressão digital, a integridade de imagem da impressão não está armazenada, simplesmente um gabarito de características únicas. Isto torna difícil a utilização do gabarito para reproduzir a impressão.

DETECÇÃO DE VITALIDADE

Um impostor poderia tentar utilizar uma fraude ou remover o dedo de um usuário autorizado para passar a um *scanner* de impressão digital. A mesma coisa acontecendo para escaneamento de íris e geometria de mão. Alguns sistemas de reconhecimento de voz poderiam ser burlados por um gravador e um sistema de reconhecimento de rosto por uma fotografia de um usuário autorizado. Entretanto, existem medidas para se evitar isto. Um sistema de verificação biométrica pode ser equipado com detecção de vitalidade para assegurar que a amostra recuperada é de um ser humano. A detecção de vitalidade vem a adequar o método de verificação. De que forma detecção de vitalidade pode ser implementada para cada método está, por consequência, aqui apresentada.

O procedimento fundamental para sistemas de verificação foi explanado anteriormente nesta seção. Descrições de diversos diferentes métodos de verificação biométrica: suas histórias, como eles funcionam, suas 5 vantagens e desvantagens, irão ser aqui apresentadas.

VERIFICAÇÃO DE IMPRESSÃO DIGITAL

Impressões digitais são provavelmente o mais bem conhecido e difundido método de identificação biométrica. 10 Durante o fim do século **XIX** e o início do século **XX** diversos diferentes tipos de métodos de identificação foram desenvolvidos. Normalmente estes métodos fazem alguma espécie de classificação bem coberta levando-se em consideração uns poucos padrões primordiais. Observando a 15 impressão digital, os sulcos e vales formam um padrão, que é caracterizado por linhas irregulares e incoerentes. Os *scanners* de hoje em dia são muito rápidos e precisos e o método está começando a se tornar aceito para utilização no dia a dia (Ver **Figura 2**).

20 Comparação da integridade de impressão toma uma grande quantia de energia de processamento e, conseqüentemente, *scanners* usualmente enfocam em características especiais, por exemplo, onde sulcos terminam ou se dividem em **dois**. Estas características são chamadas minúcias. Os *scanners* 25 utilizam algoritmos complexos para encontrar e analisar as minúcias de maneira a fazer a comparação. A idéia fundamental é mensurar as posições relativas das minúcias, da mesma maneira que uma parte do céu é reconhecida pelas posições relativas das estrelas. Existem diversos tipos de 30 características distintas da impressão para analisar, por

exemplo, loops, arcos e espirais (Ver **Figura 3**).

Os sistemas de busca automáticos de hoje em dia são usualmente feitos utilizando algoritmos de dados para classificar e comparar um gabarito recente, codificado a partir da impressão digital escaneada, com uma coleção armazenada de gabaritos.

Os *scanners* de impressão digital são primordialmente ópticos ou capacitivos ainda que outras tecnologias existam: tais como frequência de rádio (**RF**), ultra-som ou *scanners* de silício.

Um *scanner* óptico é fundamentalmente uma pequena câmera digital, que usualmente tira uma fotografia invertida da impressão digital, tornando os sulcos mais escuros sobre a fotografia. Antes de comparação da imagem, o processador de *scanner* executa uma série de testes para determinar se a imagem é boa o suficiente.

Se a fotografia é excessivamente escura ou excessivamente brilhante, o *scanner* automaticamente muda o tempo de exposição para permitir mais ou menos iluminação antes de tirar uma nova fotografia.

Um *scanner* capacitivo utiliza uma ordenação de pequenas placas, cada uma menor do que a largura de um sulco e conectada para um amplificador invertido. Quando o dedo é colocado sobre o *scanner* o dedo e as placas formam um capacitor simples. Uma carga de referência é enviada para as placas, provocando que os capacitores venham a ser carregados. Dependendo da distância entre as placas e o dedo, (se é um sulco ou um vale), o amplificador correspondente irá apresentar uma voltagem diferente. Estas voltagens formam a "imagem" da impressão digital. Isto

torna mais difícil utilizar um papel simples, com uma imagem em preto e branco da impressão, para burlar o *scanner* capacitivo. Adicionalmente, os *scanners* capacitivos podem ser feitos menores do que os *scanners* ópticos (Ver **Figura 4**).

Uma tecnologia de escaneamento de impressão digital recentemente desenvolvida é o escaneamento **RF** que utiliza um sinal de rádio de baixa energia para escanear a impressão. **RF** possui a vantagem de que ele escaneia a impressão abaixo da superfície efetiva da ponta do dedo e é, portanto, menos sensível à sujeira, aos danos e aos defeitos (Ver **Figura 5**).

Uma outra distinção a ser feita quando apresentando *scanners* é aquela entre *scanner* de varredura e *scanner* de área. Sobre um *scanner* de varredura o dedo é arrastado passado o sensor, enquanto que sobre um *scanner* de área o dedo é colocado sobre o sensor e mantido lá até que o escaneamento seja completado. A maior parte dos *scanners* de hoje em dia são sensores de área, mas o modelo possui algumas desvantagens. O sensor se torna sujo. Isto não somente afeta a execução de escaneamento; algumas pessoas podem ter aversão contra colocar seus dedos sobre um sensor sujo. Problemas com impressões latentes existem. Isto significa que a impressão precedentemente escaneada permanece sobre a superfície de sensor e se torna reativada durante o escaneamento da segunda impressão digital.

O sujeito pode colocar o dedo obliquamente sobre o sensor. A maior parte dos *scanners* não tolera um ângulo rotacional maior do que **20 graus - 30 graus**.

Sensores (particularmente sensores capacitivos) são

caros por unidade de área. A área de sensor sobre um *scanner* de varredura pode ser feita menor e, portanto, menos dispendiosa.

O *scanner* de varredura também não é uma solução
5 perfeita. As questões principais são que eles usualmente
levam algum tempo para adquirir uma técnica de varredura
correta e que as fatias têm que ser reconstruídas para uma
impressão digital, o que pode ser consumidor de tempo.
Existem, por conseqüência, muitos diferentes parâmetros
10 para serem considerados quando escolhendo um *scanner* para
circunstancias específicas. Qual técnica de sensor utilizar
é, conseqüentemente, um assunto importante.

Um *scanner* óptico pode ser enganado por uma fotografia
da impressão, um *scanner* capacitivo por um molde. Um molde
15 pode ser feito de gelatina, de silicone ou até mesmo de
massinha *play-doh*. Para criar um molde, o dedo efetivo é
requerido. Mas, para obter uma fotografia que poderia
fraudar um *scanner* óptico, é suficiente possuir alguma
coisa que uma pessoa tenha tocado, como um vidro, para
20 criar uma imagem da impressão digital daquela pessoa.
Portanto, o *scanner* óptico é mais fácil de ser enganado.
Existem numerosos outros métodos para enganar o sistema,
como luzes pisca-pisca, calor, umidade ou diversos pós.
Entretanto, estes métodos para enganar o sistema são úteis
25 se o *scanner* está equipado com a assim chamada detecção de
vitalidade.

Detecção de vitalidade pode ser realizada de um número
de maneiras; pela análise de temperatura, de pulsação, de
fluxo sanguíneo, de oximetria de pulso, de resistência
30 elétrica, de **EGG**, de permissividade dielétrica relativa,

de deformações de poro ou de pele, ou de combinações destes. Métodos de detecção de vitalidade são mais ou menos fáceis de se adquirir. Um problema primordial é o de que o *scanner* venha a determinar se a impressão escaneada é uma
5 parte do dedo, uma imagem de folha fina, ou um molde atado para a ponta de dedo. Um novo método utilizando transpiração poderia ser a solução, mas isto está ainda sob desenvolvimento e, conseqüentemente, não é possível confiar que esta solução realmente funciona bem (direito).

10 Todos os **dez** dedos possuem impressão única, o que torna possível utilizar qualquer dedo para verificação. Gêmeos idênticos poderiam possuir impressões digitais similares, mas não idênticas, na medida em que até mesmo gêmeos possuem suas próprias impressões digitais únicas. É
15 referido que uma pessoa deixa pelo menos vinte e **cinco** impressões digitais perfeitas para trás a cada dia e um problema primordial com impressões digitais é o de que elas são totalmente fáceis para serem copiadas.

A maior parte das pessoas inicialmente coloca seus
20 dedos em uma posição incorreta sobre o *scanner*, na medida em que elas assumem suas impressões digitais como sendo a ponta dos dedos, quando de fato o dedo tem que ser colocado um pouco abaixo para proporcionar uma imagem que pode ser processada para verificação. Alguns *scanners* são projetados
25 para facilitar o posicionamento correto do dedo, utilizando, por exemplo, pinos (pegas) de guia ou depressões.

Deveria ser observado que nem todas as pessoas podem utilizar este método; como uma matéria (um assunto) de
30 importância, mais de **5 %** possuem impressões digitais que

não podem ser lidas por *scanners* de impressão digital. Cicatrizes, calosidades ou outros defeitos afetam o resultado e pessoas podem possuir sulcos e vales tão finos ou danificados que a resolução de *scanners* não é boa o bastante. Além do mais, ainda que a maior parte das pessoas veja este método como não intrusivo, algumas pessoas possuem aversões contra escaneamento da impressão digital, devido para o fato com as associações forenses que podem ser feitas.

10 Apesar disto, cada dedo é referido possuir uma impressão digital única, **dois** dos padrões principais são detectados em **98 %** de todas as observações, um fato que aumenta o risco de se cometer erros. Hoje em dia, o exame visual tradicional foi substituído por automação. Existem 15 erros quando se vem a identificar uma pessoa desconhecida somente possuindo a impressão digital. Mas, quando se vem a verificar uma identidade de pessoa em uma base de dados delimitada, este é um método muito confiável.

20 **ESCANAMENTO DE ÍRIS**

O principio para este método foi formulado em **1.936**; ainda que este não tenha sido aplicado até os anos **1.990**. Todas os biométricos de íris comerciais que existem hoje em dia derivam a partir de algoritmos feitos pelo professor 25 *John Daugman* em **1.994**.

Um *scanner* de íris tira uma fotografia do olho utilizando uma câmara digital convencional. A imagem é usualmente de cerca de **120 pixels** em raio e o resultado é usualmente uma imagem de **8 bits** de uma íris. Quando a 30 fotografia é adquirida, a primeira etapa no processo de

criação de gabarito é localizar a pupila e a íris. Depois do que, o anel que ocorre quando a pupila é cortada a partir da imagem é transformada para um disco utilizando uma transformação polar. O programa de análise após isso
5 utiliza um número de algoritmos para criar um gabarito fundamentado sobre as diferentes características (Ver **Figura 6**).

Detecção de vitalidade pode ser implementada por se permitir em luz visível no olho e detectar se o tamanho da
10 pupila muda ou não. O que requer tanto uma fonte de luz suficientemente forte, ou quanto que a pessoa se coloque muito próxima para o scanner. Esta detecção de vitalidade não irá, conseqüentemente, ser adicionalmente apresentada na medida em que ela não deveria ser adequada em um
15 caminhão e, conseqüentemente, está fora do enfoque para este pedido de patente.

Existem mais do que **266** características independentes na íris. A íris é única não somente para cada pessoa, mas também para cada olho. Usualmente, cerca de **170** das **266**
20 características são utilizadas para formar o gabarito para comparação. Outros métodos de verificação biométrica somente utilizam cerca de **15** até no máximo **35** características significativas independentes para a análise. Por conseqüência, como existem tantas e excessivas
25 características no gabarito de íris, o método é muito confiável para verificação. Características físicas, como nossa aparência de rosto e nossa voz, mudam ao longo do tempo, mas a íris é, desconsiderando-se algumas flutuações de cor na juventude, invariável ao longo da integridade de
30 nosso tempo de vida. Isto é uma grande vantagem, na medida

em que a atualização consumidora de tempo da base de dados não irá ser requerida (Ver **Figura 7**).

Uma evidência da confiabilidade dos métodos é o sistema de reconhecimento de íris dos Emirados Árabes Unidos para prevenir que estrangeiros expulsos venham a re-entrar no país. Cerca de **600** pessoas estão sendo escaneadas a cada dia e hoje em dia a base de dados consiste de mais do que **355.000** íris. Mais de **1.600.000** pesquisas (buscas) foram feitas até agora e não foi detectado nenhum único emparelhamento falso. Análises estatísticas do programa sugerem que a probabilidade de um emparelhamento falso é menor do que **1** para **80 bilhões**.

A taxa de protocolo (registro) é muito boa; toda as íris podem ser analisadas, exceto aquelas de alguma pessoa visualmente prejudicada. Paralelamente, existem aplicações que capturam automaticamente uma imagem da íris a partir de distâncias acima de **três** pés, portanto, tornando o processo menos intrusivo.

Alguns sistemas, entretanto, possuem problemas escaneando pessoas com olhos muito escuros. Além do mais, lentes coloridas ou bifocais podem ser problemáticas, bem como óculos fortes (de lentes grossas).

Uma desvantagem com escaneamento de íris é a de que todo equipamento é manufaturado sob licença da *Iridian Technologies Inc.* Esta licença torna o equipamento e, por conseqüência, o método como um todo, dispendiosos. Em adição, se o método foi implementado em um veículo, as diversas condições de iluminação deveriam presumidamente provocar problemas. Se o coupê é excessivamente escuro um escaneamento apropriado deveria ser impossível,

identicamente se luz solar direta é deixada entrar na
câmera. O problema de luz solar pode ser resolvido se a
câmera for montada no espelho retrovisor traseiro,
protegendo esta da luz solar direta. Isto poderia também
5 aumentar as possibilidades para utilizar o *scanner* enquanto
dirigindo, na medida em que o motorista deveria olhar para
o espelho regularmente. Entretanto, esta solução é mais
adequada para carros de passageiros, na medida em que
caminhões não possuem espelhos retrovisores traseiros no
10 interior do coupê. Esta solução é, conseqüentemente, não
aplicável dentro dos limites deste pedido de patente.

RECONHECIMENTO DE VOZ

Este método identifica pessoas fundamentado sobre as
15 diferenças em suas vozes. O sujeito fala uma sentença pré-
definida em um microfone; o sistema captura a amostra de
voz e cria um gabarito fundamentado sobre, por exemplo,
entonação, cadência e/ou tom. O procedimento é o mesmo para
a verificação. O sujeito diz a sentença pré-definida no
20 microfone e o sistema extrai um gabarito para comparar com
os gabaritos armazenados na base de dados. Uma vantagem com
a utilização de reconhecimento de voz é a de que é difícil
o engano sem necessitar equipamento de gravação de alta
definição (*high-end*)/de *play-back*. Isto na medida em que o
25 sistema de reconhecimento de voz pode utilizar um microfone
que captura freqüências não graváveis com, por exemplo, um
ditafone. Mesmo se a senha devesse ser registrada
satisfatoriamente para enganar o sistema, a sentença falada
poderia ser alterada tornando a cópia não autorizada
30 inútil. Adicionalmente, um sistema de *play-back* sofisticado

deveria ser requerido de maneira a reproduzir todas as frequências de uma maneira apropriada. A demanda para equipamento de alta definição pode ser vista como um tipo de detecção de vitalidade.

5 Uma desvantagem com reconhecimento de voz é a de que gabaritos de voz ocupam mais espaço de armazenamento do que outras espécies de informação biométrica. Conseqüentemente, a verificação de voz poderia ocupar tempo mais longo do que outros métodos, devido para o fato da quantidade maior de
10 dados para analisar. Isto pode ser perturbador para o usuário, na medida em que ele deveria ter que esperar para a verificação. Um outro problema é o de que saúde, estado emocional, fadiga e envelhecimento são fatores que afetam as características de voz da pessoa. Por conseqüência,
15 verificação de voz não deveria ser relevante (confiável) como o método de verificação único para autorização.

RECONHECIMENTO DE ROSTO

Um método, que tem recentemente recobrado a atenção, é
20 reconhecimento de rosto. *Alphonse Bertillon* na polícia de Paris formulou o primeiro modelo para identificação visual em **1.883**. Seu sistema foi chamado Antropometria e foi descoberto sob diversas mensurações anatômicas complicadas do tamanho da cabeça, do comprimento de um dedo, da altura
25 do rosto e características especiais como a cor dos olhos, cicatrizes e a cor do cabelo. Este método não era confiável e foi em pouco tempo substituído pelas impressões digitais. Testes com câmeras de vigilância têm recentemente sido realizados na Grã Bretanha de maneira a identificar
30 criminosos. Estes testes têm mostrado que é muito difícil

identificar pessoas desta maneira, especialmente se a
câmera não conseguir uma boa tomada (uma foto limpa); ou se
a pessoa tiver alterado seus atributos com, por exemplo,
uma barba ou óculos. Apesar da falta de resultados
5 confiáveis para identificação, o método funciona
satisfatoriamente para propósitos de verificação.

O princípio é simples e similar para as análises
utilizadas para os métodos de verificação anteriormente
descritos. Uma imagem do rosto do sujeito é capturada e
10 analisada com um computador para encontrar características
proeminentes tais como as linhas de contorno das cavidades
dos olhos ou cantos da boca. Os resultados a partir das
análises são armazenados em um gabarito. Quando tentando
verificar uma pessoa, uma imagem é capturada e um gabarito
15 é criado fundamentado sobre a nova imagem. O novo gabarito
é emparelhado contra aquele armazenado na base de dados.
Um **PC** padrão (*standard*) de hoje em dia pode comparar um
gabarito com milhares de gabaritos em uma base de dados em
menos do que um segundo.

20 Existem diversas técnicas para extrair características
significativas a partir de uma imagem, tais como filtragem
de *Gabor* ou *eigenfaces* (visões computacionais e padrões de
reconhecimento para o reconhecimento automático de rostos
humanos). Estas técnicas são razoavelmente complicadas e na
25 medida em que isto não é essencial para o propósito deste
pedido de patente para serem descritas em detalhes, o
leitor interessado é direcionado para referências
conhecidas no estado da técnica para informação adicional.

Uma vantagem com reconhecimento de rosto é a de que
30 pessoas tendem a considerar este método confortável na

medida em que este estuda um rosto de pessoa, o que é a
mesma maneira como nós humanos fazemos quando identificando
um ao outro. Para conseguir resultados mais precisos,
reconhecimento de rosto pode ser utilizado em conjunção
5 com, por exemplo, movimentação labial e reconhecimento de
voz. Pesquisas têm sido feitas, tentando reforçar
(aperfeiçoar) os algoritmos para verificação de rosto para
conseguir robustez contra envelhecimento, condições de
iluminação ou expressão de rosto.

10 Hoje em dia, entretanto, não existe nenhuma solução
absoluta e a base de dados deveria necessitar ser
continuamente atualizada.

Uma decisão importante a se tomar quando considerando
reconhecimento de rosto é a de que tipo de câmera escolher;
15 uma câmera digital convencional ou uma infravermelha?
Quando a câmera utiliza o infravermelho, o método é chamado
Termografia de rosto (ver a seção a seguir).

TERMOGRAFIA DE ROSTO

20 Termografia de rosto é uma espécie (um tipo) especial
de reconhecimento de rosto. Com a utilização de uma câmera
de infravermelho um padrão de calor, encontrado sobre um
padrão de vaso sanguíneo de rosto da pessoa, pode ser
observado. Este padrão é único para cada pessoa e é difícil
25 de ser forjado (adulterado) (Ver **Figura 8**).

Uma câmera de infravermelho funciona aproximadamente
da mesma maneira como uma câmera convencional, a diferença
é a de que ela é sensível para luz infravermelha que é
radiação eletromagnética no intervalo de grosseiramente **760**
30 **nm - 0,5 nm**. Isto torna a luz infravermelha invisível para

o olho humano. Observe-se que a luz visível também é uma forma de radiação eletromagnética, mas de um diferente comprimento de onda do que o da luz infravermelha. Luz infravermelha é algumas vezes referida como radiação de calor e é enviada por todos os objetos com uma temperatura acima do zero absoluto. Por conseqüência, a câmera fotografa uma imagem de temperatura do objeto. Na medida em que diferentes partes do rosto possuem diferentes temperaturas, devido para a configuração do rosto e variações no fluxo sanguíneo, isto pode ser utilizado para verificação.

Ainda que termografia de rosto analisa um padrão de calor de rosto da pessoa, não faz qualquer diferença significativa se o sujeito estiver descansado, se exercitando ou do lado de fora no frio. Estudos mostram que câmeras de **IR** são razoavelmente insensíveis para estas circunstâncias. Uma outra vantagem é a de que o escaneamento é independente de condições de luz visual na medida em que a câmera opera no intervalo de comprimento de onda infravermelho e, conseqüentemente, é "cega" para luz visível.

Comparações entre utilização de câmeras regulares versus câmeras de **IR** para verificação de rosto têm sido feitas, a maior parte das vezes freqüentemente benéficas para as câmeras de **IR** na medida em que elas são independentes das condições de iluminação. Entretanto, um problema com as câmeras de **IR** é o de que óculos de todos os tipos são completamente opacos para ela. Isto significa que a área em torno dos olhos pode provocar problemas se uma pessoa utiliza óculos, ou se a pessoa usualmente utiliza

óculos e os tira depois, sem atualização da base de dados.

ESCANEAMENTO DE RETINA

Reconhecimento de retina foi formulado nos anos de
5 **1.930**, mas a tecnologia não foi desenvolvida o suficiente
para tornar o método comercialmente viável até os anos de
1.980. Escaneamento de retina é um método rápido e muito
exato que utiliza *laser* para analisar o padrão de vaso
sanguíneo da retina. Quando a fotografia da retina é
10 tirada, o sistema usualmente armazena um gabarito
fundamentado sobre as características extraídas a partir da
imagem, similarmente com métodos anteriormente mencionados
(Ver **Figura 9**).

Escaneamento de retina é considerado o método de
15 verificação biométrico o mais preciso na medida em que o
padrão de vaso sanguíneo é único para cada pessoa e não
muda ao longo do tempo. A vascularidade de retina
desaparece dentro de segundos se o sujeito deixa de viver
(morre), portanto, assegurando que a imagem capturada foi
20 obtida a partir de um ser humano que está vivo. Um estudo
mostrou que, ainda que a retina não seja fácil de escanear,
o tempo necessário para registrar a retina foi menor do que
o tempo requerido para registro de uma impressão digital
(veja **Figura 10**).

25

A câmera tem que possuir alta resolução e o método
demanda alinhamento preciso do olho para se ter a
capacidade de escanear. Captação de imagem pode ser feita a
partir de uma distância acima de **três** pés. Isto é,
30 entretanto, de incerteza sob que condições ambientais estas

qualidades são válidas.

RECONHECIMENTO DE MOVIMENTAÇÃO LABIAL

A maneira como as pessoas movimentam seus lábios enquanto falam difere de pessoa para pessoa, conseqüentemente, um método para reconhecimento de movimentação labial foi desenvolvido. Enquanto uma pessoa fala, uma câmera é utilizada para capturar um número de fotografias (em secessão rápida), da boca e da área circundante. Um computador é utilizado para analisar a movimentação de minúsculas rugas na área em torno da boca. Estas movimentações são representadas por um campo de vetor colocado sobre a fotografia. O campo de vetor é após isso comparado com campos de vetor na base de dados, em analogia com métodos precedentemente estabelecidos. O equipamento utilizado é fundamentalmente o mesmo como aquele para reconhecimento de rosto.

Reconhecimento de movimentação labial não é preciso o suficiente para servir como método de verificação único. É, conseqüentemente, sugerido que venha a ser utilizado em conjunção com, por exemplo, reconhecimento de voz.

Um caso especial de reconhecimento labial é chamado de reconhecimento de sorriso. As movimentações de músculos na parte inferior do rosto, ativadas enquanto sorrindo, são diferentes de pessoa para pessoa. Estes músculos são quase que impossíveis de serem controlados pela vontade e eles são visíveis mesmo se o sujeito tenta manter uma expressão de rosto (facial), como mantendo a si mesmo impedido de dar risada. Na medida em que não existem sistemas funcionais no mercado, eles não irão ser discutidos de qualquer maneira

adicionalmente.

RECONHECIMENTO DE GEOMETRIA DE MÃO

Um *scanner* de geometria de mão mensura comprimento,
5 profundidade, largura, espessura e curvatura dos dedos. O sistema consiste de uma superfície plana com um número de pinos, uma fonte de luz, um espelho e uma câmera.

A mão é colocada sobre a superfície plana, com a palma voltada para baixo e os dedos guiados pelos pinos. O
10 espelho é utilizado para projetar a lateral da mão para a câmera e as fotografias recuperadas são analisadas (Ver **Figura 11**).

Diferentemente de, por exemplo, impressões digitais, as mãos da pessoa não são únicas. Conseqüentemente, este
15 método não pode ser utilizado para propósitos de identificação, mas simplesmente de verificação. Em concordância com *Lichtermann* e outros, reconhecimento de geometria de mão não é adequado para propósitos automotivos, devido para o fato de que o equipamento é
20 desajeitado. Na medida em que o artigo foi escrito em **2.000**, é razoável de se acreditar que **cinco** anos de desenvolvimento poderiam ter diminuído o tamanho do equipamento. Entretanto, sistemas de geometria de mão ainda necessitam de aproximadamente **nove** polegadas entre a câmera
25 e a mão de maneira a recuperar uma imagem, adequada para a análise. Isto é excessivo para tornar o equipamento adequado para montagem embarcada em caminhão.

TRAÇOS CARACTERÍSTICOS BIOMÉTRICOS LEVES

30 Traços característicos (feições características)

biométricos leves ou particularidades biométricas leves são, por exemplo, idade, sexo (gênero), altura, peso, etnia, e cor de cabelo e de olho. Estes biométricos são vagos e imprecisos e diversos deles depois mudam através da vida, eles são também mais fáceis de forjar do que, por exemplo, impressões digitais. Biométricos leves não podem, conseqüentemente, ser utilizados para identificação ou verificação seguras. Entretanto, biométricos leves podem ser utilizados como um complemento para outros métodos biométricos. Um controle de peso poderia ser implementado em um veículo como um complemento para escaneamento de impressão digital.

OUTROS MÉTODOS PARA VERIFICAÇÃO

Pessoas tiveram a capacidade para identificar outros humanos utilizando características biométricas por um longo período de tempo, mas as maneiras as mais comuns para confirmar identidade atualmente são, pelos cartões, *transponders*, senhas e **PINs** (*Personal Identification Number* - Número de Identificação Pessoal). A maior parte das pessoas é utilizada para estes métodos de verificação, mas para auxiliar comparação dos diferentes métodos de verificação, uma breve descrição de cada método irá ser determinada.

25

SENHAS E PINs

Senhas e **PINs** não necessitam de muita introdução. Presumivelmente todas as pessoas lendo o presente pedido de patente já utilizaram ambos os métodos enquanto, por exemplo, acessando seus computadores, sacando dinheiro a

30

partir de um **ATM** (**ATM** - *Asynchronous Transfer Mode* - Modo de Transferência Assíncrono) ou iniciando (ligando) seu telefone celular.

A maior vantagem é a de que o sistema é completamente
5 simples. Um teclado e um computador são tudo o que é necessário. Outras vantagens são as de que é fácil de se utilizar, pessoas são utilizadas para isto e não consideram este sistema intrusivo.

As desvantagens são as de que códigos e senhas podem
10 ser facilmente copiados, roubados ou esquecidos. Pessoas também tendem a possuir senhas que são relativamente simples de adivinhar, tal como o nome de seu cachorro ou a idade de suas crianças. Isto poderia tornar fácil para um impostor imaginar (descobrir) a senha efetiva e por
15 intermédio disto passar na verificação.

CARTÕES

Existem diversos tipos de cartões para propósitos de identificação/verificação. A diferença entre eles é como o
20 cartão é utilizado no processo de verificação.

Licenças (habilitações) de motorista e outros cartões de identificação (**ID**) demandam que alguém faça a comparação (o emparelhamento) visualmente entre a foto e a pessoa efetiva.

25 Cartões de acesso possuem uma faixa magnética para armazenar informação, e alguns tipos utilizam um **PIN** para verificar que a pessoa possuindo o cartão é o legítimo proprietário. A faixa magnética é lida pelo **ATM**, terminal de acesso ou caixa registradora.

30 Um cartão inteligente é fundamentalmente um computador

simples de tamanho de cartão de crédito. Ele possui um microprocessador e uma memória embutidos no cartão. Estes cartões são mais versáteis do que um cartão de crédito regular, na medida em que muito mais informação pode ser armazenada na memória no cartão inteligente do que sobre a faixa magnética. É comum utilizar um **PIN** para verificar que o portador de cartão é o legítimo proprietário. Entretanto, o microprocessador no cartão inteligente proporciona possibilidades para implementar métodos mais sofisticados, tal como o **Matc- On-Card™**, tecnologia desenvolvida pela *Precise Biometrics*. Esta tecnologia implica que o emparelhamento efetivo seja feito pelo computador no cartão inteligente ao invés de ser por um computador externo o que é o procedimento normal.

15

IDENTIFICAÇÃO DE RÁDIO FREQUÊNCIA (RFID)

RFID é um método de armazenamento e de recuperação de dados remotamente utilizando dispositivos chamados etiquetas (*tags*) **RFID**. Estas etiquetas são tanto ativas ou quanto passivas. A diferença entre elas é a de que uma etiqueta passiva não possui qualquer suprimento de energia. Ao invés disto, ela recupera energia por indução magnética a partir do dispositivo leitor. Isto significa que uma etiqueta passiva tem que ser sustentada próxima ao leitor durante a leitura efetiva, enquanto que uma etiqueta ativa pode ser lida a partir de diversos metros. Uma etiqueta passiva pode, devido para sua falta de suprimento de energia, ser feita menor do que uma etiqueta ativa. As etiquetas passivas as menores são de cerca de **0,4 milímetro** quadrado e tão finas quanto um adesivo, enquanto as

30

etiquetas ativas as menores são grosseiramente do tamanho de uma moeda.

Etiquetas **RFID** podem ser utilizadas para propósitos de verificação no mesmo estilo como cartões. A diferença primordial é a de que é meramente requerido para suportar a
5 etiqueta contra o *scanner* (etiqueta passiva) ou carregá-la suficientemente próxima do *scanner* (etiqueta ativa) de maneira a fazer a verificação.

10 **SISTEMAS DE VERIFICAÇÃO DE MODO MÚLTIPLO (MULTIMODAL)**

Um sistema de verificação biométrico de modo múltiplo (multimodal) consiste de **dois** ou mais métodos de verificação biométricos funcionando em conjunção. Um sistema meramente utilizando um método chamado é chamado de
15 modo único (unimodal). Na medida em que eles utilizam diversos métodos ao mesmo tempo, sistemas de modo múltiplo são evidentemente mais dispendiosos, mas, como estabelecido posteriormente, existem vantagens utilizando mais do que um método de verificação.

20 Aqui segue um exemplo inventado para melhor explanação de como os sistemas de modo múltiplo funcionam. Uma maneira de se entender um sistema de modo múltiplo poderia ser imaginar um sistema consistindo de **dois** dos métodos de verificação biométricos precedentemente mencionados, por
25 exemplo, impressões digitais e escaneamento de íris. O que deveria determinar a possibilidade de se escolher entre **três** configurações.

O sujeito pode escolher um método que é o mais apropriado no momento, devido para fatores ambientais ou
30 outros. Por exemplo, se as mãos do motorista estão sujas,

escanear a íris, se está escuro no coupê, escanear a impressão digital.

O sujeito utiliza ambos os métodos independentemente um do outro e o sistema avalia ambos os resultados para 5 tomar a decisão. Esta configuração foi empiricamente provada de ter capacidade para reduzir a Taxa de Rejeição Falsa (*False Rejection Rate - FRR*) sem aumentar a Taxa de Aceitação Falsa (*False Acceptance Rate - FAR*). Se o emparelhamento para um dos métodos de verificação não é 10 satisfatório, mas o outro método proporciona um emparelhamento válido, o sujeito pode ainda passar na verificação.

O sistema demanda que o sujeito passe em ambos os métodos, independentemente um do outro. Isto aumenta o 15 nível de segurança (proteção) na medida em que é mais difícil enganar **dois** métodos do que um. Uma desvantagem é a de que estes sistemas tendem a possuir muito alta Taxa de Rejeição Falsa.

Quando utilizando sistemas de modo múltiplo, tanto 20 segurança ou quanto conveniência podem ser aperfeiçoadas, porém não ambos ao mesmo tempo. Uma desvantagem com sistemas de modo múltiplo é a de que a verificação consiste de diversas tarefas e, portanto, toma um período de tempo mais longo, o que pode ser inconveniente para o usuário.

25 **SISTEMAS BIOMÉTRICOS MÚLTIPLOS**

Os sistemas de modo múltiplo descritos na seção precedente são um caso especial dos assim chamados sistemas múltiplos. Eles utilizam diversas mensurações, mas não necessariamente diferentes métodos.

30 Existem basicamente **cinco** tipos de sistemas de

verificação múltiplos:

5 **Emparelhador múltiplo:** Um sistema de emparelhamento múltiplo analisa um escaneamento de **duas** ou mais diferentes maneiras ou com **dois** diferentes algoritmos, por exemplo, (utilizando escaneamento de impressão digital) minúcias e não minúcias fundamentadas em emparelhamentos.

10 **Sensor múltiplo:** Um sistema é chamado sistema de sensor múltiplo quando **dois** ou mais diferentes sensores são utilizados para escanear o mesmo objeto.

15 **Modo múltiplo:** Sistemas de modo múltiplo utilizam **dois** ou mais diferentes métodos, por exemplo, reconhecimento de voz e rosto.

20 **Unidade múltipla:** Um sistema de unidade múltipla escaneia **duas** ou mais unidades da mesma propriedade, por exemplo, dedo indicador e médio ou tanto o olho direito e quanto o esquerdo.

25 **Impressão múltipla:** Sistemas de impressão múltipla escaneiam a mesma propriedade um número de vezes; por exemplo, demandando o sujeito a falar sua senha **três** vezes para um sistema de verificação de voz.

30

Todos estes sistemas possuem suas vantagens e desvantagens óbvias. Na medida em que foi precedentemente decidido implementar **três** métodos enfoque irá ser sobre um sistema de modo múltiplo, os outros métodos múltiplos não irão ser, conseqüentemente, adicionalmente explanados.

TRABALHO PREPARATÓRIO

Devido para os **dois** propósitos aqui colocados, diversos diferentes métodos de trabalho foram utilizados e, por conseqüência, diversos espécies de resultados foram conseguidas. Nesta seção, método e resultados são entrelaçados juntamente de maneira a proporcionar ao leitor uma fotografia do processo de trabalho. Cada etapa está descrita separadamente seguida por seu resultado. Isto é suposto proporcionar uma visão mais clara de quais decisões que foram feitas nas diversas etapas através de todo o processo e como o trabalho prosseguiu fundamentado sobre aquelas decisões.

20

ESTUDO DE PESQUISA

Para avaliar nas opiniões dos motoristas na escolha de métodos para implementar, uma pesquisa de motorista foi feita em um estágio antecedente (inicial).

25

AS DUAS DIFERENTES PESQUISAS

A pesquisa foi dividida em **dois** documentos chamados de pesquisa de atitude e a pesquisa de método, respectivamente. O primeiro questionou, por exemplo, sobre rotinas no trabalho, conhecimento sobre métodos biométricos e sentimentos de proteção e segurança no trabalho. O último

30

deu uma explanação curta de cada método biométrico descrito na seção **2**. Os que responderam foram questionados para proporcionar comentários espontâneos para cada método. Algumas das questões questionaram os que responderam para graduar as respostas entre **1** e **5**, onde **1** foi sempre a resposta mais negativa e **5** a resposta positiva; enquanto que algumas questões somente questionaram para respostas mais refletidas. Todas as questões tiveram espaço deixado para reflexões e comentários.

10 A razão para fazer **dois** diferentes documentos foi para prevenir que os que responderam viessem a espiar as questões seguintes e, conseqüentemente, pudessem ser influenciados pelos fatos nas descrições dos diferentes métodos de verificação. Na medida em que a pesquisa foi dividida em **duas** partes, os motoristas foram forçados a responder a primeira parte antes que eles tivessem recebido a próxima parte.

A pesquisa foi distribuída de **duas** maneiras. Os primeiros a determinar suas opiniões foram motoristas de caminhão que tinham parado para uma pausa em uma parada de caminhões, exatamente fora de *Gothenburg*. Numerosos motoristas foram questionados para preencher a pesquisa, mas somente **12** concordaram em assim fazer. Como gratidão os que responderam receberam doces de confeitaria.

25 Posteriormente uma companhia de transporte em *Gothenburg* concordou em distribuir a pesquisa entre seus motoristas. Experiências antecedentes mostraram que não iriam existir assim tantas respostas quanto como as pesquisas distribuídas, e conseqüentemente, **25** pesquisas foram proporcionadas para a companhia de transporte, com a

30

esperança de recuperação de pelo menos metade delas dentro do período de tempo limitado de uma semana. **Dez** pesquisas foram respondidas e retornaram em tempo.

Existia tanto uma versão em sueco e quanto uma versão em inglês da pesquisa, de maneira que todos os motoristas devessem estar habilitados para responder às questões a despeito de se eles conhecessem sueco ou não. Isto foi importante na parada de caminhões local na medida em que muitos dos motoristas ali somente falavam muito pouco ou quase nada de sueco. Todas as pesquisas distribuídas na companhia de transporte foram escritas em sueco.

RESULTADOS A PARTIR DA PESQUISA DE ATITUDE

Onze dos que responderam trabalhavam com distribuição, **dez** dirigiam transportes de longa distância e um dirigiu tanto transporte de longa distância e quanto de distribuição. **Doze** dos motoristas foram os únicos dirigindo seus caminhões particulares, os outros compartilhavam seus caminhões com **cinco** outros motoristas em média. Eles já trabalhavam por **15** anos em média, variando a partir de **um** ano de idade até **38** anos de idade.

Oito motoristas conheciam métodos biométricos, como exemplo, eles todos conheciam verificação de impressão digital. Enquanto que esta foi a única resposta para alguns, outros poderiam mencionar diversos outros métodos como tais. Somente **um** motorista tinha sempre utilizado um método de verificação biométrica. **Nove** dos motoristas que não possuíam experiências de biométricos foram receptivos para a idéia de utilizá-los para verificação, **quatro** foram mais restritivos ou contra a integridade da idéia, e os

oito remanescentes foram nem positivos e nem negativos. O resultado médio foi de **3,6**.

Oito motoristas puderam ver desvantagens com um sistema de verificação biométrica enquanto que **onze** não puderam. **Três** motoristas não responderam à questão. Vantagens por outro lado, foram visíveis para **15** motoristas, enquanto que **cinco** não puderam ver qualquer vantagem e **dois** não responderam à questão. Sobre a questão de onde os dados biométricos deveriam ser mantidos, **15** dos motoristas responderam que eles iriam preferir que estes fossem mantidos em um cartão inteligente que eles podem estar de posse quando eles deixassem o veículo. **Cinco** acreditam que o armazenamento devesse ser mantido na companhia de transporte e **dois** desejavam estes no veículo. Observe-se que alguns motoristas escolheram mais do que uma opção e **três** não responderam a tudo.

RESULTADOS A PARTIR DA PESQUISA DE MÉTODO

Verificação de impressão digital foi de longe o método o mais apreciado; todo mundo acreditou que isto deveria ser o mais não dispendioso e o mais fácil para se utilizar. Mesmo aqueles que não desejavam métodos de verificação biométricos no veículo preferiram impressões digitais. Ainda, **quatro** motoristas ficaram preocupados que mãos sujas deveriam provocar problemas. **Dois** que responderam imaginaram cenários onde eles perderam seus dedos ou foram seqüestrados para dar partida ao veículo, mas ainda que eles pudessem ver estas desvantagens, eles poderiam ainda ver vantagens também. Paralelamente, quando questionados sobre os outros métodos, os motoristas algumas vezes

responderam que eles preferiam utilizar a impressão digital (de mais preferência do que o método em questão).

Levando-se em consideração os outros métodos, a mistura de respostas positivas e negativas tornou difícil
5 extrair quaisquer conclusões se o método era adequado ou não. De mérito é mencionar, na medida em que **seis** dos motoristas comentaram isto, é que eles foram céticos para a verificação de voz na medida em que é muito comum que um motorista trabalhe mesmo se ele tem um resfriado ou uma
10 inflamação de garganta. **Dois** tiveram experiências ruins a partir de tecnologia de reconhecimento de voz e foram, por consequência, céticos para utilizar verificação de voz.

15 **ENTREVISTA POR TELEFONE COM CONTRATADORES DE TRANSPORTE**

Um sistema de verificação como este aqui deveria não somente ser importante para os motoristas, mas também para os diferentes contratadores de transporte. Para se ter uma idéia acerca das diversas demandas a partir dos
20 contratadores de transporte, um número de entrevistas telefônicas foram realizadas.

COMO AS ENTREVISTAS TELEFÔNICAS FORAM REALIZADAS

25 **Dez** escritórios escolhidos ao acaso em *Gothenburg* foram questionados para serem entrevistados através do telefone. **Três** deles foram entrevistados e um **quarto** recebeu a pesquisa como um *e-mail*, o respondendo e retornando da mesma maneira. As questões foram quase as
30 mesmas como para as pesquisas de motorista, somente que

elas foram agora questionados verbalmente ao invés disso, e ligeiramente ajustadas para se adaptarem especialmente às companhias antes do que aos motoristas. As questões foram lidas em alta voz para o informante e explanadas se necessário. As respostas foram escritas pelo entrevistador.

Foi difícil de se buscar a pessoa correta para entrevistar e mesmo quando isto se sucedeu foi difícil encontrar alguém que tivesse tempo para responder as questões. Na medida em que as respostas foram totalmente similares, elas ainda proporcionaram uma sugestão sobre o que as companhias consideram como importante. Observe-se que devido para o baixo número de informantes, as respostas não são sempre especificadas em números exatos.

15 **RESULTADOS A PARTIR DA ENTREVISTA TELEFÔNICA COM CONTRATADORES DE TRANSPORTE**

As condições de trabalho dentro dos **quatro** escritórios entrevistados variaram, por exemplo, tanto transportes de longa distância e quanto de distribuição estavam representados, bem como cargas perigosas e de alto valor. O tamanho da companhia diferiu a partir de **oito** motoristas até **76**. Somente uma das companhias utilizou pessoal externo em caso de enfermidade ou outra ausência inesperada.

As respostas foram primordialmente positivas e as companhias pareciam saber mais sobre diferentes métodos de verificação do que os motoristas pareciam saber na pesquisa. A demanda primordial foi a de que eles não têm que ser dispendiosos, eles enfatizaram que eles precisam de alta segurança a baixo custo. O maior dos receios foi o de que se os motoristas se arriscam a perder um olho ou um

dedo, conseqüentemente, isto deveria obviamente não
desmerecer o método. O pior ceticismo foi contra a
tecnologia. "E se isto falhar?" foi um questionamento
comum. A maior parte deles poderia também ver problemas se
5 alguma coisa acontece para o motorista, um acidente, ou
alguma outra coisa, que incapacite o motorista a movimentar
o veículo. "Tem que existir uma maneira de movimentar o
veículo de qualquer forma".

Verificação por impressões digitais foi o método o
10 mais apreciado na medida em que todas as companhias foram
positivas a este. **Duas** pessoas foram severamente contra
métodos que analisam o olho. Uma terceira comentou que
deveria ser melhor com verificação de impressão digital
porque isto é menos dispendioso. Ninguém acreditou em um
15 sistema utilizando reconhecimento de voz com a
justificativa de que é comum que os motoristas vão
trabalhar até mesmo se eles estão enfermos ou roucos.
Reconhecimento de rosto foi acreditado ser mais dispendioso
do que verificação de impressão digital e foi suspeito por
20 não manipular ganho de peso ou a mesma pessoa com ou sem
uma barda. Nenhum dos outros métodos ganhou qualquer
otimismo. Geometria de mão, por exemplo, foi acreditada ser
desnecessária na medida em que foi percebido não ser tão
confiável quanto verificação de impressão digital. Também
25 deveria aumentar o risco de se perder uma mão inteira ao
invés de "somente um dedo".

Diversos dos informantes não sentiram que suas
companhias estão em necessidade de uma tal alta segurança.
Ao invés disso, eles apontaram a necessidade de
30 dispositivos de interbloqueio de álcool. Se eles ainda

tinham que escolher alguma coisa eles deveriam ir para
verificação de impressão digital. Uma das pessoas foi mais
positiva para a idéia total do que as outras e uma foi mais
negativa. De chamar atenção é que uma foi a mais negativa
5 para os métodos biométricos para verificação gostando da
idéia da assim chamada identificação de estilo de
motorista. Os veículos de hoje em dia podem monitorar e
armazenar uma quantidade de informação, por exemplo,
duração da jornada, consumo de combustível, mudanças de
10 marcha e técnica de frenagem. Por observação desta
informação, pode ser possível observar um estilo de direção
do motorista. Isto não deveria ser suficiente para
verificar uma pessoa, mas se o padrão mudou drasticamente
poderia ser assumido que alguma outra pessoa tomou o
15 veículo. O informante que gostou da idéia da identificação
de estilo do motorista sugeriu que isto deveria ser
integrado com detecção de sonolência e detecção para saber
se o motorista tiver tomado quaisquer drogas ou outras
substâncias.

20 Mesmo que as companhias não sentiram como se elas
necessitassem de um sistema de verificação no momento, eles
perceberam isto como positivo se isto fosse dificultar mais
para o furto de seus veículos.

25 **REFLEXÕES ACERCA DE COMO OS MÉTODOS SE ADEQUAM AO
PROPÓSITO**

Existem diversos diferentes métodos de verificação no
mercado atualmente; ainda não existe nenhum método perfeito
para o propósito deste pedido de patente. O estudo de
30 teoria conduz para reflexões e discussões acerca da

adequabilidade dos métodos em um contexto de caminhão. Todos os métodos têm seus prós e contras, mas não foi possível testar todos eles. Por conseqüência, foi importante teoricamente avaliar os diferentes métodos um
5 contra o outro para se ter a capacidade de escolher quais aqueles se implementar no protótipo de teste. Esta seção descreve os resultados a partir das discussões e comparações teóricas.

10 **O MÉTODO IDEAL**

As propriedades as mais desejáveis para o sistema de verificação foram listadas para proporcionar um panorama para a seleção de quais métodos implementar. Este critérios foram escolhidos na medida em que eles foram surgindo
15 durante discussões e observações refletidas levando-se em consideração como o sistema ideal deveria funcionar.

Fácil de utilizar: Nenhuma educação extensiva deveria ser necessária para operar o
20 equipamento. Deveria ser tão intuitivo quanto possível e tanto quanto possível deveria ser automatizado.

Velocidade: O processo de verificação não tem que demorar demais, uns poucos segundos no máximo. O protocolo deveria também ser rápida. Adicionalmente, o método não
25 deveria consistir excessivamente de muitas diferentes tarefas.
30

Flexibilidade: O sistema deveria ser construído para manipular diversos motoristas que deveriam mudar expedientes. Deveria ser possível verificar o motorista enquanto ele está dirigindo de maneira a evitar que um motorista verificado dê partida ao motor somente para ser arremessado para fora do veículo por um impostor.

Custo: O sistema não deve ser excessivamente dispendioso, de outro modo os proprietários de caminhão não irão considerar comprá-lo.

Aceitação de usuário: O sistema deveria ser não intrusivo. Ao lado disso, o usuário e o proprietário de caminhão tem que sentir que o sistema é significativo e benéfico para eles.

Proteção: O sistema tem que ser seguro contra ataques.

Precisão: O sistema deveria conseguir uma **TER** (*Total Error Rate - Taxa de Erro Total*) suficientemente baixa.

Adequabilidade: Os métodos do sistema tem que adaptar as diferentes propriedades de ambiente no veículo, tais como espaço, iluminação, temperatura, ruído, vibrações e umidade.

Integrabilidade: Equipamento que seja facilmente integrado para o veículo pode manter o custo baixo e tornar o sistema mais fácil de utilizar na

medida em que não iriam existir
excessivamente muitas novas
tarefas para controlar. O
equipamento necessitado não tem
que ser desajeitado, de outro modo
irá ser difícil para montá-lo no
veículo.

Confiabilidade:

O sistema não tem que cair ou
falhar nunca com a verificação, de
outro modo poderia ser incapaz de
prevenir que pessoas não
autorizadas viessem a dar partida
ao veículo. Isto pode provocar que
o motorista ou proprietário venha
a desconfiar do sistema. No mesmo
sentido, não tem que falhar nunca
em conceder acesso para o próprio
motorista.

NOÇÕES ACERCA DOS DIFERENTES MÉTODOS

Esta seção contém algumas anotações argumentando para,
ou contra, os diferentes métodos de verificação. As
seguintes questões e reflexões estão conectadas para os
critérios do sistema ideal descrito anteriormente. Estas
noções têm influenciado diversos aspectos do pedido de
patente.

**NOÇÕES LEVANDO-SE EM CONSIDERAÇÃO VERIFICAÇÃO DE
IMPRESSÃO DIGITAL**

Tecnologia de impressão digital está bem testada no

sentido de que ela foi utilizada e desenvolvida por um longo período de tempo. Os *scanners* podem ser feitos pequenos e não dispendiosos e o método é experimentado como não intrusivo pela maior parte das pessoas. Uma grande
5 variedade de marcas está disponível no mercado, o que garante boas oportunidades para encontrar um produto que se adapta aos requerimentos desejados.

Uma maneira de aumentar a proteção para um sistema de verificação deveria ser utilizar mais do que um dedo para a
10 verificação. Existem **duas** diferentes maneiras de fazer isto; tanto o sistema requer o escaneamento de um conjunto pré-definido de dedos, ou quanto o sistema randomicamente demanda qual dedo deve ser escaneado naquele tempo específico. Uma desvantagem com estas alternativas é
15 evidentemente a de que se um conjunto de impressões é demandado, um impostor poderia tentar furtar todas as impressões de uma pessoa. Neste caso, a proteção aumentada poderia ser ao custo da segurança do usuário.

Considerando-se mérito levando-se em consideração a
20 perspectiva automotiva, é que muitos motoristas trabalham muito com suas mãos, provocando que as mãos venham a adquirir sujeira ou desgaste, o que poderia afetar o resultado de escaneamento. Se o *scanner* em si mesmo vem a adquirir sujeira, o próprio escaneamento se torna difícil.
25 Isto poderia ser solucionado utilizando uma escovinha de *scanner* na medida em que ele não tende a se tornar sujo como um *scanner* de toque.

Irá existir sempre a possibilidade de pessoas não autorizadas tentarem enganar o sistema. Embora detecção de
30 vitalidade proteja contra cópias, ou o cenário horrível

quando o impostor furte o dedo completo (ou a mão), é impossível fazer um sistema absolutamente seguro. Drogas ou ameaças podem ser utilizadas para forçar o motorista autorizado a colocar seu dedo sobre o scanner. Para resumir, escaneamento de impressão digital é um método rápido, não dispendioso e não intrusivo que pode facilmente ser integrado no veículo.

NOÇÕES LEVANDO-SE EM CONSIDERAÇÃO ESCANEAMENTO DE ÍRIS

Escaneamento de íris é considerado ser um método de verificação preciso, confiável e seguro. Em concordância com a literatura existe agora um equipamento disponível que pode capturar uma imagem a partir de uma distância de aproximadamente **um metro** e ainda conseguir qualidade alta o suficiente para emparelhar a imagem contra o gabarito. Isto significa que poderia ser possível instalar uma câmera no coupê de uma maneira tal que a câmera não atrapalhe o motorista ou obscure sua visão. É, entretanto, duvidoso se estas aplicações são adequadas para veículos e ainda mais duvidoso se é possível escanear enquanto dirigindo, na medida em que nenhum teste foi realizado nesta área.

Escaneamento de íris é, por conseqüência, rápido e poderia ser não intrusivo, entretanto, a adequabilidade bem como a integrabilidade faltam para este método e o equipamento é dispendioso devido à licença de patente.

NOÇÕES LEVANDO-SE EM CONSIDERAÇÃO RECONHECIMENTO DE VOZ

Um sistema para verificação de voz pode facilmente ser integrado em um veículo, possivelmente utilizando

equipamento existente, tal como sistema de telefonia celular de mãos livres. Deveria ser possível utilizar verificação de voz enquanto dirigindo, pelo menos no sentido que a maior parte das pessoas têm a capacidade de

5 falar e dirigir ao mesmo tempo. Se o motorista utiliza o telefone celular ou outro sistema de comunicação verbal, a demanda de verificação poderia ser suprimida por uns poucos minutos. No caso quando o motorista ouve o aparelho de som, é sugerido que o som seja silenciado durante a verificação.

10 O coupê de um caminhão moderno é acusticamente isolado, que é digno de atenção quando acessando ao interior. Devido ao isolamento acústico, ruído de fundo a partir do motor, do vento e do tráfego ao redor é bastante constante. Poderia, conseqüentemente, ser possível utilizar

15 um filtro adaptativo para remover o ruído a partir da amostra de voz durante verificação. Mas, mesmo que a maior parte dos coupês dos caminhões seja bem isolada, os sistemas de verificação de voz são desenvolvidos para utilização em interiores de escritórios, por conseqüência,

20 é difícil referir se é adequado ou não sem testagem do sistema em um ambiente de veículo.

A desvantagem é a de que a base de dados irá continuamente necessitar de atualizações na medida em que uma voz e sotaque de pessoa mudam ao longo do tempo.

25 Adicionalmente, uma voz de pessoa pode mudar rapidamente devido para a saúde relacionada e a fatores emocionais. Estes aspectos provocaram desconfiança da tecnologia a algumas pessoas.

Na medida em que o enfoque deste pedido de patente é

30 verificar uma identidade de motorista, a utilização de uma

sentença de verificação pré-definida é sugerida. Se cada motorista possui uma única senha, tanto a sentença em si mesma e quanto a amostra de voz, podem ser utilizadas para verificação. Verificação de voz é, por conseqüência, um método não dispendioso, que pode facilmente ser implementado em um caminhão. Entretanto, devido ao ambiente ruidoso e ao fato de que a voz muda ao longo do tempo, é duvidoso se este método funciona suficientemente bem em situações reais.

10

NOÇÕES LEVANDO-SE EM CONSIDERAÇÃO RECONHECIMENTO DE ROSTO

Reconhecimento de rosto é sensível para condições de iluminação, mas este pode ser uma alternativa para utilizar antes de dar partida ao veículo na medida em que é possível adicionar mais iluminação ao coupê durante a verificação. Entretanto, não é recomendado assim proceder enquanto dirigindo, na medida em que isto pode ser perturbador para o motorista. As condições de luz mudam através de todo o dia, e é, conseqüentemente, duvidoso se reconhecimento de rosto pode ser utilizado enquanto dirigindo. Uma fotografia tirada durante período noturno poderia não ser similar o suficiente para a imagem armazenada para o sistema ser bem sucedido com a verificação. Diferentes condições de luz irão ser testadas aqui, na medida em que uma câmera no veículo proporciona muitas outras possibilidades como detecção de sonolência, vigilância de coupê, etc. Entretanto, estas possibilidades estão além do propósito deste pedido de patente, por conseqüência, elas não irão ser adicionalmente investigadas.

30

A parte consumidora de tempo de reconhecimento de rosto é a criação de gabarito. Durante verificação, o sistema poderia necessitar tirar **três** ou mais fotografias para assegurar que pelo menos uma delas está boa o suficiente. A criação de gabarito leva cerca de **3 segundos** - **5 segundos** o que significa que a integridade de processo de verificação irá levar cerca de **10 segundos - 15 segundos** o que é muito longo.

Um interessante efeito secundário é o fato de que a câmera utilizada efetivamente tira fotografias da pessoa intencionada a dirigir o veículo. Se um impostor dirige o veículo, a verificação irá falhar, mas fotografias são ainda tiradas e armazenadas. Estas fotografias podem após isso ser utilizadas quando tentando identificá-lo.

Resumindo, reconhecimento de rosto é um método amigável de usuário, não dispendioso e não intrusivo. Ainda mais, não foi possível encontrar qualquer pesquisa sobre reconhecimento de rosto em ambientes que se assemelham ao coupê de um veículo e é, conseqüentemente, duvidoso como o método se adapta bem ao propósito.

NOÇÕES LEVANDO-SE EM CONSIDERAÇÃO TERMOGRAFIA DE ROSTO

Uma idéia levando-se em consideração a utilização de reconhecimento de rosto é a de que poderia ser possível utilizá-lo para verificação automática enquanto dirigindo. Isto, entretanto, irá somente ser possível se o sistema não for excessivamente sensível para mudança de condições de luz. Como explanado anteriormente, termografia de rosto e reconhecimento de rosto são praticamente a mesma coisa; a diferença é qual o tipo de câmera que é utilizada.

Termografia de rosto utiliza uma câmera de **IR**, o que significa que o método não é tão sensível para condições de luz comparado com reconhecimento de rosto.

É difícil dizer como termografia de rosto corresponde para o método ideal na medida em que nenhum teste foi realizado e nenhum *kit* de desenvolvimento está disponível.

NOÇÕES LEVANDO-SE EM CONSIDERAÇÃO ESCANEAMENTO DE RETINA

Atualmente equipamento de escaneamento de retina tem diminuído tanto em tamanho e quanto em custo, por conseqüência, solucionando alguns dos problemas práticos. Um grande problema é o fato de que algumas pessoas possuem aversão contra ter seus olhos escaneados. Ao lado disto, o método não é adequado para utilização em veículo (embarcada), especialmente não enquanto dirigindo, na medida em que o motorista deveria ter que olhar em uma direção específica durante o escaneamento. Isto pode render problemas para manter os olhos concentrados sobre um único ponto longe o suficiente para a verificação e isto pode afetar negativamente a segurança de tráfego. Portanto, com a tecnologia de hoje em dia, este não é um método para utilizar para os propósitos deste pedido de patente.

NOÇÕES LEVANDO-SE EM CONSIDERAÇÃO RECONHECIMENTO DE GEOMETRIA DE MÃO

O principal benefício com reconhecimento de geometria de mão é o de que este método é bastante insensível à sujeira, calos e cicatrizes (dentro de limites razoáveis). Na medida em que existem diversas características da

integridade de mão que são mensuradas, não tem importância se os dedos estão sujos ou se a pessoa tenha acidentalmente se cortado, etc. O equipamento é barato e a verificação lema menos do que **um segundo**, mas o equipamento não desajeitado torna o método inadequado para propósitos automotivos.

NOÇÕES LEVANDO-SE EM CONSIDERAÇÃO SISTEMAS DE MODO MÚLTIPLO

10 Com um sistema de modo múltiplo, níveis diferentes de proteção podem ser complementados pela combinação de diferentes métodos. Para a utilização no dia a dia isto pode ser suficiente com verificação de impressão digital. Quando dirigindo em áreas perigosas, ou transportando 15 mercadorias perigosas, a verificação pode ser feita utilizando diversos métodos (por exemplo, tanto impressão digital e quanto escaneamento de íris) e, portanto, aumentando o nível de proteção.

20 Um aspecto interessante de sistemas de modo múltiplo é o de que eles podem ser utilizados para atualização automática da base de dados de gabarito. Imagine-se um sistema de verificação que utiliza **três** métodos de verificação randomicamente, por exemplo, **PIN**, impressão 25 digital e reconhecimento de rosto. Quando o sistema demanda para verificação de motorista, este sistema analisa todas as **três** características. Se **dois** dos métodos se completam de forma bem sucedida, a base de dados pode ser atualizada utilizando a terceira amostra. Por conseqüência, se o **PIN** 30 estiver correto e o *scanner* de impressão digital

proporciona um bom emparelhamento, o sistema pode tirar uma fotografia do rosto para atualizar a base de dados de gabarito. Isto pode economizar grandes quantidades de tempo na medida em que o sistema continuamente atualiza a si mesmo; por conseqüência, reduzindo manutenção do sistema.

SELEÇÃO DE MÉTODOS PARA IMPLEMENTAÇÃO DE PROTÓTIPO

A análise teórica dos diferentes métodos de verificação, conduz para noções e reflexões, que foram listadas na seção precedente. As noções e as análises de **SWOT** formam a plataforma principal para seleção de métodos de verificação para a implementação de protótipo.

SELEÇÃO DE MÉTODO

Nenhum método de verificação sozinho pode preencher os critérios do sistema ideal. As decisões finais de quais métodos utilizar foram fundamentadas sobre um balanço entre precisão e custo e bem como entre facilidade de utilizar e facilidade de enganar. Os outros critérios a partir do sistema ideal não diferem significativamente entre os métodos e não foram, conseqüentemente, considerados durante a seleção. Os prós e contras para cada método foram discutidos, e bem como o preço e o tempo de entrega.

MÉTODOS SELECIONADOS

As razões para descartar um método estão listadas abaixo, seguidas pelas razões para escolha dos métodos que são para serem implementados.

Termografia de rosto: câmeras de **IR** são mais

dispendiosas do que câmeras regulares, mas na medida em que o método é muito preciso e difícil de falsificar, esta é definitivamente uma área para dar uma olhada com mais cuidado. Infelizmente, pouca pesquisa foi feita levando-se em consideração termografia de rosto para propósitos de verificação e os autores foram incapazes de encontrar uma companhia que manufatura equipamento para este tipo de verificação.

Escaneamento de íris:

Um kit desenvolvido para escaneamento de íris custa cerca de **\$25000 - \$35000** (coroas suecas) o que está além do orçamento de projeto.

Movimentação labial:

Um outro método de verificação é necessário para que reconhecimento de movimentação labial venha a ser confiável o bastante. A idéia é a de implementação de **três** métodos para verificação para testar sua adequabilidade e compará-los um para o outro. De maneira a

garantir a possibilidade de diferentes níveis de proteção, todos os **três** métodos deveriam ser confiáveis por si mesmos, por conseqüência, reconhecimento de movimentação labial não é uma opção.

Escaneamento de retina: Escaneamento da retina não é adequado para propósitos automotivos devido para o exato alinhamento de olho requerido.

Geometria de mão: O equipamento requerido para escaneamento de geometria de mão é excessivamente desajeitado para se adaptar no coupê.

Os **três** sistemas remanescentes, verificação de impressão digital, reconhecimento de voz e reconhecimento de rosto são todos adequados para montagem no carro (embarcada) e existem fabricantes que poderiam oferecer *kits* com preços e em tempos de entrega razoáveis.

De maneira a tornar a integração de sistema tão fácil quanto possível, foi desejado que todos os sistemas fossem compatíveis com a mesma plataforma. Isto, juntamente com a habilidade para suporte de entrega, foram os **dois** critérios primordiais quando escolhendo o fabricante.

PINs são comuns hoje em dia e o método pode facilmente

ser implementado em um veículo utilizando o teclado para o telefone celular. Conseqüentemente, um sistema de verificação de **PIN** foi implementado como tal. Isto deveria também possibilitar uma comparação entre um método de verificação comum e os métodos de verificação biométricos.

Como apresentado nos resultados a partir da pesquisa, muitos dos que responderam preferiram que os gabaritos biométricos fossem armazenados sobre um cartão, que eles poderiam carregar com eles quando deixassem o veículo. Para ilustrar a possibilidade de integrar o armazenamento de gabarito com o tacômetro digital ativo, um leitor de cartão inteligente foi também incluído no sistema.

Para resumir, os métodos escolhidos para o sistema de protótipo são: impressão digital, reconhecimento de rosto, reconhecimento de voz mais **PIN** e verificação de cartão.

CASOS DE UTILIZAÇÃO

Diferentes espécies de situações e áreas de trabalho onde caminhões estão sendo utilizados levantam diversos desafios para um sistema de verificação. Reflexões sobre como o sistema deve ser utilizado conduziram para o desenvolvimento de um número de casos de utilização. Pela criação de casos de utilização realísticos, os benefícios e bem como uma demonstração da necessidade efetiva para um sistema de verificação de motorista são apontados.

DESENVOLVIMENTO DOS CASOS DE UTILIZAÇÃO

Estes casos de utilização são fundamentados sobre discussões e debates de idéias durante o processo de escolha de métodos para a implementação.

VERIFICAÇÃO DE MODO MÚLTIPLO UTILIZANDO TODOS OS MÉTODOS BIOMÉTRICOS

Este é o nível de proteção o mais alto, intencionado para veículos transportando mercadorias perigosas ou valiosas ou enquanto dirigindo em áreas de alto risco. O motorista verifica sua identidade utilizando todos os métodos para assegurar que ele é a pessoa apropriada. Abaixo estão alguns exemplos de como esta verificação poderia prosseguir.

O motorista chega à garagem para iniciar o dia de trabalho. Assim que ele adentra o veículo, ele insere seu cartão inteligente (integrado no cartão para o tacógrafo) no leitor, disca seu código **PIN** e após isso coloca seu dedo sobre o *scanner*. O **PIN** está correto e o dedo é verificado contra o cartão, e assim o sistema questiona por uma amostra de voz. O motorista pronuncia sua senha no microfone. Uma mensagem de sistema aparece, dizendo ao motorista para sentar em uma posição de dirigir normal, de maneira a executar a verificação de rosto. Dados registrados são analisados e comparados com os dados de gabarito armazenados sobre o cartão inteligente - a verificação foi bem sucedida. O nome e número de identificação de empregado são enviados, criptografados, para o escritório de apoio (*back-office*).

O motorista continua com o procedimento de verificação, mas falha com um dos métodos. Uma mensagem de sistema informa ao motorista acerca da verificação falha. O procedimento continua, como no exemplo antecedente e pelo menos um método é bem sucedido. O nome e número de

identificação de empregado são enviados, criptografados, para o escritório de apoio, juntamente com informação acerca da verificação(ões) falha(s).

Ao longo de uma viagem de transporte de longa
5 distância, o motorista tira uma soneca no coupê. Quando ele desperta, ele vai para fora para esticar suas pernas antes de continuar sua jornada. A porta de passageiro se abre e um impostor sobe e toma o assento de motorista. O impostor tenta partida ao veículo, mas não é bem sucedido com a
10 verificação, por conseqüência, o veículo é imobilizado. Um alarme é imediatamente enviado para o escritório de apoio e o sistema tira uma fotografia da pessoa atrás do volante de direção. Esta fotografia é também enviada para o escritório de apoio.

15

VERIFICAÇÃO DE MODO MÚLTIPLO UTILIZANDO DOIS MÉTODOS BIOMÉTRICOS

O propósito com este caso de utilização é o de assegurar que a pessoa que adentra ao assento de motorista
20 é o motorista apropriado. **Quatro** diferentes situações neste nível de proteção foram desenvolvidas, ver posteriormente. Observe-se que é possível possuir o veículo equipado com somente **dois** métodos de verificação biométricos. Entretanto, existe também a possibilidade de possuir todo o
25 equipamento necessário para todos os métodos e após isso randomicamente alterar qual método utilizar em cada ocasião.

O motorista chega à garagem para iniciar o dia de trabalho. Assim que ele adentra o veículo ele insere seu
30 cartão inteligente (integrado no cartão para o tacógrafo)

no leitor, disca seu código **PIN** e após isso coloca seu dedo sobre o scanner. O **PIN** está correto e o dedo é verificado contra o cartão. O sistema questiona por uma amostra de voz assim o motorista pronuncia sua senha no microfone. Dados 5 registrados são analisados e comparados com os dados de gabarito armazenados sobre o cartão inteligente - a verificação foi bem sucedida. O nome e número de identificação de empregado são enviados, criptografados, para o escritório de apoio.

10 O mesmo cenário como anteriormente, mas ao invés da verificação de voz uma mensagem de sistema aparece dizendo ao motorista para sentar em uma posição de dirigir normal, de maneira a executar a verificação de rosto. Dados registrados são analisados e comparados com os dados de 15 gabarito armazenados sobre o cartão inteligente - a verificação foi bem sucedida. O nome e número de identificação de empregado são enviados, criptografados, para o escritório de apoio.

O motorista falha com um ou mais método(s), mas pelo 20 menos um método é bem sucedido. O nome do motorista e número de identificação de empregado são enviados, criptografados, para o escritório de apoio, juntamente com informação sobre a verificação(ões) falha(s).

25 Nenhuma das verificações é bem sucedida, por consequência, o veículo é imobilizado e um alarme é imediatamente enviado para o escritório de apoio.

VERIFICAÇÃO BIOMÉTRICA ÚNICA EM DIFERENTES NÍVEIS DE
30 **PROTEÇÃO**

Esta verificação é sugerida para ocorrer depois de uma parada mais curta, depois que o motorista já foi verificado com diversos métodos, ou se o nível de proteção se torna suficiente com somente um método biométrico. Os níveis de 5 proteção podem evidentemente ser discutidos, mas nestes exemplos, eles são classificados como níveis de proteção altos, médios e baixos. Aqui, se seguem alguns exemplos para alta proteção.

O motorista está descarregando carga em uma de muitas 10 paradas durante o dia. O veículo é mantido parado com o motor funcionando. Quando termina o descarregamento, o motorista sobe de volta para o caminhão. Esta é uma parada curta, conseqüentemente, somente um método de verificação é requerido, método que irá ser estabelecido randomicamente. 15 Desta vez, o sistema requer verificação de impressão digital, de maneira que o motorista põe seu dedo sobre o *scanner*, para verificar que ele é ainda o próprio motorista dirigindo o veículo. Na medida em que o sistema verifica o motorista ele pode dirigir, enquanto seu nome e número de 20 identificação de empregado são enviados, criptografados, para o escritório de apoio para confirmação.

O motorista parou para comprar alguns salgadinhos em uma parada para caminhões. Isto é uma rápida parada com o motor deixado funcionando, por conseqüência, somente um dos 25 métodos disponíveis irá ser requerido para verificação antes de dirigir. Um impostor toma lugar no assento de motorista, que inicia a verificação. Na medida em que nenhuma verificação bem sucedida é realizada, o sistema tira uma fotografia com a câmera e envia esta juntamente 30 com um alarme para o escritório de apoio. O caminhão é

imobilizado.

O sistema de verificação está intencionado para aumentar a proteção, mas ele não tem que afetar a rotina de trabalho do motorista. Para tornar tão fácil quanto
5 possível o nível de proteção médio proporciona ao motorista mais independência do que o nível mais alto proporciona.

O motorista faz uma de muitas paradas durante o dia para descarregar alguma carga. O veículo é mantido parado com o motor ligado. Quando termina o descarregamento, o
10 motorista sobe de volta para o caminhão. Assim que ele se senta, ele coloca seu dedo sobre o *scanner*, para verificar sua identidade. O sistema verifica se é certo utilizar impressão digital desta vez, ou se o motorista tem que utilizar um dos outros métodos. Desta vez, o sistema requer
15 um outro tipo de verificação porque o motorista é encorajado a verificar sua identidade pronunciando sua senha. A verificação é bem sucedida e a motorista pode sair dirigindo, enquanto seu nome e número de identificação de empregado são enviados, criptografados, para o escritório
20 de apoio para confirmação.

O motorista parou para descarregar alguma das cargas. O motor é deixado funcionando. O motorista volta ao veículo e disca seu código **PIN**. Na medida em que o motorista está estressado ele disca os números errados, ele tenta de novo
25 e de novo, mas ele ainda não se lembra do código corretamente - a verificação falha. O sistema informa ao motorista que a verificação falhou e questiona a ele para verificar sua identidade utilizando ao invés disso escaneamento de impressão digital. A verificação é bem
30 sucedida e o motorista pode dirigir. O nome do motorista e

número de identificação de empregado são enviados, criptografados, para o escritório de apoio para confirmação, juntamente com informação acerca da falha de verificação **PIN**.

5 Um baixo nível de proteção pode somente requerer um método para verificação. Isto significa que este pode ser suficiente para o veículo possuir equipamento para um único método de verificação. Isto também proporciona a possibilidade de possuir diversos métodos em um caminhão e
10 dependendo, por exemplo, da carga, rota, ou extensão de uma parada, somente demanda para um método. Um sistema de verificação no veículo pode ser presumido aumentar proteção. Entretanto, com somente um método, existe naturalmente um alto mais risco de fraudes bem sucedidas do
15 que com diversos métodos de verificação.

O motorista está descarregando carga em uma de muitas paradas durante o dia. O veículo é mantido parado com o motor funcionando. Quando termina o descarregamento, o motorista sobe de volta para o caminhão. Ele senta e coloca
20 seu dedo sobre o *scanner*, para verificar sua identidade. Na medida em que o sistema verificou o motorista ele dirige e seu nome e número de identificação de empregado são enviados, criptografados, para o escritório de apoio para confirmação.

25 O motorista parou para descarregar carga. Na medida em que o motorista já se identificou mais cedo naquele dia, um método de verificação irá ser suficiente, ainda que o veículo possua um nível mais alto de proteção. Um outro motorista, que também possui um cartão inteligente com seus
30 dados biométricos armazenados, toma o lugar do motorista e

tenta verificar sua identidade. O sistema noticia que o cartão foi tomado e um novo cartão é colocado, e assim uma verificação única não irá ser suficiente. O motorista verifica sua identidade com todos os métodos e a informação é enviada, criptografada, para o escritório de apoio, onde rapidamente é descoberto que não é o motorista apropriado quem está dirigindo o veículo.

O motorista parou para comprar salgadinhos em uma parada para caminhões. Isto é uma parada rápida com o motor deixado funcionando, por consequência, somente um dos métodos disponíveis irá ser requerido para verificação antes de dirigir. Um impostor toma lugar no assento de motorista, que inicia a verificação. Na medida em que nenhuma verificação bem sucedida é realizada o veículo é imobilizado. O sistema tira uma fotografia com a câmera e envia esta juntamente com um alarme para o escritório de apoio.

Um motorista adentra o veículo. Ele coloca seu dedo sobre o *scanner*, mas não é bem sucedido com a verificação. Na medida em que este era o único método disponível, um alarme sobre a verificação falha é imediatamente enviado para o escritório de apoio. O veículo é imobilizado.

VERIFICAÇÃO MANUAL ENQUANTO DIRIGINDO

Um cenário possível pode ser o de que um impostor force o motorista para verificar sua identidade e após isso o joga para fora do veículo. Para evitar isto e riscos similares, o motorista deveria também ser verificado enquanto dirigindo. Abaixo se seguem alguns exemplos para explanar a idéia.

O veículo está rodando nas estradas. Uma mensagem de sistema aparece, questionando o motorista a dizer sua senha para verificar sua identidade. O motorista assim o faz e é bem sucedido com a verificação. Seu nome e número de 5 identificação de empregado são enviados, criptografados, para o escritório de apoio.

O motorista está fora em uma tarefa de transporte de longa distância. Uma mensagem de sistema aparece, questionando o motorista para dizer sua senha para 10 verificar sua identidade. O motorista assim o faz, mas a verificação falha na medida em ele está rouco neste dia. O motorista tenta **duas** vezes mais, mas a verificação ainda falha, e assim o sistema questiona a ele para ao invés disso colocar um dedo sobre o *scanner*. Desta vez, a 15 verificação é bem sucedida. O nome do motorista e número de identificação de empregado são enviados, criptografados, para o escritório de apoio juntamente com informação acerca da verificação falha.

O veículo está rodando nas estradas. Uma mensagem de 20 sistema aparece, questionando o motorista a colocar um dedo sobre o *scanner* para verificar sua identidade. O motorista não pode verificar sua identidade com quaisquer dos métodos. Um alarme é imediatamente enviado para o escritório de apoio, juntamente com uma foto do motorista 25 não verificado tirada pela câmera para verificação de rosto. Na medida em que o motorista foi verificado antes de dar partida ao veículo, aquele nome do motorista e número de identificação de empregado são enviados, criptografados, para o escritório de apoio juntamente com informação acerca 30 da verificação falha enquanto dirigindo.

Um veículo, com equipamento para diversos métodos de verificação, está rodando nas estradas. Uma mensagem de sistema aparece, questionando o motorista a colocar um dedo sobre o *scanner* para verificar sua identidade. Nenhuma
5 verificação é feita dentro dos **três** minutos seguintes, um alarme é, conseqüentemente, enviado para o escritório de apoio.

O veículo está rodando nas estradas. Uma mensagem de sistema aparece, questionando o motorista a colocar um dedo
10 sobre o *scanner* para verificar sua identidade. A verificação falha e na medida em que este é o único método para verificação neste veículo, um alarme é imediatamente enviado para o escritório de apoio.

15 **VERIFICAÇÃO AUTOMÁTICA ENQUANTO DIRIGINDO**

Esta verificação é feita sem intervenção a partir do motorista. Isto implica em diversas vantagens, por exemplo, o motorista não é perturbado mesmo se sua identidade for verificada enquanto ele está dirigindo e um impostor nem
20 sempre sabe que o sistema tenta verificá-lo. Para tornar uma verificação automática possível, o veículo tem que proporcionar equipamento de reconhecimento de rosto. Abaixo se seguem alguns exemplos de verificação automática enquanto dirigindo.

25 O veículo está rodando nas estradas. O sistema tira fotografias do motorista e compara as características com o gabarito sobre o cartão inteligente no tacógrafo. A verificação é bem sucedida e o nome do motorista e número de identificação de empregado são enviados, criptografados,
30 para o escritório de apoio.

O motorista está fora em um transporte de longa distância em um veículo com diversos métodos de verificação possíveis. O sistema tenta verificar o motorista contra o gabarito no cartão inteligente no tacógrafo. A verificação
5 falha, e assim uma mensagem de sistema aparece questionando o motorista a colocar um dedo sobre o *scanner*. Desta vez, a verificação é bem sucedida. Uma criptografia (código secreto) do nome do motorista e número de identificação de empregado, é enviada para o escritório de apoio juntamente
10 com informação acerca da verificação falha.

Em uma situação similar como anteriormente, a verificação falha e assim o motorista é questionado a colocar um dedo sobre o *scanner*. Nenhum método para verificação é bem sucedido e assim um alarme é
15 imediatamente enviado para o escritório de apoio, juntamente com uma foto do motorista não verificado tirada pela câmera para verificação de rosto.

O veículo está rodando nas estradas. A verificação automática falha e uma mensagem de sistema aparece,
20 questionando o motorista a colocar um dedo sobre o *scanner* para verificar sua identidade. Nenhuma verificação é feita dentro dos **três** minutos seguintes, um alarme é, conseqüentemente, enviado para o escritório de apoio juntamente com informação acerca da verificação de rosto
25 falha e a ausência da verificação por qualquer método adicional.

PROJETO E IMPLEMENTAÇÃO DO SISTEMA DE PROTÓTIPO

Quando os métodos de verificação foram escolhidos, e o
30 equipamento chegou, era tempo de colocar o sistema

juntamente. O sistema foi desenvolvido utilizando um processo de desenvolvimento interativo e resultou no projeto mostrado nesta seção. Uma visão global do sistema de verificação implementado está demonstrada e as demandas de *software* para um tal sistema estão explanadas juntamente com uma descrição da implementação.

HARDWARE

Manufaturadores para o *hardware* foram primordialmente escolhidos a partir de **três** critérios: custo, tempo de entrega e compatibilidade. A primeira parte desta seção descreve o *hardware* e a segunda parte desta seção descreve o resultado da implementação.

O HARDWARE DO SISTEMA

O equipamento utilizado para este projeto está listado e descrito abaixo.

O sistema de verificação de impressão digital utilizado é um *BioCoreII* da *Precise Biometrics AB*, Suécia. É um sistema embutido (fechado), portanto, o *hardware* estava incluído no *kit*.

O sistema de verificação de rosto é um *VeriLook SDK 1.1* da *Neurotechnologija Inc.*, Lituânia. A câmera, uma *Logitech QuickCam 4000 Pro*, foi escolhida levando-se em consideração as recomendações da *Neurotechnologija Inc.*

Para o reconhecimento de voz, uma licença para *VoiceKey SDK* da *SpeechPro Inc.*, Rússia, foi comprada. A câmera de reconhecimento de rosto possuía um microfone embutido de maneira a ser utilizado para conferências via *internet*; isto era um bônus na medida em que o microfone

avaliação de resultados juntamente para proporcionar/negar autorização.

Mostrador de PC: O mostrador de **PC** executa a **GUI** e apresenta informação sobre a tela de toque montada no console central da cabine de caminhão.

Tela de toque: monitor sensível ao toque **TFT** wide screen de **7"** montado no painel da cabine de caminhão. Utilizado para apresentar informação e instruções e para servir como teclado durante a verificação de **PIN**.

COLOCAÇÃO DO EQUIPAMENTO

Antes de implementação do sistema no simulador, a colocação do equipamento foi discutida. Existiram planos para colocar o scanner de impressão digital sobre a alavanca de mudança de marcha, mas na medida em que este ficou meio escondido no simulador, o scanner foi colocado sobre o volante de direção. O sistema de reconhecimento de rosto requer uma fotografia recuperada a partir de um ângulo não excedendo **5 graus** em qualquer direção. Isto proporcionou **duas** possibilidades de colocação de câmera, tanto acima do painel (grupo) de instrumentos ou quanto no teto acima do pára-brisa. Com a última colocação o sistema tem pior desempenho e, por consequência, a câmera foi colocada acima do painel de instrumentos. O painel possuía uma abertura que adaptava bem a tela. Esta montagem também determinou ao teclado uma colocação de autenticidade. Posteriormente, está uma fotografia de partes do sistema

montado no coupê de caminhão (Ver **Figura 13**).

SOFTWARE

Todos os **três** fabricantes ofereceram *kits* de desenvolvimento para um ambiente **C++** e, conseqüentemente, esta plataforma de desenvolvimento foi escolhida. A implementação efetiva (por exemplo, o código em si mesmo) não é importante para o propósito ou os resultados deste pedido de patente e não irá, conseqüentemente, ser descrito em detalhes adicionais.

INTERFACE GRÁFICA DE USUÁRIO (GUI)

O propósito da **GUI** foi o de permitir que o usuário e o sistema se comunicassem um com o outro. A fase de projeto e bem com o resultado estão apresentados nesta seção.

DESENVOLVIMENTO DA GUI

Primeiro um protótipo de baixa **f1** foi esboçado sobre papel, um papel para cada mensagem que deveria ser mostrada durante o teste. Existiam tanto mensagens escritas e quanto ilustrações, e algumas das mensagens possuíam **duas** ou **três** versões. As mensagens escritas estavam todas em suco na medida em que foi suposto ser esta a língua pátria para os participantes do teste. Uma busca para sons adequados para complementar as mensagens foi também realizada. A **GUI** de baixa **f1** foi mostrada, individualmente, para **cinco** empregados da **VTEC** que possuem pouca ou nenhuma experiência em projeto de **GUIs**, de maneira a determinar suas reações. Eles primeiro mostraram uma versão das mensagens na sucessão em que elas apareciam no teste. Posteriormente,

eles mostraram versões alternativas e foram questionados a determinar suas opiniões sobre qual delas utilizar.

A **GUI** de baixo **f1** foi após isso mostrada para uma pessoa com vasta experiência de trabalho com **GUIs** e situações de teste. O cenário de teste e bem como a **GUI** foram discutidos e **duas** anotações foram adicionadas. A **GUI** foi após isso implementada em *Macromedia Director MX*.

RESULTADO DA GUI IMPLEMENTADA

10 Cada etapa no procedimento de verificação possuía uma mensagem escrita (em sueco), uma ilustração e um som. **Dois** diferentes sons foram utilizados para atrair a atenção do motorista para a tela. O primeiro visto como indicação que uma nova tarefa foi demandada, ou que a tarefa recente foi
15 realizada com sucesso. O segundo som foi utilizado para ilustrar se a verificação falhou ou se um erro ocorreu. Adicionalmente, a fotografia se tornou verde para sucesso e vermelho para falha. Abaixo estão **dois** exemplos a partir da **GUI** (Ver **Figura 14**).

20

O SIMULADOR DE DIREÇÃO

Um simulador foi requerido para possibilitar circunstâncias tão realísticas quanto possível durante o teste do protótipo de sistema. A **VTEC** possui um simulador,
25 que foi suprido para este teste. O simulador possui **três** projetores iluminando uma grande tela arqueada. Este tipo de ajuste (*setup*) é para reforçar a sensação de movimentação efetivamente e para possibilitar ao motorista perceber as circundâncias de uma maneira mais natural do
30 que com utilização de somente um projetor e uma tela plana.

Uma cabine **Volvo FH12** é colocada no meio da sala, de frente para a tela. Foi possível acionar os alto-falantes com um som de motor simulado.

O simulador foi utilizado até recentemente para testes com um carro, a cabine e o simulador, conseqüentemente, ainda não foram completamente sincronizados. Existiram propriedades adicionais que não são se adequaram muito bem ao teste e os autores não possuíam possibilidades de mudá-las. Por exemplo, no interior o motorista possuía controle de acelerador e de freio, mas não controle de freio de estacionamento, de embreagem, de alavanca de câmbio e nem de cruzeiro (*cruise control*). O tanque estava sempre vazio e nem o tacômetro e nem o odômetro foram ajustados para representar um caminhão. Na medida em que não existia freio de estacionamento, o simulador tinha que ser desligado se o motorista necessitasse parar e deixar o veículo. Na medida em que o freio foi pressionado para baixo, o simulador não se movimentou, mas quando liberando o freio (tal como quando deixando o coupê) o veículo simulado continuou lentamente a sua movimentação para frente (Ver a **Figura 15** e a **Figura 16**).

AS PREPARAÇÕES ANTES DO TESTE

A idéia de se colocar um sistema de verificação no interior de um caminhão conduziu para diversas questões acerca de quando um tal sistema deveria ser utilizado, para o que ele poderia ser utilizado e como freqüentemente a verificação deveria ser feita. Algumas das questões hipotéticas poderiam ser possíveis de ser respondidas com a ajuda de um teste de simulador; outros necessitam de mais

pesquisas e testes de autenticidade.

As preparações para o teste consistem primordialmente de **quatro** partes; para preparar as questões da entrevista, para esboçar um cenário para o simulador, para encontrar um número satisfatório de assuntos de teste apropriados e para conduzir um teste piloto. Como precedentemente mencionado, questões levando-se em consideração quando e como a verificação deveria ser realizada foram levantadas durante o trabalho de preparação. As entrevistas e o cenário de teste foram esboçados de maneira a responder estas questões (entre outras).

ENTREVISTAS

Como o teste abordou, as questões de pesquisa foram ajustadas de maneira a se ajustar às entrevistas. Para possibilitar uma comparação, com os resultados a partir das pesquisas precedentes, muitas questões foram feitas similarmente.

DESENVOLVIMENTO DAS QUESTÕES DE ENTREVISTA

Dois entrevistas foram preparadas. A primeira foi para suporte antes do teste de simulador e a segunda, mais exaustiva, entrevista foi para suporte mais tarde. Algumas das questões a partir das entrevistas precedentes foram repetidas para ver se o motorista mudou de opinião durante o teste.

As questões foram lidas e comentadas por **dois** cientistas do comportamento de maneira a ver se deveriam existir quaisquer questões re-definidas, adicionadas ou eliminadas.

AS QUESTÕES

A primeira entrevista foi iniciada com questões acerca das rotinas de trabalho dos motoristas. As questões também
5 trataram salvaguardas como proteção e o que isto significa para o motorista. Depois investigando o conhecimento do motorista de biométricos, os diferentes métodos utilizados no teste foram introduzidos para possibilitar reações espontâneas. O motorista foi também questionado se ele
10 poderia ver quaisquer vantagens ou desvantagens com um sistema de verificação.

A segunda entrevista questionou acerca da experiência de teste. O motorista foi questionado para graduar os diferentes métodos e uma vez novamente proporcionou sua
15 opinião de possíveis vantagens ou desvantagens.

Muitas das questões foram graduadas, sempre a partir de 1 até 5, onde 1 foi estabelecido para a opinião negativa e 5 foi estabelecido para a opinião positiva.

O CENÁRIO DE TESTE

Para encontrar o que era necessitado para a implementação no simulador e tentar ver o que deveria ser possível testar, um cenário de teste foi delineado.

DELINEANDO O CENÁRIO

Estas noções serviram como inspiração durante a criação do cenário de teste. Este foi delineado através de reflexões e discussões, e conduziu para um cenário de teste final onde diversos aspectos do problema foram incluídos.
30 Foi desejado testar tantos métodos quanto possíveis, tanto

enquanto estando parado e quanto enquanto dirigindo. Ao mesmo tempo, o cenário deveria ser tão mais realístico quanto possível, evitando o risco de que este poderia conter excessivas diferentes tarefas sobre a curta duração do teste. De outro modo, o participante do teste poderia perceber que ele tem que verificar sua identidade extremamente freqüentemente, o que pode não deveria ser o caso na vida real. O resultado foi um cenário equilibrado, mas ainda assim exaustivo.

10

O CENÁRIO DE TESTE

O cenário de teste se inicia com uma verificação inicial completa. Ao motorista deveria então ser concedido algum tempo para ser utilizado para o simulador antes de verificação de impressão digital enquanto dirigindo viesse a ser requisitada.

Depois de aproximadamente metade do tempo no simulador um "coffee break" (intervalo) teve lugar. Depois do intervalo o motorista tinha que prosseguir através de uma verificação curta, utilizando tanto impressão digital ou quanto voz. Ainda uma outra verificação enquanto dirigindo foi requisitada antes do teste finalizado, desta vez esta foi verificação de voz. **Dois** verificações automáticas foram feitas enquanto dirigindo, uma no começo e uma depois do intervalo. Se elas falhassem, o motorista deveria ser questionado para verificação de impressão digital ao invés disso, mas se bem sucedido, ele não deveria ser informado acerca disto durante o teste (Ver **Figura 17**).

30

RECRUTANDO PESSOAS PARA O TESTE

O recrutamento de motoristas de caminhão para o teste foi terceirizado para uma companhia externa. Eles foram questionados para recrutar **20** motoristas e a eles foi também ensinado que uma mistura de motoristas de transporte de longa distância e de distribuição era desejada. Durante o recrutamento, aos motoristas foi ensinado que eles deveriam participar em um teste de simulador de direção, onde usabilidade e aceitação do usuário viriam a ser avaliadas. O propósito em se dar informação vaga acerca do teste durante o recrutamento foi o de receber uma mistura satisfatória de motoristas com diferentes fundamentos (panoramas) e expectativas.

TESTE PILOTO

Testes piloto foram realizados antes do teste efetivo, para tornar possível aperfeiçoar o sistema e ajustar o cenário e as entrevistas.

Questões que foram significativas para serem respondidas pelo teste piloto foram, por exemplo:

- O cenário é realístico? São excessivas/muito poucas tarefas, em tempo excessivo ou insuficiente? As coisas deveriam acontecer em uma ordem diferente?

- A **GUI** é bem projetada? É evidente o que fazer todo o tempo? O som é audível e adequado naquele momento em particular?

- A colocação da câmera é aceitável? Você pode facilmente alcançar o sensor de impressão digital e o teclado? É sentido embaraçoso se dizer a senha no ar ao invés de diretamente em um microfone?

- As questões de entrevista são significativas e

corretamente formuladas? São excessivas/poucas questões?

- O teste é excessivamente demorado ou podem ser adicionadas tarefas adicionais? Se sente confortável sendo filmado e observado por um supervisor de teste na cabine?

5

O PROCEDIMENTO DO TESTE PILOTO

Empregados na **VTEC** com vasta experiência em direção de caminhão foram questionados a participar; entre eles um cientista em comportamento, que foi especialmente questionado para dar opiniões sobre as entrevistas. Todos juntos, **seis** homens participaram. **Três** deles fizeram o procedimento de teste em sua integridade, tanto com entrevistas, e quanto pesquisa de aceitação e cenário de simulador. Os outros **três** não foram entrevistados, mas simplesmente listados no sistema, instruídos acerca do simulador e testagem do cenário. Diferentes condições de luz foram testadas para ver os requerimentos para a verificação de rosto.

15

RESULTADOS A PARTIR DO TESTE PILOTO

O teste piloto implicou em modificações para o sistema de maneira a aumentar estabilidade e usabilidade, e para fazer o teste tão autêntico e exaustivo quanto possível. Um terceiro som foi adicionado de maneira que o usuário recebeu o retorno audível quando discando um dígito, ao invés de somente os asteriscos que são mostrados na tela durante a verificação de **PIN**. Algumas das questões de entrevista foram ajustadas para serem mais especificadas.

Nenhum dos participantes poderia ser registrado (para reconhecimento de rosto) se estivesse excessivamente escuro

25
30

e se tornou aparente que a luz a partir das telas de simulador sozinha não foi suficiente para o registro. Por outro lado, a sala não tem que estar excessivamente clara na medida em que isto afeta a qualidade de imagem do simulador. Quando experimentando com mais luz no interior do coupê, problemas ocorreram com pessoas utilizando óculos, na medida em que iluminação extra provocou reflexos. Eventualmente, um ajuste de iluminação foi encontrado, que tornou possível para todos os sujeitos de teste serem registrados e verificados pelo sistema. Uma observação interessante durante estes experimentos de luz foi a de que foi possível verificar algumas pessoas (que não utilizavam óculos) com menos luz na sala, do que aconteceu quando elas foram registradas.

15

O TESTE

Esta seção descreve o teste final do protótipo de sistema. A primeira parte descreve como o teste e as entrevistas foram realizadas, a segunda parte apresenta os resultados.

20

O PROCEDIMENTO DE TESTE

O sistema de verificação foi testado em um simulador, como anteriormente mencionado, para fazer a situação de teste tão autêntica quanto possível. Infelizmente, **dois** motoristas tiveram de cancelar, por conseqüência, somente **18** dos motoristas convidados tiveram a capacidade de atender, todos homens. Os motoristas foram testados e entrevistados um de cada vez.

30

ANTES DO TESTE DE SIMULADOR

Quando o participante de teste, a partir de agora em
diante também referido como o motorista, chegou ele foi
recepcionado pelo supervisor de teste. Ele foi informado,
5 tanto verbalmente e quanto por escrito, de seus direitos e
obrigações, por exemplo, que seu anonimato estava garantido
e que ele poderia descontinuar o teste a qualquer tempo.
Ele foi avisado que ele primeiro deveria ser entrevistado
acerca de seu trabalho e após isso dirigir o simulador
10 antes que ele viesse a ser entrevistado novamente acerca
daquela experiência de teste. O supervisor de teste pediu
permissão para registrar (gravar) as entrevistas.

Um dos inventores foi supervisor de teste durante todo
os testes; o outro inventor atuou como o técnico e foi
15 responsável pelos registros (listagens) e pela gravação de
vídeo.

PRIMEIRA ENTREVISTA

A fase de testagem começou com uma entrevista acerca
20 do dia de trabalho normal do motorista, rotinas no
trabalho, suas opiniões sobre proteção e qual espécie de
conhecimento e experiências ele possuía de biométricos. A
primeira entrevista durou por aproximadamente **20 minutos** e
foi organizada em uma sala de conferências próxima ao
25 simulador. O supervisor de teste escreveu as respostas do
motorista ou interpretadas e graduadas a partir de **1** (valor
negativo) para **5** (valor positivo), dependendo do tipo de
questão. Se a resposta para uma questão graduada era vaga o
motorista foi questionado para graduar entre **1** e **5**. No caso
30 do motorista aparentar não ter compreendido uma questão,

esta foi explanada pelo supervisor de teste.

REGISTRO (PROTOCOLO)

Depois da entrevista inicial, o participante de teste
5 foi mostrado para o simulador e solicitado a tomar lugar e
ajustar o assento e o volante de direção para uma posição
de dirigir normal e confortável. Antes que o registro
começasse, o técnico verificou que a câmera poderia
determinar uma visão clara do motorista e, se necessário, o
10 motorista foi solicitado a abaixar o volante de direção.

Foi determinado ao motorista um **PIN** e após isso a fase
de registro começou. Foi mostrada a ele que parte da
impressão digital colocar sobre o *scanner*. Na medida em que
o *scanner* foi colocado sobre o volante de direção, o
15 participante teve que utilizar o polegar direito, os outros
dedos deveriam ser difíceis de conseguir a posição correta
para o escaneamento. Ele teve uma chance de tentar colocar
o polegar sobre o *scanner* de maneira a conseguir utilizar a
colocação apropriada. Depois do que a impressão digital foi
20 registrada. O técnico após isso solicitou ao motorista para
olhar diretamente à frente na tela de simulador como se ele
estivesse dirigindo, isto de maneira a recuperar o gabarito
de reconhecimento de rosto. Para a verificação de voz, ao
motorista foi dito que uma sentença que demorasse pelo
25 menos **três segundos** fosse requerida, de maneira a tornar
possível para o computador analisa-la. A ele foi dito
também que o microfone estava embutido na câmera, de
maneira que ele somente devia dizer a senha em voz alta. Ao
motorista foi determinada a senha "Meu nome é primeiro
30 nome, sobrenome". Como precedentemente mencionado, a função

da verificação da voz foi somente simulada.

INSTRUÇÕES DE SIMILADOR

Quando o registro foi completado, ao motorista foi
5 dado o cartão inteligente e foi solicitado que este fosse
seu cartão de tacógrafo digital pessoal durante o teste.
Ele foi após isso questionado para descer do veículo para
receber instruções acerca do simulador e do cenário de
teste.

10 O motorista foi informado de que ele deveria ser
filmado durante o teste e de que ele deveria estar
completamente certo de descontinuar o teste a qualquer
tempo se ele viesse a se sentir desconfortável. A ele foi
avisado que algumas pessoas se tornam nauseadas no
15 simulador ainda que elas normalmente não se sentissem
enjoadas em veículos. A atenção do motorista foi
direcionada para a imagem de simulador, que no momento
estava parado no meio de uma auto-estrada. Ele foi avisado
que o supervisor de teste estava indo se sentar ao lado
20 dele no coupê para guiá-lo ao longo do caminho. Ele foi
instruído que ele deveria estar dirigindo na auto-estrada
por enquanto, e após isso converter para a direita e
continuar até que ele viesse a chegar em um vilarejo. No
vilarejo ele deveria parar para um intervalo, depois do que
25 o cenário continuaria ainda por uns poucos minutos de
direção. O motorista foi informado acerca do equipamento
existente no simulador e bem como o equipamento
desaparecido (mencionado em "O simulador de direção"). O
motorista foi solicitado a imaginar que o cenário perdurou
30 por uma tarde, ao invés dos **20 minutos** que ele efetivamente

esteve dirigindo.

Depois destas breves instruções, o motorista foi solicitado a re-adentrar a cabine para começar o teste. O supervisor de teste adentrou o veículo a partir da outra lateral e iniciou a simulação quando o motorista estava
5 sentado e fechou a porta.

O TESTE DE SIMULADOR

O motorista assumiu o assento de direção. O supervisor de teste adentrou o veículo a partir da outra lateral e iniciou o cenário quando o motorista fechou a porta. Na medida em que inseriu o cartão inteligente a verificação inicial começou. Esta primeira verificação consistiu de todos os **quatro** métodos e foi permitido ao motorista falhar
10 em cada método **três** vezes antes que o sistema mudasse para o próximo método. Se o motorista passasse em pelo menos **dois** dos **três** primeiros métodos, a integridade de verificação inicial era considerada bem sucedida. O quarto método foi reconhecimento de voz, que foi somente simulado
15 durante o teste.

Como precedentemente descrito o teste começou sobre uma auto-estrada simulada. Depois de algum tempo, o supervisor de teste disparou a primeira verificação enquanto dirigindo, que foi o reconhecimento de rosto
20 automatizado. Observe-se que o motorista não foi informado sobre esta verificação a menos que esta falhasse. No caso em que a verificação automática falhasse, o sistema deveria questionar o motorista a verificar sua identidade utilizando verificação de impressão digital. Se isto também
25 falhasse, o sistema questiona o motorista a discar seu **PIN**.

O participante de teste continuou dirigindo e depois de algum tempo o supervisor de teste disparou a próxima etapa, que foi a segunda verificação enquanto dirigindo. dialogo de sistema **r~** apareceu, questionando o motorista a
5 verificar sua identidade pela utilização de impressão digital. No caso em que a verificação falhasse, o motorista foi demandado para uma verificação de **PIN**.

Depois ainda de dirigir algum tempo, a estrada conduziu para um pequeno vilarejo onde o motorista foi
10 solicitado a descer para um intervalo (*coffee break*). (Isto durou aproximadamente **12 minutos - 13 minutos** a partir de quando o motorista adentrou o veículo para iniciar o cenário). O motorista e o supervisor de teste desceram do caminhão e foram para uma outra sala onde foram oferecidos
15 ao motorista alguns refrescos. Isto tinha **dois** propósitos; o primeiro foi o de simular um intervalo mais curto iniciando um procedimento de verificação mais curto quando tentando dirigir novamente. O segundo foi o de determinar ao motorista uma oportunidade para determinar ao supervisor
20 de teste comentários e reações espontâneas sobre a primeira parte do teste. Para possibilitar comparações estatísticas com outros sistemas automotivos uma escala de aceitação **[56]** foi manipulada para os motoristas durante o intervalo. Na medida em que a língua pátria dos participantes era o
25 sueco, todos eles receberam uma versão sueca da escala de aceitação. A escala consiste de **nove** pares de palavras contrárias, **cinco** são acreditadas refletir a utilidade e **quatro** a satisfação. Por adição as respostas levando-se em consideração utilidade e satisfação, respectivamente, uma
30 média pôde ser calculada a partir daquela e, por intermédio

disso, contabilizando a utilidade e a satisfação entre **-2** e **+2**. O supervisor de teste explicou que isto era somente o sistema de verificação, não o simulador, que era para ser avaliado. Se o motorista não compreende a escala de aceitação pela leitura das instruções escritas, o supervisor de teste explicou adicionalmente e após isso deixou o motorista preencher as respostas em privacidade.

Alguns dos motoristas levaram o "cartão de tacógrafo" com eles para o intervalo, mas a maior parte deles o deixou no leitor. O cenário foi continuado pelo supervisor de teste na medida em que o motorista uma vez mais novamente tomou lugar no assento do motorista depois do intervalo. Se o motorista deixou seu cartão, o sistema iniciou rapidamente com a verificação. Se o motorista levou o cartão com ele, o sistema iniciou questionando pelo cartão, antes de começar a verificação. Para os primeiros **dez** participantes, o sistema questionou o motorista a verificar sua identidade utilizando impressões digitais, para os **oito** remanescentes, verificação de voz foi utilizada. Se esta verificação única falhasse, o motorista era questionado a discar seu **PIN**. O cenário foi programado de uma maneira tal que a **GUI** anunciava "verificação de voz bem sucedida" depois de aproximadamente **6 segundos** a partir da demanda para verificação. Para evitar que os participantes descobrissem a simulação, eles foram lembrados pelo supervisor de teste se eles não dissessem sua senha breve o suficiente.

Depois de algum tempo a estrada conduziu para uma cidade e o supervisor de teste disparou a segunda verificação automática enquanto dirigindo, que era similar

para a primeira recentemente descrita anteriormente. Se o sistema não fosse bem sucedido com a verificação, o motorista era informado acerca da falha e questionado para verificar sua identidade utilizando impressões digitais ao invés disso. No caso em que verificação tivesse falhado, também o motorista deveria ter sido solicitado a discar seu código **PIN**.

O participante continuou dirigindo em consequência do que o supervisor de teste disparou o último procedimento de verificação, verificação de voz enquanto dirigindo. Brevemente depois desta verificação, o motorista foi solicitado a encostar e parar o veículo.

ENTREVISTA ACOMPANHADA

Depois do teste, o motorista foi levado de volta à sala de conferências para ser entrevistado novamente. A segunda entrevista tratou da experiência do motorista do teste em sua totalidade, pontuando cada método de verificação, a **GUI** e o cenário.

O motorista foi questionado sobre suas experiências da primeira verificação inicial e das verificações enquanto dirigindo (escaneamento de impressão digital e reconhecimento de voz, respectivamente). Se as verificações automáticas fossem bem sucedidas, o motorista era informado sobre suas existências. Ele foi encorajado a compartilhar suas opiniões sobre a utilização de tais métodos e sobre a idéia de ter de fazer uma outra espécie de verificação no caso em que a verificação automática tivesse falhado. Os motoristas que não tinham sido totalmente bem sucedidos verificados pela verificação automática foram questionados

acerca de suas experiências de ter de fazer ainda uma outra espécie de verificação enquanto dirigindo. Eles também foram encorajados a compartilhar suas opiniões sobre terem uma verificação automática enquanto dirigindo. Para possibilitar comparações dos diferentes métodos e verificações que tinham ocorrido no teste, o motorista recebeu as mesmas questões para cada ocasião, respectivamente. Questões repetidas foram graduadas (a partir de 1 até 5) se a verificação/o método foi complicada ou fácil, consumidora de tempo ou rápida, estranha ou razoável, chata ou divertida, desinteressante ou interessante e desnecessária ou necessária.

O motorista foi interrogado sobre seus pensamentos em torno de proteção (segurança) e a implementação de um sistema de verificação em um veículo. Ele foi encorajado a compartilhar seus pensamentos sobre isto antes do teste, e depois do teste, para ver se o teste tinha mudado sua opinião. Antes que a seção terminasse, o motorista foi questionado se ele desejava de adicionar qualquer coisa, se alguma coisa foi perdida no teste ou se ele tinha quaisquer questões (dúvidas).

RESULTADOS A PARTIR DOS TESTES

Esta seção começa com uma introdução dos participantes do teste. Mais tarde, os resultados a partir da primeira entrevista, o teste de simulador e a entrevista detalhada que se seguiu ao teste de simulador irão ser apresentados. Todas as entrevistas foram organizadas em sueco, por consequência, as citações aqui apresentadas são das traduções dos autores.

A idade média dos participantes foi de **41 anos**, com um desvio padrão de **onze anos**. O participante o mais jovem tinha **23 anos** e o mais idoso **60 anos**. Os participantes trabalharam como motoristas de caminhão por uma média de **18**
5 **anos**, se espalhando (distribuindo) a partir de **três anos** até **quarenta anos**. **Quatro** dos motoristas dirigiram unicamente transporte de longa distância, **seis** dos motoristas dirigiram primordialmente na área local de *Gotemburgo* e os **oito** remanescentes dirigiram fretamentos
10 misturados.

RESULTADOS A PARTIR DA PRIMEIRA ENTREVISTA

Acerca da questão do que "proteção" significa para eles, a maior parte dos motoristas falou sobre veículos
15 seguros. Quando a questão foi especificada para proteção contra ações criminais, a maior parte dos motoristas falou sobre o alarme de combustível que muitos motoristas de transporte de longa distância possuem em seus carros. Todos os motoristas referiram que eles se sentem seguros no
20 trabalho, exceto para um que contabilizou nem seguro nem inseguro. A contabilidade média foi **4,78** com um desvio padrão de **0,55**. As circunstâncias ou a área onde alguém está dirigindo poderia afetar a sensação de segurança em concordância com **dez** dos motoristas. **Três** deles acreditaram
25 que tempo também era um fator juntamente com as circunstâncias. Em concordância com **três** dos motoristas existem outras coisas que afetam suas sensações de segurança, por exemplo, que espécie de carga eles estão transportando. **Dois** dos motoristas se sentiram seguros não
30 importando o que e não vêem quaisquer fatores que afetaram

aquele sensação de segurança.

Todos, exceto um, utilizaram um cartão no trabalho para conseguirem acesso a itens ou áreas específicas. O único que não utilizou qualquer cartão utilizou um **PIN** para
5 conseguir acesso. **Oito** dos motoristas utilizaram tanto cartões e quanto **PINs**.

Onze dos motoristas compartilharam seu veículo com um, ou mais, outro(s) motorista(s). Os outros possuíam seu próprio veículo pessoal, mas alguns deles referiram que em
10 caso de doença, outros poderiam dirigir o veículo e também ocorreu que eles emprestaram seu veículo para alguma outra pessoa.

Simplemente **dois** motoristas poderiam mencionar métodos biométricos sem qualquer assistência a partir do
15 entrevistador. **Dois** não poderiam se entender com qualquer outro método, mesmo que a eles fosse determinada verificação de impressão digital como um exemplo. Nada menos do que **três** motoristas sofreram verificação /
identificação com métodos biométricos e nenhum deles teve
20 nada contra isto. Os únicos que nunca tinham utilizado quaisquer biométricos contabilizaram uma média de **4,20** sobre uma escala a partir de **1** (negativo) até **5** (positivo), com o desvio padrão de **1,42**. Entre eles **onze** foram positivos e todos eles contabilizaram **5**. Um motorista
25 contabilizou **1**, **dois** contabilizaram **2** e o último contabilizou **3**, como nem negativo nem positivo.

Quando questionados sobre possíveis desvantagens para a utilização de métodos de verificação biométricos **seis**
motoristas poderiam ver riscos. Por outro lado, **dois** destes
30 motoristas poderiam também ver possibilidades ou vantagens

para biométricos. **Dez** motoristas poderiam ver somente vantagens e possibilidades. Os **dois** remanescentes não tinham respostas para as questões.

5 **RESULTADOS A PARTIR DO CENÁRIO DE TESTE**

O sistema funcionou bem através de todos os **18** testes. Esta seção irá brevemente discutir o resultado. Poderia ser observado que os resultados meramente discutem quão freqüentemente os participantes foram bem sucedidos com a
10 passagem da verificação. Os autores testaram o sistema brevemente para falsa aceitação. Nem uma única ocasião ocorreu.

A VERIFICAÇÃO INICIAL

15 A verificação inicial consistiu de todos os métodos de verificação implementados. Pelo menos um dos métodos foi bem sucedido para todos os participantes, por conseqüência, todos foram aprovados para dar partida ao motor.

Todos os **18** participantes foram bem sucedidos com a
20 verificação **PIN**. Um discou o código incorreto uma vez, mas foi bem sucedido em sua segunda tentativa.

A verificação de impressão digital foi bem sucedida para **14** participantes. Um destes **14** participantes necessitou de mais do que uma tentativa. Alguns dos
25 participantes foram guiados onde colocar o polegar se o sistema falhasse para encontrar a impressão. (Como descrito aqui anteriormente com respeito à teoria, é um problema comum que o dedo não seja corretamente colocado).

Uma única tentativa foi suficiente para um
30 reconhecimento de rosto bem sucedido para **11** dos

participantes. Um por um, todos os **16** participantes foram bem sucedidos no reconhecimento de rosto.

O reconhecimento de rosto foi simulado e, por conseqüência, todos os participantes passaram, mesmo que
5 alguns deles necessitassem de ser lembrados sobre o que dizer.

Um dos participantes não foi verificado nem pela verificação de impressão digital e nem pelo reconhecimento de rosto, mas foram aprovados na medida em que o **PIN** estava
10 correto. **Dois** dos outros participantes também não foram verificados pela verificação de impressão digital. Nestes casos, o reconhecimento de rosto requereu **duas** tentativas antes que verificações bem sucedidas fossem conseguidas. Tanto o reconhecimento de rosto ou quanto a verificação de
15 impressão digital provocaram problemas enquanto verificando **três** dos participantes remanescentes, entretanto todos eles foram totalmente bem sucedidos na verificação, na medida em que todos os métodos poderiam ser tentados mais do que uma vez cada um.

20

**PRIMEIRA VERIFICAÇÃO ENQUANTO DIRIGINDO
(RECONHECIMENTO DE ROSTO AUTOMÁTICO)**

O sistema automaticamente reconheceu **13** dos participantes. **Dois** daqueles que não tinham sido
25 automaticamente reconhecidos tiveram que discar seus **PINs** na medida em que a verificação de impressão digital falhou como tal.

**SEGUNDA VERIFICAÇÃO ENQUANTO DIRIGINDO (VERIFICAÇÃO DE
30 IMPRESSÃO DIGITAL)**

A verificação de impressão digital foi bem sucedida para **13** dos motoristas, entre eles **10** passaram em suas primeiras tentativas. Os remanescentes passaram a verificação **PIN** em suas primeiras tentativas.

5

RESULTADOS A PARTIR DA ESCALA DE ACEITAÇÃO [DURANTE O INTERVALO (COFFE BREAK)]

As pesquisas que foram respondidas durante o intervalo (*coffe break*) mostraram que o sistema foi percebido como mais útil do que satisfatório. Ver abaixo a contabilidade média para cada participante levando-se em consideração utilidade e satisfação (sobre a escala entre **-2** e **+2**) (Ver **Figura 18**).

Na medida em que a escala é suposta para apresentar **cinco** questões acerca da utilização do sistema e **quatro** questões acerca da satisfação, um cálculo das respostas foi feito para ver se o motorista contabilizou similarmente sobre todas as questões de satisfação e todas as questões de utilidade, respectivamente. *Cronbach's Alpha* foi utilizado para este cálculo. Neste caso as estatísticas de confiabilidade para a escala de aceitação contabilizaram **0,787** para a utilidade e **0,698** para a satisfação, o que indica que os motoristas perceberam as questões como intencionadas.

As opiniões variaram entre os participantes na medida em que todas as questões receberam pelo menos uma graduação máxima e quase todas delas receberam pelo menos uma graduação mínima. Nenhum dos motoristas percebeu o sistema como inútil, mas **três** contabilizaram este em direção a ruim e **três** contabilizaram como nem ruim nem bom. A utilidade

30

contabilizou uma média de **0,80** com um desvio padrão de **0,72** e a satisfação foi contabilizada com uma média de **0,24** com um desvio padrão de **0,89**. Alguns motoristas perceberam o sistema como irritante. Os comentários verbais indicaram que foi especialmente a verificação enquanto dirigindo que despertou irritação. Por conseqüência, o sistema não agradou a todo mundo, mas existiram respostas mais positivas do que negativas.

10 **VERIFICAÇÃO DEPOIS DO CURTO INTERVALO (IMPRESSÃO DIGITAL/VERIFICAÇÃO DE VOZ)**

Os primeiros **dez** participantes utilizaram verificação de impressão digital antes de dar partida ao veículo depois do intervalo. **Nove** destes **dez** foram verificados, **oito** deles em suas primeiras tentativas. O participante que não foi verificado de forma bem sucedida teve que discar seu código **PIN** para ser autorizado. A verificação **PIN** foi bem sucedida na primeira tentativa.

Os **oito** participantes remanescentes utilizaram reconhecimento de voz. Esta verificação foi simulada de maneira que todos passaram, mesmo que alguns motoristas tivessem de ser lembrados pelo líder de teste do que dizer.

25 **TERCEIRA VERIFICAÇÃO ENQUANTO DIRIGINDO (VERIFICAÇÃO DE ROSTO AUTOMÁTICA)**

A verificação automática de forma bem sucedida verificou **15 dos** participantes, **12** deles foram verificados na primeira tentativa. A verificação de impressão digital seguinte foi bem sucedida na primeira tentativa para **dois** dos **três** participantes remanescentes. O terceiro teve que

discar seu código **PIN** na medida em que a verificação de impressão digital falhou como tal. Ele foi verificado de forma bem sucedida por seu código **PIN** na primeira tentativa.

5

QUARTA VERIFICAÇÃO ENQUANTO DIRIGINDO (VERIFICAÇÃO DE VOZ)

A **quarta** verificação enquanto dirigindo foi reconhecimento de voz e na medida em que esta foi simulada, todos os participantes passaram.

10

RESULTADOS A PARTIR DA ENTREVISTA ACOMPANHADA

Esta entrevista questionou questões específicas sobre os diferentes métodos, e bem como questões mais gerais relativas a métodos biométricos e de verificação. Em adição, os motoristas foram questionados sobre a **GUI** e os sons conectados para esta. Tudo isto está apresentado nesta seção e, conseqüentemente, isto foi dividido em partes diferentes.

15

A PRIMEIRA RESPOSTA PARA O SISTEMA

A primeira resposta a partir dos motoristas depois do teste foi primordialmente positiva. **Nove** dos motoristas perceberam o teste como realístico. **Sete** dos motoristas acreditam nisto sendo uma visão do futuro. Um motorista achou o teste não realístico e o motorista remanescente nunca determinou uma resposta especificada para a questão.

20

A GUI E SEUS SONS

Todos os motoristas, mas um, determinaram a

25

30

contabilidade a mais alta **(5)** para a **GUI**. Esta pessoa determinou a graduação **(3)**, por conseqüência, a **GUI** contabilizou uma classificação média de **4,89**. **Doze** dos motoristas perceberam os sons conectados para a **GUI**. "Eu
5 *ainda aprendi as diferenças entre quando está correto e quando está incorreto.*", mencionou um motorista. Na medida em que uma resposta para a questão se foi bom ou ruim possuir sons, os motoristas classificaram isto como uma média de **4,5**, com um desvio padrão de **1,24**. Isto se
10 assemelha como se os motoristas gostassem ou desgostassem dos sons na medida em que **dez** dos **doze** motoristas que perceberam os sons contabilizaram tanto **1** ou quanto **5**. A contabilidade média foi de **3,38**, com o desvio padrão de **1,89**, por conseqüência, é difícil dizer se os sons ajudaram
15 ou perturbaram.

Os motoristas manipularam a **GUI** por sua própria conta e espontaneamente fizeram o que foi suposto que eles fizessem, ainda que a eles não fossem determinadas quaisquer instruções de antemão. Algumas vezes eles estavam
20 impacientes para iniciar e questionaram o supervisor de teste se eles deveriam inserir o cartão, antes da **GUI** ser iniciada, mas nestes casos a primeira mensagem usualmente foi mostrada antes que o supervisor do teste tivesse tempo para responder. Uma pessoa discou erradamente no terceiro
25 dígito, ele então retornou para o supervisor de teste: "*Eu disquei o número incorreto, o que deveria fazer agora?*". O supervisor de teste o encorajou a tentar o que ele sentia ser a coisa certa a fazer, por intermédio do que ele instintivamente utilizou o botão correto para apagar a
30 dígito incorreto e continuar normalmente.

A VERIFICAÇÃO INICIAL

Todos os motoristas acharam a primeira verificação, antes de iniciar a jornada, como sendo fácil. A contabilidade média para fácil de utilizar foi de **4,89** com o desvio padrão de **0,32**. (**Dois** classificaram **4**, o restante classificou **5**). **Dez** dos motoristas acreditaram ser isto razoável para possuir esta verificação. **Um** motorista não sabia se isto era razoável ou estranho. Os **sete** motoristas remanescentes acreditaram ser isto estranho ou um pouco estranho. Sobre a questão de necessidade, a contabilidade média foi de **3,14** com o desvio padrão de **1,80**. Com todas as questões resumidas, esta primeira verificação recebeu a contabilidade média de **3,71**, com o desvio padrão de **0,68**.

15

A VERIFICAÇÃO DE ROSTO AUTOMÁTICA

Quando disseram que uma verificação automática foi realizada utilizando a câmera, a maior parte dos motoristas acreditou que isto é uma boa idéia. Os motoristas que não foram verificados pela câmera e tiveram que fazer a verificação de impressão digital acreditaram que isto é absolutamente razoável. Aqueles que foram verificados sem conhecimento foram na maior parte positivos para a idéia de que se tivessem falhado eles teriam que ter realizado uma verificação de impressão digital.

25

Um dos **quatro** motoristas que o sistema falhou para verificar foi negativo para o sistema. Levando-se em consideração os outros motoristas não foi possível extrair quaisquer conclusões a partir da correlação entre a verificação bem sucedida/verificação falha e a percepção do

30

motorista do sistema. Um deles não tem em mente nem o fato de que o sistema tinha tentado a verificação automática e nem de que ele teve que fazer outras verificações na medida em que o sistema falhou na verificação automática. Ainda um
5 outro mencionou que seria bom se o sistema realizasse a verificação automaticamente, mas se isto não foi bem sucedido, deveria se alertar o motorista para sentar corretamente de maneira que a verificação pudesse ir em frente. A quarta pessoa não gostou de quaisquer das
10 verificações enquanto dirigindo e, por consequência, não gostou da verificação automática também. *"As menores coisas que chegam durante a jornada, são as melhores"*.

A VERIFICAÇÃO DE IMPRESSÃO DIGITAL ENQUANTO DIRIGINDO

15 A primeira verificação enquanto dirigindo, quando os motoristas tiveram que fazer um escaneamento de impressão digital não foi percebida como sendo tão fácil quanto a primeira verificação. A verificação de impressão digital enquanto dirigindo contabilizou **3,19** como a média, com um
20 desvio padrão de **1,67**. Esta verificação se inclinou mais na direção de ser percebida como especialmente estranha do que razoável. Sobre a escala a partir de **1** (estranha) até **5** (razoável) o escaneamento de impressão digital enquanto dirigindo contabilizou em média **2,94** com o desvio padrão de
25 **1,86**. Se esta verificação era necessária ou não contabilizou **3,1** com o desvio padrão de **1,78**. Como uma contabilidade global esta verificação de impressão digital enquanto dirigindo se classificou como **3,19** com o desvio padrão de **0,38**.

**A VERIFICAÇÃO DEPOIS DO INTERVALO (COFFE BREAK)
(IMPRESSÃO DIGITAL/VOZ)**

Depois do intervalo (*coffe break*) os primeiros **dez** motoristas verificaram a si mesmos com suas impressões digitais, os outros **oito** utilizaram verificação de voz. Não importando qual método eles utilizaram, todos os motoristas contabilizaram esta verificação como fácil. Com os **dois** métodos juntamente, esta verificação contabilizou **4,17** em direção de razoável mais especialmente do que estranho, com o desvio padrão de **1,50**. A necessidade foi classificada como **3,78** com o desvio padrão de **1,83**. Com todas as questões incluídas e ambos os métodos adicionados juntamente, esta verificação contabilizou **4,12** com o desvio padrão de **0,68**.

Os únicos que utilizaram verificação de impressão digital depois do intervalo classificaram esta com uma média de **4,60** em direção de razoável, com o desvio padrão de **0,97**. A necessidade foi contabilizada com a média de **4,40** com o desvio padrão de **1,35**. Uma pessoa falhou a verificação de impressão digital e, por consequência, teve que discar seu código **PIN** também. Ele ainda contabilizou **5** em ambos como fácil de utilizar e bem como para achar o sistema razoável, mas ele contabilizou **3** sobre a questão de necessidade.

Os únicos que tiveram que fazer o reconhecimento de voz depois do intervalo contabilizaram uma média de **3,63** com o desvio padrão de **1,92** sobre a questão se esta verificação foi estranha **(1)** ou razoável **(5)**. Esta foi classificada como nem necessária e nem desnecessária na medida em que a média sobre esta questão foi de **3,00** com o

desvio padrão de **2,14**. Alguns dos motoristas tiveram que ser lembrados acerca da senha. Esta foi feita somente para evitar que os participantes descobrissem que esta verificação foi simulada.

5

A VERIFICAÇÃO DE VOZ ENQUANTO DIRIGINDO

A segunda verificação enquanto dirigindo foi simulada, portanto, ela nunca falhou, mesmo que alguns motoristas cometessem pequenos erros quando dizendo a senha. Alguns dos motoristas que não utilizaram a verificação de voz depois da verificação inicial tiveram que ser lembrados acerca da senha. Todos os motoristas que utilizaram a verificação de voz depois do intervalo foram rápidos para responder ao sistema. Esta verificação foi percebida como fácil na medida em que todos os motoristas contabilizaram **5**, sem exceções. Sobre a questão de se isto era razoável ou estranho possuir esta verificação, a classificação média foi de **3,41** com o desvio padrão de **1,84**. Foi levada em consideração a mínima verificação necessária na medida em que esta contabilizou uma média de **2,71** com o desvio padrão de **1,99**. Com todas as questões resumidas, esta verificação contabilizou **3,65**, com o desvio padrão de **1,08**.

15

GENERALIDADES ACERCA DOS MÉTODOS

Quando questionado acerca dos métodos de verificação em geral, como os motoristas se sentiram sobre utilização de verificação de impressão digital, de voz, de rosto ou de código, a verificação de voz contabilizou a média a mais alta com **4,61** e o desvio padrão de **0,66**. Verificação de impressão digital e de voz compartilharam a mais alta

30

classificação para confiança. Estas ambas receberam **4,28** como a contabilidade média. Verificação de impressão digital teve um desvio padrão de **1,23** e verificação de voz de **1,27**. A verificação de rosto contabilizou uma média de **3,67** e verificação de código de **3,72** na questão de confiança. Estas tiveram desvios padrão de **1,61** e **1,60**, respectivamente.

Alguns dos motoristas não gostaram da colocação nem do *scanner* de impressão digital e nem da tela para a **GUI**. Eles não quiseram tirar os olhos da estrada e sugeriram instruções de voz ao invés da **GUI** mais próxima para o volante de direção ou integrada no painel (grupo) de instrumentos. Uma outra sugestão foi a de colocar o *scanner* de impressão digital sobre a lateral direita do assento de motorista.

No final da entrevista, os motoristas foram encorajados a graduar os métodos de verificação testados em suas ordens de preferência, aquele mais preferido como número **um**, o segundo como número **dois** e assim sucessivamente. Metade dos participantes preferiu verificação de impressão digital. Reconhecimento de rosto, reconhecimento de voz e **PIN** foram preferidos por **três** participantes cada. Levando-se em consideração a classificação média para esta contabilidade de preferência, impressão digital foi a mais popular e reconhecimento de rosto veio em segundo lugar, até mesmo reconhecimento de voz não ficou tão para trás. Somente **dois** motoristas mencionaram o cartão. Um achou este ser o segundo melhor método depois de **PIN**, mas o outro meramente o graduou em último, depois de todos os outros métodos. É possível que

os motoristas não perceberam o cartão como um método de verificação na medida em que este foi apresentado como seu cartão de tacógrafo, caso em que isto poderia explicar porque ninguém mais o tenha mencionado.

5 Um dos participantes acreditou na verificação da impressão digital como sendo a menos confiável enquanto ele achou o reconhecimento de rosto como sendo o melhor na medida em que ele nem sempre tem notícia daquela. Um outro participante preferiu impressão digital mesmo que ele
10 percebeu esta como o método o mais difícil para utilização. Ele admitiu reconhecimento de rosto como o método o mais fácil, mas ele não gostou como um todo na medida em que ele se sentiu desconfortável tendo uma câmera em frente a ele.

15 **GENERALIDADES ACERCA DE SALVAGUARDAS DE VERIFICAÇÃO**

Dez dos motoristas deveriam gostar de possuir esta espécie de sistema em seus veículos. Entretanto, somente **dois** motoristas queriam todos os métodos, **oito** dos motoristas pensavam ser suficiente possuir um método de
20 verificação, **um** motorista não queria qualquer método enfim e os motoristas remanescentes fizeram diversas recomendações de mais do que um método, mas nem todos eles. O número médio de métodos desejados no sistema foi de **1,72** com o desvio padrão de **1,32**.

25 **Cinco** motoristas daqueles que antes do teste não viam quaisquer desvantagens em possuir verificações biométricas passaram a ver desvantagens depois do teste. **Quatro** motoristas daqueles que viam desvantagens antes do teste responderam diferentemente depois do teste. **Um** motorista
30 que poderia ver vantagens antes do teste não viu estas

posteriormente ao teste. **Cinco** motoristas poderiam ver vantagens depois do teste que eles não teriam visto antes.

Os **15** participantes que nunca tinham utilizado biométricos antes deste teste foram questionados na primeira entrevista se eles eram positivos (**5**) ou negativos (**1**) para métodos de verificação biométricos. Depois do teste de simulador eles foram questionados novamente acerca do que eles pensavam de métodos de verificação biométricos agora, depois do teste. **Seis** dos participantes contabilizaram mais negativo depois do teste do que antes, **três** participantes contabilizaram mais positivo e **seis** participantes contabilizaram da mesma forma como antes. Estas respostas estão apresentadas no diagrama posteriormente (Ver **Figura 19**).

Levando-se em consideração suas contabilidades **onze** destes **15** motoristas foram positivos para biométricos (contabilizando **4 - 5**), **dois** deles foram negativos (contabilizando **1 - 2**) e **dois** foram nem positivos e nem negativos (contabilizando **3**).

É de se notar que diversos dos participantes mencionaram a si mesmos serem mais positivos depois do teste do que antes do teste, mesmo que eles não proporcionaram um grau mais alto do que aqueles anteriormente.

Na medida em que os participantes foram requisitados depois do teste a contar o que eles tinham contabilizado antes do teste, é assumido que alguns deles mencionaram a si mesmos tendo classificado mais baixo antes do teste do que o que eles tinham efetivamente feito.

Quatro dos participantes foram mais positivos para

possuir biométricos no veículo do que em outras situações. Outros **quatro** pensaram o oposto, que biométricos são bons (OK), mas não no veículo. Os motoristas remanescentes contabilizaram igualmente para biométricos no veículo e para biométricos em geral. Como uma contabilidade média um sistema de verificação no veículo recebeu **3,78** com o desvio padrão de **1,35**. Biométricos em geral contabilizaram em média **3,76** com o desvio padrão de **1,48**.

Diversos motoristas foram positivos para a idéia de um sistema de verificação nos veículos, mas referiram que eles não têm necessidade para isto em seu trabalho diário. O fato de que eles em si mesmos não tenham sido expostos para quaisquer crimes ou ataques foi um comentário freqüente a partir dos motoristas. Eles acreditam que poderia ser mais fácil responder as questões de entrevista se eles fossem forçados a pensar acerca destas salvaguardas. Como eles se sentiam seguros no trabalho eles mencionaram como sendo difícil para eles se referirem aos problemas. **4,3** foram os resultados técnicos gerais.

Esta seção deixou claras algumas observações feitas durante os testes, levando-se em consideração a tecnologia.

O SISTEMA DE VERIFICAÇÃO DE IMPRESSÃO DIGITAL

O sistema de impressão digital funcionou bem através de todos os testes. Em umas poucas ocasiões o sistema se tornou não responsivo, mas isto é mais provavelmente dependente de problemas com o portal de **COM** no **PC** principal do que o sistema *BioCoreII*. Nenhum dos participantes falhou na fase de registro, mesmo se algumas vezes diversas tentativas fossem necessárias de maneira a recuperar uma

imagem suficientemente boa. Todos os participantes foram bem sucedidos pelo menos uma vez com verificação de si mesmos utilizando suas impressões digitais.

5 **O SISTEMA DE VERIFICAÇÃO DE ROSTO**

O sistema de verificação de rosto teve um comportamento mais estável do que aquele para verificação de impressão digital. Nenhum dos participantes falhou no registro de rosto. Entretanto, um dos participantes não
10 pôde ser registrado até que ele tivesse tirado seu boné de beisebol. É possível que o boné sobrepuja sombras sobre seu rosto o que é complicado para o sistema.

Alguns problemas com óculos bem como ocorreram. Isto na medida em que reflexos nos óculos podem torná-los opacos
15 para a câmera. Em uma ocasião, a fase de registro teve que ser repetida na medida em que o reconhecimento de rosto não foi bem sucedido para localizar a posição dos olhos do motorista. Este motorista utilizava óculos e foi também o único a falhar em todas as **três** verificações de rosto
20 durante o teste.

O SISTEMA DE RECONHECIMENTO DE VOZ

O reconhecimento de voz foi somente simulado durante os testes e, conseqüentemente, não é possível dizer
25 qualquer coisa acerca da funcionalidade do sistema.

ANÁLISE E RESUMO DOS RESULTADOS

Os participantes foram mais positivos do que negativos para o sistema de verificação e foram primordialmente
30 positivos para a idéia de utilização de verificação

biométrica em seus veículos. A verificação de impressão digital foi, como mencionado, a única que a maior parte dos participantes preferiu e também contabilizada com o mais alto grau de média. Foi também o método que a maior parte dos participantes conhecia. Aqueles que poderiam dar mais exemplos mencionaram que eles tinham visto coisas em filmes e falaram sobre escaneamento de olhos e reconhecimento de rosto/voz, contudo, pareceu como se até mesmo aqueles que poderiam mencionar outros métodos percebessem aqueles métodos como futurísticos. É possível que o sentimento futurista tenha influenciado suas escolhas de método preferido.

Diversos participantes foram positivos para o reconhecimento de rosto, mas não deve ser esquecido que outros se sentiram controlados pelo sistema e não gostaram da câmera. Um motorista mencionou; *"Eu gosto da liberdade que se tem com este trabalho. Tanto quanto eu percebo como as coisas são, como deveriam ser feitas, eu posso fazê-las da maneira que eu gosto, isto não é da conta de ninguém mais. Com este sistema eu me sinto como se eu não fosse mais quem estava no controle. Foi o sistema que me disse quando eu poderia dirigir ou não"*. Este participante e ainda um outro mencionaram que eles deveriam considerar mudar de emprego se uma verificação de motorista fosse regulamentada. Os participantes remanescentes não foram assim tão drásticos, mas comentaram que eles não estavam acostumados a utilizar um tal sistema como este. Oportunidades de treinamento e informação poderiam reforçar a recepção positiva do sistema.

Um outro exemplo de quando informação é importante

para conseguir aceitação é o de que diversos participantes questionaram a necessidade para verificação enquanto dirigindo. Entretanto, quando o líder de teste e o participante conversaram sobre isto depois das entrevistas e o participante questionou sobre a verificação enquanto dirigindo, o líder de teste deu este exemplo: *"Imagine um motorista de caminhão que foi verificado e deu partida ao motor quando ele viu que uma recusa que necessitava estar atado para a carga. Quando o motorista deixou o coupê para consertar o fio um impostor poderia tomar seu lugar e tentar sair com o veículo"*. Os participantes mencionaram que isto era alguma coisa sobre a qual eles não tinham pensado antes, mas mencionaram que isto acontece que eles descem depois de dar partida ao veículo. Com a explanação de porque o motorista deveria ser verificado enquanto dirigindo, os participantes perceberam isto como razoável, mesmo que eles não quisessem ser perturbados por uma verificação de impressão digital. Reconhecimento de rosto ou de voz foram mais apreciados enquanto dirigindo.

Um sistema de verificação em veículos comerciais deveria ser desenvolvido levando-se em consideração a privacidade dos usuários. Se assim for, este irá ser provavelmente bem recebido na medida em que a maior parte dos participantes foi positiva para a idéia.

25

CONCLUSÕES

O sistema que foi testado é um protótipo e o sistema não é estável o suficiente para utilização na vida real. Com métodos de verificação especialmente adaptados para propósitos automotivos, combinados com um sistema de

30

controle embutido ao invés dos ambos computadores, é provável que um sistema estável, seguro e robusto pode ser conseguido. Verificação automática enquanto dirigindo é recomendada, entretanto, se os problemas com a 5 sensibilidade de iluminação permanecem, reconhecimento de voz parece ser o segundo melhor. Isto na medida em que reconhecimento de voz não requer uma quantidade de atenção a partir do motorista, mas se o método deve ser testado antes é possível mencionar se isto é realmente adequado 10 para utilização em veículo (embarcada).

Verificação de **PIN** é um método que é adequado a partir de uma perceptiva técnica, mas a maior parte dos usuários preferiu verificação biométrica na medida em que o **PIN** é ainda um outro código a ser lembrado. O método funcionou 15 razoavelmente bem enquanto permanecendo parado, mas não é sugerido para utilização enquanto dirigindo na medida em que alguns destes motoristas quase perderam o controle sobre o veículo enquanto discavam o código. O mesmo vale para escaneamento de impressão digital, alguma coisa que os 20 motoristas em si mesmos comentaram.

Como mencionado nos resultados, alguns dos motoristas não gostaram desta colocação do *scanner* de impressão digital, mas ao lado e a partir disto, este método de verificação é rápido e confiável. Se os usuários recebem 25 treinamento, é altamente provável que este poderia ser adequado para o propósito para verificar o motorista de caminhão. Mãos sujas não são supostas provocar quaisquer problemas, na medida em que todos os participantes foram registrados e verificados mesmo que a maior parte deles 30 chegou para o teste diretamente do trabalho (por

conseqüência, uma situação de autenticidade para o escaneamento de dedo como este é similar para se eles devessem ter adentrado seus próprios veículos). O *scanner* deve ser colocado de maneira que é fácil para escanear qualquer um dos dedos da mão direita, ao invés de como foi até agora, quando somente o polegar poderia ser utilizado para verificação. Um *scanner* maior, preferivelmente com direcionadores para o dedo encontrar a posição correta, deveria facilitar a verificação para os usuários. Mesmo que a verificação de impressão digital fosse preferida entre os participantes de teste, este não deveria ser o único método em um sistema de verificação na medida em que nem todas as pessoas possuem impressões digitais suficientemente distintas para escaneamento.

A tecnologia de reconhecimento de rosto ainda não está amadurecida para estes tipos de aplicações na medida em que esta é muito sensível à luz. Entretanto, a verificação de rosto contabilizou alta e a parte primordial dos motoristas foi positiva para a verificação automática. Isto indica que a verificação de rosto é preferida, observada a partir de perspectivas de usuários. Deveria ser importante assegurar aos motoristas que eles não estavam constantemente sob vigilância, na medida em que alguns dos motoristas se sentiram desconfortáveis encarando uma câmera durante a integridade da jornada. Como este equilíbrio entre o controle do motorista e sua privacidade deve ser encontrado é ainda deixado para investigação adicional.

Diversos dos motoristas foram positivos para o sistema de reconhecimento de voz, mas na medida em que este foi simulado para ser bem sucedido em todas as vezes não é

possível extrair quaisquer conclusões sobre como este deveria efetivamente se adaptar no contexto de caminhão. Especialmente na medida em que muitos motoristas não confiavam neste no começo, devido para experiências ruins com sistemas similares de reconhecimento de voz, esta 5 verificação falseada determinou a eles uma falsa confiança.

As percepções dos motoristas de se os sons da **GUI** ajudaram ou exatamente perturbaram variaram enormemente. É, conseqüentemente, sugerido que o usuário deveria ter a 10 capacidade de ligar/desligar o som.

O pior ceticismo entre os contratadores de transporte interrogados foi contra a tecnologia. "*E se isto falhar?*" foi uma questão rotineira. A maior parte deles poderia também ver problemas se alguma coisa acontecer para o 15 motorista, um acidente, ou alguma outra coisa, que o impeça de movimentar o veículo. "*Tem que existir uma maneira para movimentar o veículo de alguma maneira*". Também os participantes de teste enfatizaram a importância de uma solução para movimentação do veículo em caso de acidentes. 20 Adicionalmente, os participantes de teste demandaram para possibilidades de trocar o motorista do veículo com curta notificação. Soluções possíveis para estes problemas estão discutidas na seção **6.10**, Aspectos automotivos.

Para resumir os resultados, é considerado ser possível 25 criar um sistema de verificação adequado para um ambiente automotivo. Ainda, não deve ser esquecido que é quase impossível se eliminar todos os riscos. O **IRA**, por exemplo, exclusivamente utiliza pessoas que são desconhecidas para as autoridades para quaisquer operações maiores. Uma tática 30 que é rotineira em muitos ataques terroristas, se este é um

homem-bomba suicida ou um seqüestrador de uma aeronave. Ainda um outro exemplo é o de que diversos dos terroristas que executaram o ataque contra o *World Trade Center* utilizaram suas próprias identidades. Conseqüentemente, mesmo que de qualquer forma todos os motoristas devessem ser verificados, deveria ser impossível assegurar que seus veículos nunca devessem ser utilizados em quaisquer ações terroristas. Existem numerosos exemplos de quando o indesejável ocorre a despeito das precauções tomadas. Contudo, um sistema de verificação em um caminhão deveria provavelmente intimidar impostores e terroristas, o que deveria beneficiar tanto o motorista e quanto o contratador de transporte de longa distância e toda a sociedade.

15 **FUTUROS ESTUDOS**

As descobertas aqui discutidas proporcionam uma quantidade de inspiração para adicionalmente cuidar para os muitos diferentes aspectos da idéia e das possibilidades com verificação de motorista. Muitas questões apareceram durante o processo de trabalho, mas não foi possível dentro de tempo razoável responder todas as questões dentro deste pedido de patente. Este sistema simulado e as entrevistas proporcionaram uma idéia das opiniões dos motoristas, contudo, é importante testar o sistema sob condições de mais autenticidade. Por conseqüência, para futuros estudos é sugerido implementar o sistema em um caminhão real e testá-lo. Abaixo, está uma lista de diferentes questões em salvaguarda que também têm que ser consideradas.

Na medida em que alguns motoristas estavam desconfortáveis com a colocação do sensor, deveria ser interessante encontrar uma melhor colocação.

O sistema tem que ser testado sob condições de autenticidade de maneira a investigar como sujeira, cicatrizes, calosidades e etc., afetam o desempenho do sistema.

RECONHECIMENTO DE ROSTO

10 Para futuros estudos é sugerido montar o sistema em um caminhão real e testá-lo sob condições de autenticidade. Durante o teste, o motorista deveria ser filmado e as condições de luz no coupê deveriam ser mensuradas de maneira a testar sob quais circunstâncias o sistema é
15 funcional. Estes testes deveriam ser complementados com entrevistas aprofundadas com os usuários para ver como eles se adapta a usuários para se ter uma câmera no interior do coupê. Isto é uma salvaguarda importante na medida em que alguns dos motoristas estavam desconfortáveis tendo a
20 câmera os encarando durante o teste, enquanto outros não se preocuparam em nada e estavam muito satisfeitos com a idéia da verificação automática. Um tal sistema poderia necessitar de restrições para como ele pode ser utilizado, por conseqüência, poderia ser necessário criar novas leis
25 para estas circunstâncias de vigilância por câmera.

Quando termografia se tornar mais desenvolvida deveria ser considerado utilizar este método no sistema de verificação. O método deveria então necessitar ser testado durante diferentes circunstâncias de troca de turnos do
30 dia, preferivelmente em um caminhão real.

No limite entre os intervalos de comprimento de onda de luz visível e de luz infravermelha, o assim chamado intervalo de **NIR** (*Near Infra Red* - Infra Vermelho Próximo) pode ser encontrado. O problema com termografia de rosto é o de que não existe sistema de verificação viável disponível no mercado, pode ser problemático utilizar reconhecimento de rosto rotineiro na medida em que este é sensível às condições de luz. Pela utilização de uma câmera de **NIR** poderia ser possível solucionar ambos estes problemas, na medida em que o rosto do motorista pode ser iluminado com diodos de **NIR**, invisíveis para ele, mas não para a câmera de **NIR**.

15 **RECONHECIMENTO DE VOZ**

Primeiro de tudo é desejável testar um sistema de verificação de voz funcionando. Se os resultados são satisfatórios, o sistema deveria ser testado para robustez em um caminhão real. Isto na medida em que o nível de ruído no simulador não varia particularmente. Ruídos podem freqüentemente ser removidos por filtragem e o sistema *VoiceKey* se adapta (dentro de limites razoáveis) para o nível efetivo de ruído. Mas tem que ser testado se as variações de ruído em um caminhão estão dentro destes limites.

Na medida em que poderia ser sentido desajeitado para o motorista falar alto diretamente para o ar, poderia ser necessário implementar um microfone próximo do assento do motorista. Se o microfone está equipado com um interruptor de força, os motoristas podem sentir que eles estão no

controle de quando o sistema pode "aquecer" (incomodar) a eles. Ao lado do sentimento desajeitado que alguns motoristas mencionaram durante o teste, este parece ser um método adequado para utilização enquanto dirigindo. Se as 5 instruções forem determinadas excessivamente autoritárias poderia parecer mais natural para o motorista realizar a verificação de voz como se fosse mais uma conversa entre ele e o sistema.

Deveria ser interessante implementar uma **GUI** com 10 somente as fotografias e os sons, juntamente com instruções faladas a partir do sistema ao invés do texto que foi utilizado neste protótipo. Deveria ser possível para o motorista desligar/ligar as instruções de voz e os sons de maneira que cada indivíduo poderia possuir o sistema que 15 melhor se adequasse a ele.

AÇÕES ADEQUADAS EM DIFERENTES SITUAÇÕES

O que deveria acontecer quando o motorista tivesse verificado sua identidade? Existem diversos cenários 20 possíveis levando-se em consideração a verificação e os eventos que se seguem e estes estão discutidos mais nos casos de utilização aqui posteriormente.

Uma salvaguarda que deve que ser considerada e discutida é; o que deveria acontecer se a verificação não 25 for bem sucedida de qualquer forma? Considerando a verificação inicial (antes de dar partida ao motor), existem primordialmente **quatro** possibilidades; é impossível dar partida ao veículo; é possível dar partida ao veículo e dirigir o veículo como usualmente, mas depois de alguma 30 distância ela desacelera para velocidade de passeio sem

possibilidades adicionais de aumentar a velocidade; se tem capacidade de dar partida ao veículo e dirigir como usualmente, mas um alarme é enviado para o proprietário, deixando para ele tomar as precauções apropriadas; a
5 verificação falha é logada (*logged*) embarcada no veículo, mas nenhuma ação adicional é tomada.

É sempre difícil avaliar as diferentes situações uma contra a outra. Se o veículo se movimenta mesmo se o motorista não é aquele apropriado, ou nem mesmo um
10 motorista autorizado, o risco que o veículo poderia estar sendo utilizado para propósitos indesejados aumenta.

Ainda, se for impossível movimentar um veículo sem um motorista autorizado o alto risco para roubar veículos com o motorista dentro aumenta. Se a sociedade ou o motorista
15 quisesse, a mais alta prioridade poderia se alterar dependendo da espécie da carga que o veículo está transportando e também de onde o veículo está situado no momento da verificação falha.

O que deveria ser feito se o motorista falha para
20 verificar sua identidade durante a jornada? Esta questão foi também discutida durante este processo, mas para se obter respostas adequadas diversos testes têm que ser conduzidos. As possibilidades são completamente as mesmas como as situações anteriormente com a modificação de que
25 nos primeiros **dois** exemplos o veículo pára ou desacelera para velocidade de passeio, respectivamente.

QUANDO A VERIFICAÇÃO DEVERIA ACONTECER

Quando demandar verificação é também uma salvaguarda
30 importante. Se a imaginação é deixada viajar livremente

existem cenários possíveis ilimitados e em algum lugar a linha irá ser delineada. Os autores sugerem que o motorista tem que verificar sua identidade mais uma vez quando as portas fossem abertas e o sensor de assento informa que
5 alguém tomou o assento de motorista. O sensor de assento é o único disparando o sinal de aperto de cinto de segurança e a maior parte dos caminhões possui sensores verificando se as portas estão devidamente fechadas de maneira que deveria ser razoavelmente fácil de implementar.

10 Se for desejado verificar a identidade de motorista enquanto dirigindo, o que freqüentemente deveria ser feito? Nas nossas pesquisas, motoristas de transporte de longa distância nos disseram que eles algumas vezes dirigem no máximo **4,5** horas em uma fileira (em um comboio) e algumas
15 vezes fazem **oito** paradas em uma viagem de **duas horas**. O tempo ou distância dirigida entre as paradas tem que ser considerado, avaliando proteção e conveniência uma contra a outra.

É sugerido que a demanda para verificação não deveria
20 ser excessivamente elevada freqüentemente na medida em que isto poderia ser perturbador para o motorista. Além do mais, se o motorista pára para carregamento / descarregamento, é altamente provável que ele desça do veículo e se assim for, verificação tem que acontecer antes
25 de partir novamente.

O ideal deveria ser se a verificação enquanto dirigindo pudesse ser realizada sem nenhuma ação tomada a partir do motorista, como no caso com reconhecimento de rosto automático. Mas, então como tal, a verificação não
30 deveria ser excessivamente elevada freqüentemente, devido

para o fato de que se a verificação automática falha, o motorista tem que ser verificado de alguma outra maneira.

POSSIBILIDADES ADICIONAIS

5 É possível possuir ainda mais níveis de proteção do que aqueles que foram feitos para este protótipo. Se o sistema de verificação possui informação acerca da carga e em que área geográfica o veículo está operando, o sistema pode ajustar o nível de proteção automaticamente. Por
10 exemplo, um transporte de ouro em *Cape Town* demanda um nível de proteção mais alto do que quando entregando calcário para um sitio de construção em *Laplander Forest*.

 Como sugerido nos casos de utilização, um sistema de modo múltiplo pode requerer somente um método biométrico
15 para verificação. Método no qual se é requerido se selecionar randomicamente de maneira que o motorista necessita todos eles registrados, mas somente utiliza um de cada vez. Com esta randomização um impostor pode não ter certeza do que ele necessita para verificação e ele irá
20 possuir uma quantidade de trabalho para preparar uma falsa amostra de todas as diferentes características.

 Um outro beneficio quando os diferentes métodos são randomicamente testados é o de que o motorista irá estar mais bem habituado do que se ele somente utilizasse um
25 método o tempo todo e então repentinamente tenha que trocar, devido para a perda de um dedo ou alguma coisa menos drástica.

 Isto deveria também proporcionar a possibilidade para atualizar um gabarito na base de dados se a verificação foi
30 um sucesso total. Para ilustrar um exemplo; imagine que o

motorista recentemente foi verificado utilizando seu cartão, o **PIN** e sua impressão digital. Se após isso todos estes métodos são bem sucedidos, o sistema poderia tirar uma nova foto do rosto para atualizar o registro. Isto pode
5 facilitar a verificação se um motorista está, por exemplo, com a barba crescida ou tenha somente se barbeado, ou se o motorista ganhou ou perdeu peso desde o registro.

Uma idéia que veio neste estágio foi a de combinar escaneamento de geometria de mão com escaneamento de
10 impressão digital. A resolução das câmeras digitais de hoje em dia é alta o suficiente para capturar uma imagem suficientemente detalhada da palma da mão, de maneira a analisar tanto mensurações de dedos e bem como impressões digitais.

15

COLOCAÇÃO DE BASE DE DADOS E ADMINISTRAÇÃO DE SISTEMA

Na medida em que todos os métodos descritos requerem uma base de dados para armazenar os gabaritos originais que são criados durante o processo de registro, estudos
20 levando-se em consideração a colocação da base de dados têm que ser realizados. Esta base de dados é necessária para a comparação durante a verificação. No protótipo a base de dados foi armazenada em um computador próximo para a cabine; na realidade existem basicamente **três** colocações
25 diferentes a serem consideradas; escritório de apoio (*back-office*); em veículo (embarcada); cartão inteligente.

Qual colocação que é a melhor depende de diversos parâmetros e deve de ser considerada de caso a caso. Uma coisa é completamente clara, se o sistema é utilizado para
30 prevenir que pessoas não autorizadas venham a dar partida

ao veículo, a comunicação entre o dispositivo biométrico e a base de dados nunca deve (não pode) falhar. Isto na medida em que de outro modo, um motorista autorizado pode ser imobilizado no meio do nada devido para problemas de comunicação entre o veículo e a base de dados.

COLOCAÇÃO DE ESCRITÓRIO DE APOIO (BACK-OFFICE)

Colocação de escritório de apoio significa que a base de dados de gabarito está colocada em um computador, por exemplo, no escritório do contratante de transporte.

Um sistema de verificação pode necessitar de atualização em tempo real e, portanto, uma ligação (*link*) entre o veículo e a base de dados é requerida. Se um motorista está doente e alguma outra pessoa toma aquela assinatura o sistema tem que ser atualizado para aceitar o novo motorista como aquele apropriado. Como mencionado anteriormente, o governo dos Estados Unidos da América quer evitar que pessoas na base de dados do **FBI** venham a dirigir caminhões transportando mercadorias perigosas. A base de dados do **FBI** muda, por conseqüência, atualização em tempo real para o sistema de verificação deveria ser desejada.

COLOCAÇÃO EM VEÍCULO (EMBARCADA)

Colocação em veículo é quando os gabaritos são colocados em um computador no caminhão. Isto limita os problemas provocados pela comunicação sem fio, mas ao invés da proteção contra roubo ou invasão de sistema não irá ser tão forte quanto com a colocação de escritório de apoio. Esta é a solução a mais simples, mas também provavelmente a mais dispendiosa na medida em que isto demanda uma base de

dados em cada veículo.

COLOCAÇÃO DE CARTÃO INTELIGENTE

Colocação de cartão inteligente se refere para quando
5 os gabaritos são armazenados em um cartão inteligente, que
o motorista pode levar com ele quando deixando o veículo.
Isto aumenta a proteção na medida em que o motorista também
necessita trazer o cartão inteligente para passar no
sistema. Ao lado disto, o fato de que o motorista em si
10 mesmo carrega seus gabaritos biométricos pode aumentar sua
sensação de privacidade.

Um benefício se a base de dados é mantida tanto em um
cartão ou quanto no escritório de apoio é o de que isto não
está ligado para um veículo específico. Se um motorista
15 necessitar trocar de veículo devido a uma falha de motor e
etc., isto não irá ser um problema na medida em que todos
os motoristas podem dirigir todos os veículos, devido ao
fato de que eles carregam seus próprios cartões
inteligentes e estão registrados na base de dados. Observe-
20 se que uma atualização dinâmica da base de dados irá ser
muito importante.

A partir de **5** de agosto de **2005** todos os veículos
novos, dentro de toda a União Européia, têm que ser
equipados com um tacógrafo digital. Tacógrafos de hoje em
25 dia são simples discos de papel e não é raro que os dados
sejam manipulados. O tacógrafo digital é um cartão
inteligente que automaticamente registra dados, tais como
velocidade e tempo dirigido entre as paradas. O cartão
inteligente torna muito mais complicado para os motoristas
30 manipularem os dados registrados e na jornada longa o

tacógrafo digital é intencionado para ser padrão (*standard*) para todos os veículos. O tacógrafo digital abre possibilidades para integração com o cartão inteligente biométrico que pode ser utilizado para os gabaritos. Desta
5 maneira, o motorista somente necessita de um cartão, mas tanto os parâmetros do veículo e quanto os gabaritos para verificação irão ser armazenados juntamente. Isto poderia ser uma maneira de adicionalmente aumentar a proteção ainda adicionalmente na medida em que irá ser assegurado que os
10 dados a partir do tacógrafo pertençam ao motorista (assumindo que ele tenha sido verificado).

Se o motorista perde seu cartão, isto abre a possibilidade para que um impostor venha a registrar a si mesmo e armazenar (salvar) seus gabaritos no cartão. Isto
15 irá, entretanto, ser difícil na medida em que ele não somente necessita conhecer quais métodos são utilizados. Ele tem que também conhecer a estrutura dos gabaritos e ter a capacidade de conseguir passar os dados criptografados embutidos no cartão. De maneira a armazenar alguma coisa no
20 cartão, ele tem que também ter conhecimento do sistema de operação daquele cartão específico. Os sistemas de operação variam enormemente de fabricante para fabricante.

ADMINISTRAÇÃO DO SISTEMA

25 Relacionado para a discussão acerca da colocação de base de dados estão reflexões sobre como administrar o sistema. Alguns contratantes de transporte possuem um grande número de veículos e de motoristas e se o sistema não tem habilidade para administrar, eles poderiam ser
30 forçados a recrutar pessoal adicional unicamente para

administrar o sistema de verificação. Neste sentido, colocação em veículo (embarcada) da base de dados não é sugerida. Isto na medida em que cada motorista tem que tanto ser registrado em cada veículo que ele deveria 5 dirigir, ou quanto seus gabaritos devem ser baixados (*downloaded*) naqueles veículos.

Com a colocação de escritório de apoio da base de dados de gabarito, uma alternativa deveria ser baixar (*download*) os gabaritos temporariamente para uma memória no 10 veículo de maneira a fazer o emparelhamento (a comparação). A outra alternativa é a de enviar os gabaritos escaneados durante verificação para o escritório de apoio para emparelhamento. Isto não é sugerido devido para o risco de que o veículo venha a adentrar uma área com recepção (de 15 sinal) insuficiente, ou para a possibilidade de que a conexão sem fio esteja corrompida. Ainda que se for mencionado que deveria ser impossível recriar as características efetivas a partir do gabarito, poderia ser desconfortável para o usuário saber seus gabaritos 20 biométricos são enviados para fora.

Se os gabaritos estão armazenados em um cartão, por exemplo, o tacógrafo digital estes problemas não ocorrem. Ao invés disso, existe um risco de que o motorista venha a perder seu cartão. Entretanto, é proibido dirigir o veículo 25 sem o cartão de tacógrafo inserido e, conseqüentemente, é provável que o motorista irá tomar cuidadosamente conta de seus cartões.

TELEMÁTICAS

30 Para possibilitar que o sistema venha a se comunicar

com o escritório de apoio, telemáticas são requeridas. A maior parte dos caminhões de hoje em dia são equipados com alguma espécie de sistema de comunicação. Este pode ser qualquer coisa a partir da comunicação de rádio analógica
5 fundamental para sistemas avançados. Na medida em que o enfoque aqui é o sistema de verificação em si mesmo, é simplesmente assumido que é possível transferir dados entre o caminhão e o escritório.

É sugerido enviar nome, **ID** de empregado e informação
10 sobre o resultado das diferentes verificações para o escritório de apoio. O risco de uma conexão corrompida sugere que nem os gabaritos nem informação excessiva acerca do motorista (por exemplo, número de seguridade social) deveriam ser enviados.

15 Uma outra recomendação, devido para o risco de uma conexão corrompida, é a de enviar a informação em um estilo criptografado para reduzir o risco de que a informação venha a cair em mãos erradas. Existem numerosos produtos no mercado para criptografar dados. A maior parte dos sistemas
20 processa os dados em concordância com uma chave criptografada. Os dados são após isso enviados para o receptor que possui uma idêntica chave criptografada para decodificar a informação.

25 **DISTRIBUIÇÃO DE INFORMAÇÃO**

Para onde deveriam os dados ser enviados e para quem? Ao proprietário do caminhão pertence a informação, mas existem outros atores que poderiam querer fazer parte disto. Tais atores podem, por exemplo, ser as companhias de
30 seguro, a associação nacional de estradas, a polícia e o

serviço de bombeiro e de resgate (serviço de salvamento). De quem deveria ser a responsabilidade de atualizar, armazenar e distribuir a informação tem que ser considerado.

5

ASPECTOS AUTOMOTIVOS IMPORTANTES

Existe um número de cenários complicadores que podem ocorrer para a perspectiva automotiva, por exemplo:

- 10 - Se o veículo é utilizado para aluguel, tem que ser fácil registrar e bem como remover pessoas a partir do sistema. Um benefício pode ser o de que a companhia de aluguel possa ter certeza de que o veículo é somente dirigido pela pessoa registrada no estande de vendas.
- 15 - Se o veículo está emprestado para alguém, um fácil *bypass* (alternativa) ou procedimento de registro/remoção é requerido.
- Se o veículo está em necessidade de serviço de oficina, tem que existir uma maneira simples de *bypassing* (contornar) o sistema ao invés de registrar os mecânicos na oficina. Uma solução possível poderia ser a de permitir que o caminhão venha a se movimentar, por exemplo, a **5 Km/h** sem o cartão de tacógrafo ou qualquer outra verificação.
- 20
- 25 - Se o motorista está ferido ou de qualquer outra maneira incapacitado de dirigir o veículo, tem que existir uma maneira de movimentar o veículo em caso de emergência. A solução poderia ser como sugerida no cenário precedente.
- 30 - Se o veículo for vendido para alguém sem a

necessidade do sistema de verificação, tem que ser possível remover o sistema de verificação.

5 - A manipulação do veículo durante nanufatura ou transporte é também um problema para considerar. Isto pode ser solucionado de uma maneira similar como durante o serviço de oficina.

Estes aspectos têm que ser considerados completamente antes de permitir que o sistema venha a sair do mercado. Também se o sistema biométrico for substituído, a chave de ignição para dar partida ao motor, a maneira de manipular 10 suprimento elétrico, a partida de motor e tranca da direção têm que ser levados em consideração.

15 **JULGAMENTO (CRITICISMO) DE MÉTODO**

Na primeira pesquisa de motorista os documentos foram distribuídos em uma parada de caminhão. Os motoristas foram questionados se eles poderiam responder algumas questões acerca de seu trabalho e das possibilidades para um sistema 20 de verificação de motorista. Existe um risco de que somente aqueles que foram fortemente contra isto ou muito positivos quisessem responder enquanto que o restante não desse importância o suficiente para perder tempo para responder as questões.

25 O mesmo acontece para os documentos que foram distribuídos em um contratante de transporte em *Gothenburg*. Somente a metade dos documentos distribuídos retornou, o que conduz para as questões; quem escolheu responder/não responder, e por quê? Estes documentos foram deixados com 30 uma instrução para um empregado no escritório. Se

existissem quaisquer questões, os motoristas não tinham ninguém para responder acerca informação/explicações adicionais.

5 A seleção tanto de métodos e quanto de equipamento foi limitada pelo tempo insuficiente e bem como pela consolidação, e é, conseqüentemente, duvidoso se o equipamento utilizado é o melhor dos sistemas disponíveis. Adicionalmente, o *software* foi implementado por um programador relativamente sem experiência e isto pode ter
10 afetado o desempenho do sistema.

O simulador foi, como precedentemente estabelecido, não perfeitamente adequado para o cenário e devido para o fato de tempo insuficiente, não foi possível fazer quaisquer ajustamentos. Alguns dos participantes fizeram
15 comentários levando em consideração seus comportamentos. Isto pode ter afetado seus julgamentos acerca do sistema de verificação. O resultado da testagem teria sido provavelmente mais correto se o simulador tivesse sido de mais autenticidade.

20 O cenário foi mais especialmente intensivo com **seis** verificações em cerca de **30 minutos**. Deveria ter sido melhor ter feito um teste mais longo, mas isto não foi possível devido para o fato das limitações em tempo.

É possível que os motoristas que escolheram participar
25 do teste estivessem particularmente interessados na nova tecnologia e, conseqüentemente, mais positivos do que a média de motoristas de caminhão. É possível que todos os participantes não proporcionaram exatamente a mesma informação durante a fase de registro e isto poderia ter
30 afetado seus comportamentos.

Durante o registro, os participantes foram questionados para abaixar o volante de direção de maneira a obter uma tomada limpa com a câmera de reconhecimento de rosto. Durante o teste, alguns deles levantaram o volante de direção novamente enquanto dirigindo. Não foi possível abortar o teste daquela vez. Isto poderia ter afetado o desempenho do sistema de verificação de rosto.

Muitas palavras e abreviações utilizadas neste pedido de patente podem ser desconhecidas para o leitor e, conseqüentemente, nós listamos as de ocorrência mais rotineiramente.

Antropometria: O estudo de mensuração do corpo humano para utilização em classificação e comparação (antropológica).

Automotivo: Uma expressão genérica para tecnologia conectada para a indústria de veículos.

Biométrico: Uma expressão genérica para métodos utilizando análise das características de corpo únicas do sujeito.

Dielétrico: Dielétricos são materiais de isolamento com diversas propriedades.

ECG: Abreviação para Eletrocardiograma. Mensuração de sinais elétricos no coração.

FAR: Abreviação para Taxa de Autenticação Falsa (*False Authentication Rate*). Indica quão freqüentemente o sistema toma um impostor por um usuário autorizado. **FAR** e **FRR** (observadas posteriormente) estão fortemente correlacionadas; alta **FAR** implica em baixa **FRR** e vice-versa.

5
10 **Forense:** Expressão genérica utilizada para coisas associadas com investigações para crime e justiça.

FRR: Abreviação para Taxa de Rejeição Falsa (*False Rejection Rate*). Indica quão freqüentemente o sistema rejeita um usuário autorizado. **FRR** e **FAR** (observadas anteriormente) estão fortemente correlacionadas; alta **FRR** implica em baixa **FAR** e vice-versa.

15
20 **IR:** Abreviação para Infravermelho (*Infrared*). Luz com maior comprimento de onda do que luz vermelha visível, portanto, invisível para o olho humano.

25 **Minúcias:** Características especiais de uma impressão digital, por exemplo, extremidades de sulcos ou divisão em duas.

Mock-up: Partes, tipicamente ambiente de motorista, de um veículo colocadas em um laboratório para propósitos de simulação e testagem.

5

NIR: Abreviação para Infravermelho Próximo (*Near Infrared*).

10

Oximetria: Oximetria de pulso é um método não evasivo simples de monitoramento da porcentagem de hemoglobina (**Hb**) que está saturada com oxigênio.

15

Permissividade: Uma mensuração de quanto um meio muda para absorver energia quando submetido a um campo elétrico.

20

PIN: Abreviação para Número de Identificação Pessoal (*Personal Identification Number*).

Sulco: As linhas delimitadoras de uma impressão digital.

25

Cartão inteligente: Um processador codificado seguro fino embutido dentro de um cartão de dimensão de cartão de crédito ou cartão ainda menor. Um exemplo são cartões **SIM** para telefones celulares **GSM**.

30

TER: Abreviação para Taxa de Erro Total (*Total Error Rate*), a soma de **FAR** e **FRR**.

5 **Termografia:** Mensuração de diferenças de calor utilizando uma câmera de **IR**.

Vale: As depressões entre os sulcos de uma impressão digital.

10

TABELAS DE ANÁLISES DE SWOT

Figura 20 - Impressões digitais como método de verificação.

15 **Figura 21 -** Escaneamento de íris como método de verificação.

Figura 22 - Verificação de voz como método de verificação.

20 **Figura 23 -** Reconhecimento de rosto como método de verificação.

Figura 24 - Termografia de rosto como método de verificação.

Figura 25 - Escaneamento de retina como método de verificação.

25 **Figura 26 -** Escaneamento de movimentação labial como método de verificação.

Figura 27 - Reconhecimento de geometria de mão como método de verificação.

30 **Figura 28 -** Escaneamento de senhas e de **PIN's** como método de verificação.

Figura 29 - Cartões como método de verificação.

Figura 30 - **RFID** como método de verificação.

Figura 31 - Estatísticas a partir da Escala de Aceitação de *van der Laans* (*van der Laans Acceptance Scale*).

5

VERIFICAÇÃO DE MODO MÚLTIPLO UTILIZANDO TODOS OS MÉTODOS BIOMÉTRICOS

10

Caso de utilização: verificação de modo múltiplo no nível de proteção o mais alto (todos os métodos biométricos).

Referência:

15

Propósito: Verificação é feita para assegurar que o motorista é aquele apropriado. O motorista utiliza todos os métodos biométricos disponíveis para verificação devido ao fato de que o veículo está classificado com o nível de proteção o mais alto.

20

Atores: O Sistema de Verificação, o Motorista, o Escritório de apoio (*Back-office*).

25

Pré-condições: O veículo está bloqueado, ou recentemente desbloqueado.

FLUXO PRIMORDIAL DE EVENTOS

Um motorista adentra o veículo e vira a chave, em consequência do que o sistema demanda para verificação

30

utilizando diversos métodos para assegurar que aquele é o motorista apropriado. O motorista começa pela verificação de si mesmo com um dos métodos, após isso ele continua com o próximo, e o próximo, até que a verificação esteja
5 completada. Quando o motorista está verificado, a informação é enviada, criptografada, para o escritório de apoio (*back-office*) e o motorista pode sair com o veículo.

FLUXO ALTERNATIVO DE EVENTOS

10 Um motorista adentra o veículo e vira a chave, em consequência do que o sistema demanda para verificação utilizando diversos métodos para assegurar que aquele é o motorista apropriado. O motorista não é bem sucedido com um ou mais dos métodos de verificação. Depois de **três** falhas
15 com um método, a verificação continua com os outros métodos (ou termina sem o último método se aquele foi o único a falhar). Pelo menos um dos métodos é bem sucedido e a informação é enviada, criptografada, para o escritório de apoio (*back-office*), e o motorista pode sair com o veículo.
20 Juntamente com a informação verificada acerca do motorista, o escritório de apoio também recebe informação acerca da verificação falha.

FLUXO ALTERNATIVO DE EVENTOS

25 Um motorista adentra o veículo e vira a chave, em consequência do que o sistema demanda para verificação utilizando diversos métodos para assegurar que aquele é o motorista apropriado. O motorista não é bem sucedido com o primeiro método de verificação, depois de **três** falhas o
30 sistema continua com o próximo método. Nenhum dos métodos é

bem sucedido, em consequência do que um alarme é imediatamente enviado para o escritório de apoio (*back-office*).

5 **REQUERIMENTO ESPECIAL**

O sistema deveria receber informação quando uma pessoa desbloqueia (destrava) as portas. O sistema necessita de telemáticas para ter a capacidade de enviar a informação entre o veículo e o escritório de apoio (*back-office*).

10

Exemplo 1

O motorista chegou à garagem para começar o dia de trabalho. Na medida em que ele adentra o veículo ele insere seu cartão inteligente (integrado no cartão para o tacógrafo) no leitor, disca seu código **PIN** e após isso coloca seu dedo sobre o *scanner*. O **PIN** está correto e o dedo é verificado contra o cartão, de maneira que o sistema questiona por uma amostra de voz. O motorista diz sua senha no microfone. Uma mensagem de sistema aparece, dizendo para 15 o motorista sentar em uma posição de dirigir normal, de maneira a desempenhar a verificação de rosto. Dados registrados são analisados e comparados com os dados de gabarito armazenados no cartão inteligente - a verificação foi bem sucedida. O nome e número de identificação de 20 empregado são enviados, criptografados, para o escritório de apoio (*back-office*).

Exemplo 2

O motorista chegou à garagem para começar o dia de 30 trabalho. Na medida em que ele adentra o veículo ele insere

seu cartão inteligente (integrado no cartão para o tacógrafo) no leitor, disca seu código **PIN** e após isso coloca seu dedo sobre o scanner. Ele tenta verificar sua identidade pela sua voz, mas isto falha tendo em vista que ele pegou um resfriado hoje. Um sinal informa ao motorista acerca da verificação falha. O procedimento continua com verificação de rosto bem sucedida. O nome e número de identificação de empregado são enviados, criptografados, para o escritório de apoio (*back-office*), juntamente com informação acerca da identificação de voz falha.

Exemplo 3

Ao longo de uma viagem de transporte de longa distância, o motorista tira uma soneca no coupê. Na medida em que ele desperta, ele vai para fora para esticar suas pernas antes de continuar sua jornada. A porta de passageiro se abre e um impostor sobe e toma o assento de motorista. O impostor tenta dar partida ao veículo, mas não é bem sucedido com a verificação, por conseqüência, o veículo é imobilizado. Um alarme é imediatamente enviado para o escritório de apoio (*back-office*), e o sistema tira uma fotografia da pessoa atrás do volante de direção. Esta fotografia é também enviada para o escritório de apoio (*back-office*).

VERIFICAÇÃO DE MODO MÚLTIPLO UTILIZANDO DOIS MÉTODOS BIOMÉTRICOS

Caso de utilização: Verificação de modo múltiplo em nível de proteção médio (**duas**

características biométricas).

Referência:

Propósito:

Verificação é feita para assegurar que o motorista é aquele apropriado. Para se acomodar para a classificação do veículo, nível de proteção médio, o motorista verifica sua identidade utilizando **duas** características biométricas.

5

Atores:

O Sistema de Verificação, o Motorista, o Escritório de apoio (*Back-office*).

10

Pré-condições:

O veículo está bloqueado, ou recentemente desbloqueado.

15

FLUXO PRIMORDIAL DE EVENTOS

Um motorista adentra o veículo e vira a chave, em consequência do que o sistema demanda para verificação utilizando diversos métodos para assegurar que aquele é o motorista apropriado. O motorista começa pela verificação de si mesmo com um dos métodos, após isso ele continua com o próximo, e o próximo, até que a verificação esteja completada. Quando o motorista está verificado a informação é enviada, criptografada, para o escritório de apoio (*back-office*) e o motorista pode sair com o veículo.

20

25

FLUXO ALTERNATIVO DE EVENTOS

Um motorista adentra o veículo e vira a chave, em consequência do que o sistema demanda para verificação utilizando diversos métodos para assegurar que aquele é o

30

motorista apropriado. O motorista não é bem sucedido com um ou mais dos métodos de verificação. Depois de **três** falhas com um método, a verificação continua com os outros métodos (ou termina sem o último se aquele é o único a falhar).

5 Pelo menos um dos métodos é bem sucedido e a informação é enviada, criptografada, para o escritório de apoio (*back-office*), e o motorista pode sair com o veículo. Juntamente com a informação verificada acerca do motorista, o escritório de apoio (*back-office*) também recebe informação

10 acerca da verificação falha.

FLUXO ALTERNATIVO DE EVENTOS

Um motorista adentra o veículo e vira a chave, em consequência do que o sistema demanda para verificação

15 utilizando diversos métodos para assegurar que aquele é o motorista apropriado. O motorista não é bem sucedido com o primeiro método de verificação, depois de **três** falhas o sistema continua com o próximo método. Nenhum dos métodos é bem sucedido, em consequência do que um alarme é

20 imediatamente enviado para o escritório de apoio (*back-office*).

REQUERIMENTO ESPECIAL

O sistema deveria receber informação quando uma pessoa

25 desbloqueia (destrava) as portas. O sistema necessita de telemáticas para ter a capacidade de enviar a informação entre o veículo e o escritório de apoio (*back-office*).

Exemplo 1

30 O motorista chegou à garagem para começar o dia de

trabalho. Na medida em que ele adentra o veículo ele insere seu cartão inteligente (integrado no cartão para o tacógrafo) no leitor, disca seu código **PIN** e após isso coloca seu dedo sobre o *scanner*. O **PIN** está correto e o
5 dedo é verificado contra o cartão. Uma mensagem de sistema aparece, dizendo para o motorista sentar em uma posição de dirigir normal, de maneira a desempenhar a verificação de rosto. Dados registrados são analisados e comparados com os dados de gabarito armazenados no cartão inteligente - a
10 verificação foi bem sucedida. O nome e número de identificação de empregado são enviados, criptografados, para o escritório de apoio (*back-office*).

Exemplo 2

15 O motorista chegou à garagem para começar o dia de trabalho. Na medida em que ele adentra o veículo ele insere seu cartão inteligente (integrado no cartão para o tacógrafo) no leitor, disca seu código **PIN** e após isso coloca seu dedo sobre o *scanner*. O **PIN** está correto e o
20 dedo é verificado contra o cartão. Uma mensagem de sistema aparece, dizendo para o motorista sentar em uma posição normal de dirigir, de maneira a desempenhar a verificação de rosto. Dados registrados são analisados e comparados com os dados de gabarito armazenados no cartão inteligente - a
25 verificação foi bem sucedida. O nome e número de identificação de empregado são enviados, criptografados, para o escritório de apoio (*back-office*).

Exemplo 3

30 O motorista chegou à garagem para começar o dia de

trabalho. Na medida em que ele adentra o veículo ele insere seu cartão inteligente (integrado no cartão para o tacógrafo) no leitor, disca seu código **PIN** e após isso coloca seu dedo sobre o scanner. Ele tenta verificar sua identidade pela sua voz, mas isto falha tendo em vista que ele pegou um resfriado hoje. O nome e número de identificação de empregado são enviados, criptografados, para o escritório de apoio (*back-office*), juntamente com informação acerca da verificação de voz falha.

10

Exemplo 4

O motorista chegou à garagem para começar o dia de trabalho. Na medida em que ele adentra o veículo ele insere seu cartão inteligente (integrado no cartão para o tacógrafo) no leitor, disca seu código **PIN** e após isso coloca seu dedo sobre o scanner. Uma fotografia é tirada do rosto do motorista, mas tendo em vista que ele deixou sua barba crescer durante suas férias, a verificação falha. O nome e número de identificação de empregado são enviados, criptografados, para o escritório de apoio (*back-office*), juntamente com informação acerca da verificação de rosto falha.

Implementações exemplificantes da(s) presente(s) invenção(ões) apresentada(s) está(ão) descrita(s) aqui precedentemente. Aquelas características para as quais proteção de patente está sendo solicitada estão prescritas e estabelecidas nas **reivindicações de patente** subsequente.

Portanto, como mencionado precedentemente, embora a presente invenção tenha sido descrita com referência para

30

concretizações específicas, deverá ser observado por aqueles especializados no estado da técnica que a presente invenção não é para ser considerada como estando limitada para as concretizações ilustrativas, preferidas e 5 vantajosas descritas anteriormente, mas certamente, um número de variações e de modificações é conceptível dentro do escopo de proteção das **reivindicações de patente** posteriormente.





REIVINDICAÇÕES

1. Um método para assegurar que o operador de um veículo é um motorista autorizado, **caracterizado pelo fato**
5 de que referido método compreende:

- utilização de um sistema, no veículo, de verificação de motorista de modo múltiplo, para verificar se um operador é um motorista autorizado;

10 - execução de um primeiro procedimento de verificação de motorista sobre um operador presente do veículo e determinar se o operador presente é um motorista autorizado ou não autorizado do veículo;

15 - execução de um segundo procedimento de verificação de motorista sobre o operador presente do veículo e determinar se o operador presente é um motorista autorizado ou não autorizado do veículo, em que referidos primeiro e segundo procedimentos de verificação de motorista são executados com um intervalo de tempo dentre eles, referido intervalo de tempo sendo dependente da natureza de trabalho
20 sendo executado pelo operador;

- exercício de uma mensuração remediadora para impedir impacto potencialmente negativo quando o operador presente do veículo é determinado ser um motorista não autorizado fundamentado sobre pelo menos um dos procedimentos de
25 verificação executados; e

- em que pelo menos um dos procedimentos de verificação compreende utilização de dados biométricos que podem mudar ao longo do tempo para uma pessoa em particular por intermédio disso potencialmente permitindo uma falha de

verificação daquela pessoa fundamentada sobre uma
comparação de mensurações biométricas normais contra um
gabarito (*template*) previamente produzido das mesmas
características, e automaticamente atualizando o padrão
5 previamente produzido.

2. O método de acordo com a reivindicação **1**,
caracterizado pelo fato de que referida atualização
automática é conseguida em um sistema de verificação de
modo múltiplo, em que o sistema de verificação utiliza mais
10 do que um cartão biométrico/de código **PIN**/inteligente e o
segundo procedimento de verificação de motorista é
diferente a partir de referido primeiro procedimento de
verificação de motorista.

3. O método de acordo com a reivindicação **1**,
15 **caracterizado pelo fato** de que pelo menos um procedimento
de verificação utiliza dados biométricos de reconhecimento
de rosto atualizados que foram mudados ao longo do tempo.

4. O método de acordo com a reivindicação **1**,
caracterizado pelo fato de que sobre o operador adentrando
20 o veículo um lembrete (*prompt*) é emitido requerendo
verificação de identidade utilizando código **PIN**, impressão
digital e reconhecimento de rosto, e depois do que o
sistema verifica a identidade de operador utilizando código
PIN e reconhecimento de rosto e utiliza a impressão digital
25 biométrica para atualizar o gabarito de impressão digital
na base de dados.

5. O método de acordo com a reivindicação **1**,
caracterizado pelo fato de que procedimentos de verificação
de motorista múltiplos são executados durante uma única
30 ação de condução do operador, e referida única ação de

condução do operador se estendendo a partir de quando o operador adentra o veículo pela primeira vez quando venha a chegar para trabalhar e até que o operador finalmente venha a deixar o veículo quando venha a deixar o trabalho.

5 6. O método de acordo com a reivindicação 1, **caracterizado pelo fato** de que referido segundo procedimento de verificação de motorista é executado somente quando um operador do veículo não é determinado ser um motorista autorizado fundamentado sobre performance do primeiro procedimento de verificação de motorista.

10 7. O método de acordo com a reivindicação 1, **caracterizado pelo fato** de que pelo menos um de referidos primeiro e segundo procedimentos de verificação de motorista é um teste de verificação passivo que não requer interação consciente pelo operador em associação com a execução do pelo menos um de referidos procedimentos de verificação de motorista.

15 8. O método de acordo com a reivindicação 7, **caracterizado pelo fato** de que referido teste de verificação passivo compreende um escaneamento de uma característica física do operador a partir da qual uma imagem é comparada com um conjunto de imagens de controle representativas de motoristas autorizados do veículo.

20 9. O método de acordo com a reivindicação 8, **caracterizado pelo fato** de que referida característica física escaneada do operador é a íris de pelo menos um dos olhos do operador.

25 10. O método de acordo com a reivindicação 8, **caracterizado pelo fato** de que referida característica física escaneada do operador é a retina de pelo menos um

30

dos olhos do operador.

11. O método de acordo com a reivindicação **8**, **caracterizado pelo fato** de que referida característica física escaneada é um termograma facial do operador.

5 12. O método de acordo com a reivindicação **8**, **caracterizado pelo fato** de que referido teste de verificação passivo possui uma taxa de falha devida para pelo menos uma condição ambiental que previne que um escaneamento adequado da característica física do operador
10 venha a ser obtido.

13. O método de acordo com a reivindicação **12**, **caracterizado pelo fato** de que a pelo menos uma condição ambiental é iluminação insuficiente.

14. O método de acordo com a reivindicação **1**,
15 **caracterizado pelo fato** de que pelo menos um de referidos primeiro e segundo procedimentos de verificação de motorista é um teste de verificação ativo que requer interação consciente pelo operador em associação com a execução do pelo menos um de referidos procedimentos de
20 verificação de motorista.

15. O método de acordo com a reivindicação **14**, **caracterizado pelo fato** de que referido teste de verificação ativo compreende um escaneamento de uma característica física do operador a partir da qual uma
25 imagem é comparada com um conjunto de imagens de controle representativas de motoristas autorizados do veículo, referido escaneamento requerendo que o operador venha a colocar uma porção do corpo sobre um scanner.

16. O método de acordo com a reivindicação **15**,
30 **caracterizado pelo fato** de que referida característica

física escaneada do operador é um padrão de impressão de pelo menos um dos dedos do operador.

17. O método de acordo com a reivindicação **15**, **caracterizado pelo fato** de que referida característica física escaneada é a geometria de mão do operador.

18. O método de acordo com a reivindicação **14**, **caracterizado pelo fato** de que referido teste de verificação ativo compreende emissão de uma requisição para que o operador venha a inserir um número de verificação pessoal no sistema que venha a identificar o operador como um motorista autorizado.

19. O método de acordo com a reivindicação **14**, **caracterizado pelo fato** de que referido teste de verificação ativo compreende leitura de informação de verificação severamente codificada sobre um cartão de verificação apresentado pelo operador e requerendo que o operador venha a inserir um número de verificação pessoal no sistema que venha a corresponder a um número de verificação severamente codificado lido a partir do cartão de verificação.

20. O método de acordo com a reivindicação **14**, **caracterizado pelo fato** de que referido teste de verificação ativo compreende emissão de um comando para o operador falar uma sentença pré-escrita e registrando referida sentença falada como um padrão de fala e comparando aquele padrão com um conjunto de padrões de fala de controle de motoristas autorizados do veículo.

21. Um método para assegurar que o operador de um veículo é um motorista autorizado, **caracterizado pelo fato** de que referido método compreende:

- utilização de um sistema no veículo de verificação de motorista de modo múltiplo, para verificar se um operador é um motorista autorizado;

5 - execução de um primeiro procedimento de verificação de motorista sobre um operador presente do veículo e determinar se o operador presente é um motorista autorizado ou não autorizado do veículo;

10 - execução de um segundo procedimento de verificação de motorista sobre o operador presente do veículo e determinar se o operador presente é um motorista autorizado ou não autorizado do veículo, em que referido segundo procedimento de verificação de motorista é diferente a partir de referido primeiro procedimento de verificação de motorista;

15 - exercício de uma mensuração remediadora para impedir impacto potencialmente negativo quando o operador presente do veículo é determinado ser um motorista não autorizado fundamentado sobre pelo menos um dos procedimentos de verificação executados; e

20 - em que pelo menos um dos procedimentos de verificação compreende utilização de dados biométricos que podem mudar ao longo do tempo para uma pessoa em particular por intermédio disso potencialmente permitindo uma falha de verificação daquela pessoa fundamentada sobre uma
25 comparação de mensurações biométricas normais contra um gabarito (*template*) previamente produzido das mesmas características, e automaticamente atualizando o gabarito previamente produzido.

30 **22.** O método de acordo com a reivindicação **21**, **caracterizado pelo fato** de que referida mensuração

remediadora é exercida quando o operador presente do veículo é determinado ser um motorista não autorizado fundamentada sobre pelo menos dois dos procedimentos de verificação executados.

5 **23.** O método de acordo com a reivindicação **21**, **caracterizado pelo fato** de que adicionalmente compreende execução de um terceiro procedimento de verificação de motorista sobre o operador presente do veículo e determinar se o operador presente é um motorista autorizado ou não
10 autorizado do veículo.

24. O método de acordo com a reivindicação **23**, **caracterizado pelo fato** de que referida mensuração remediadora é exercida quando o operador presente do veículo é determinado ser um motorista não autorizado
15 fundamentado sobre pelo menos três dos procedimentos de verificação executados.

25. O método de acordo com a reivindicação **21**, **caracterizado pelo fato** de que cada um dos procedimentos de verificação de motorista são executados durante uma única
20 sessão de ação de condução do operador, referida única sessão de ação de condução se estendendo a partir de quando o operador venha a ocupar o assento do motorista e começa a ação de condução do veículo e até que o operador venha a desocupar e deixar o assento do motorista.

25 **26.** O método de acordo com a reivindicação **21**, **caracterizado pelo fato** de que referido segundo procedimento de verificação de motorista é executado somente quando um operador do veículo é determinado ser um motorista não autorizado fundamentado sobre a execução do
30 primeiro procedimento de verificação de motorista.

27. O método de acordo com a reivindicação **21**, **caracterizado pelo fato** de que pelo menos um de referidos primeiro e segundo procedimentos de verificação de motorista é um teste de verificação passivo que não requer interação consciente pelo operador em associação com a execução do pelo menos um de referidos procedimentos de verificação de motorista.

28. O método de acordo com a reivindicação **27**, **caracterizado pelo fato** de que referido teste de verificação passivo compreende um escaneamento de uma característica física do operador a partir da qual uma imagem é comparada para um conjunto de imagens de controle representativas de motoristas autorizados do veículo.

29. O método de acordo com a reivindicação **28**, **caracterizado pelo fato** de que referida característica física escaneada do operador é a íris de pelo menos um dos olhos do operador.

30. O método de acordo com a reivindicação **28**, **caracterizado pelo fato** de que referida característica física escaneada do operador é a retina de pelo menos um dos olhos do operador.

31. O método de acordo com a reivindicação **28**, **caracterizado pelo fato** de que referida característica física escaneada é um termograma facial do operador.

32. O método de acordo com a reivindicação **28**, **caracterizado pelo fato** de que referido teste de verificação passivo possui uma taxa de falha devida para pelo menos uma condição ambiental que previne que um escaneamento adequado da característica física do operador venha a ser obtido.

33. O método de acordo com a reivindicação **32**, **caracterizado pelo fato** de que a pelo menos uma condição ambiental é iluminação insuficiente.

5 34. O método de acordo com a reivindicação **21**, **caracterizado pelo fato** de que pelo menos um dos referidos primeiro e segundo procedimentos de verificação de motorista é um teste de verificação ativo que requer interação consciente pelo operador em associação com a execução de pelo menos um de referidos procedimentos de
10 verificação de motorista.

35. O método de acordo com a reivindicação **34**, **caracterizado pelo fato** de que referido teste de verificação ativo compreende um escaneamento de uma característica física do operador a partir da qual uma
15 imagem é comparada com um conjunto de imagens de controle representativas de motoristas autorizados do veículo, referido escaneamento requerendo que o operador venha a colocar uma porção do corpo sobre um *scanner*.

20 36. O método de acordo com a reivindicação **35**, **caracterizado pelo fato** de que de que referida característica física escaneada do operador é um padrão de impressão de pelo menos um dos dedos do operador.

37. O método de acordo com a reivindicação **35**, **caracterizado pelo fato** de que referida característica
25 física escaneada é a geometria de mão do operador.

38. O método de acordo com a reivindicação **34**, **caracterizado pelo fato** de que referido teste de verificação ativo compreende emissão de uma requisição para que o operador venha a inserir um número de verificação
30 pessoal no sistema que venha a identificar o operador como

um motorista autorizado.

39. O método de acordo com a reivindicação **34**, **caracterizado pelo fato** de que referido teste de verificação ativo compreende leitura de informação de verificação severamente codificada sobre um cartão de verificação apresentado pelo operador e requerendo que o operador venha a inserir um número de verificação pessoal no sistema que venha a corresponder a um número de verificação severamente codificado lido a partir do cartão de verificação.

40. O método de acordo com a reivindicação **34**, **caracterizado pelo fato** de que de que referido teste de verificação ativo compreende emissão de um comando para o operador falar uma sentença pré-escrita e registrando referida sentença falada como um padrão de fala e comparando aquele padrão com um conjunto de padrões de fala de controle de motoristas autorizados do veículo.

41. Um método para assegurar que o operador de um veículo é um motorista autorizado, **caracterizado pelo fato** de que referido método compreende:

- utilização de um sistema de verificação, no veículo, de motorista de modo múltiplo, para verificar se um operador é um motorista autorizado;

- execução de um primeiro tipo de procedimento de verificação de motorista sobre um operador presente do veículo e determinar se o operador presente é um motorista autorizado ou não autorizado do veículo;

- execução de um segundo tipo de procedimento de verificação de motorista sobre o operador presente do veículo e determinar se o operador presente é um motorista

autorizado ou não autorizado do veículo, em que referido segundo procedimentos de verificação de motorista são de tipos diferentes um a partir do outro e são executados com intervalos de tempo randômicos dentre eles;

5 - exercício de uma mensuração remediadora para impedir impacto potencialmente negativo quando o operador presente do veículo é determinado ser um motorista não autorizado fundamentado sobre pelo menos um dos procedimentos de verificação executados; e

10 - em que pelo menos um dos procedimentos de verificação compreende utilização de dados biométricos que podem mudar ao longo do tempo para uma pessoa em particular por intermédio disso potencialmente permitindo uma falha de verificação daquela pessoa fundamentada sobre uma
15 comparação de mensurações biométricas normais contra um gabarito (*template*) previamente produzido das mesmas características, e automaticamente atualizando o gabarito previamente produzido.

42. O método de acordo com a reivindicação **41**,
20 **caracterizado pelo fato** de que referida mensuração remediadora é exercida quando o operador presente do veículo é determinado ser um motorista não autorizado fundamentada sobre pelo menos dois dos procedimentos de verificação executados.

25 **43.** O método de acordo com a reivindicação **41**, **caracterizado pelo fato** de que referidos procedimentos de verificação de motorista são executados com intervalos de tempo randômicos dentre eles.

44. O método de acordo com a reivindicação **41**,
30 **caracterizado pelo fato** de que adicionalmente compreende

iniciação de referida segunda verificação de motorista imediatamente seguindo-se uma determinação que o operador presente é um motorista não autorizado em referido primeiro procedimento de verificação de motorista.

5 **45.** O método de acordo com a reivindicação **41**, **caracterizado pelo fato** de que cada um dos procedimentos de verificação de motorista são executados durante uma única sessão de ação de condução do operador, referida única sessão de ação de condução se estendendo a partir de quando
10 o operador venha a ocupar o assento do motorista e começa a ação de condução do veículo e até que o operador venha a desocupar e deixar o assento do motorista.

46. O método de acordo com a reivindicação **41**, **caracterizado pelo fato** de que referido segundo
15 procedimento de verificação de motorista é executado somente quando um operador do veículo é determinado ser um motorista não autorizado fundamentado sobre a execução do primeiro procedimento de verificação de motorista.

47. O método de acordo com a reivindicação **41**,
20 **caracterizado pelo fato** de que pelo menos um de referidos primeiro e segundo procedimentos de verificação de motorista é um teste de verificação passivo que não requer interação consciente pelo operador em associação com a execução do pelo menos um de referidos procedimentos de
25 verificação de motorista.

48. O método de acordo com a reivindicação **47**, **caracterizado pelo fato** de que referido teste de verificação passivo compreende um escaneamento de uma característica física do operador a partir da qual uma
30 imagem é comparada com um conjunto de imagens de controle

representativas de motoristas autorizados do veículo.

5 **49.** O método de acordo com a reivindicação **48**,
caracterizado pelo fato de que referida característica
física escaneada do operador é a íris de pelo menos um dos
olhos do operador.

50. O método de acordo com a reivindicação **48**,
caracterizado pelo fato de que referida característica
física escaneada do operador é a retina de pelo menos um
dos olhos do operador.

10 **51.** O método de acordo com a reivindicação **48**,
caracterizado pelo fato de que referida característica
física escaneada é um termograma facial do operador.

52. O método de acordo com a reivindicação **48**,
caracterizado pelo fato de que referido teste de
15 verificação passivo possui uma taxa de falha devida para
pelo menos uma condição ambiental que previne que um
escaneamento adequado da característica física do operador
venha a ser obtido.

53. O método de acordo com a reivindicação **52**,
20 **caracterizado pelo fato** de que a pelo menos uma condição
ambiental é iluminação insuficiente.

54. O método de acordo com a reivindicação **41**,
caracterizado pelo fato de que pelo menos um de referidos
primeiro e segundo procedimentos de verificação de
25 motorista é um teste de verificação ativo que requer
interação consciente pelo operador em associação com a
execução do pelo menos um de referidos procedimentos de
verificação de motorista.

55. O método de acordo com a reivindicação **54**,
30 **caracterizado pelo fato** de que referido teste de

verificação ativo compreende um escaneamento de uma característica física do operador a partir da qual uma imagem é comparada com um conjunto de imagens de controle representativas de motoristas autorizados do veículo, 5 referido escaneamento requerendo que o operador venha a colocar uma porção do corpo sobre um *scanner*.

56. O método de acordo com a reivindicação 55, **caracterizado pelo fato** de que referida característica física escaneada do operador é um padrão de impressão de 10 pelo menos um dos dedos do operador.

57. O método de acordo com a reivindicação 55, **caracterizado pelo fato** de que referida característica física escaneada é a geometria de mão do operador.

58. O método de acordo com a reivindicação 54, 15 **caracterizado pelo fato** de que referido teste de verificação ativo compreende emissão de uma requisição para que o operador venha a inserir um número de verificação pessoal no sistema que venha a identificar o operador como um motorista autorizado.

20 59. O método de acordo com a reivindicação 54, **caracterizado pelo fato** de que referido teste de verificação ativo compreende leitura de informação de verificação severamente codificada sobre um cartão de verificação apresentado pelo operador e requerendo que o 25 operador venha a inserir um número de verificação pessoal no sistema que venha a corresponder a um número de verificação severamente codificado lido a partir do cartão de verificação.

30 60. O método de acordo com a reivindicação 54, **caracterizado pelo fato** de que referido teste de

verificação ativo compreende emissão de um comando para o operador falar uma sentença pré-escrita e registrando referida sentença falada como um padrão de fala e comparando aquele padrão com um conjunto de padrões de fala de controle de motoristas autorizados do veículo.

5
61. Um método para verificação de uma identidade do operador de veículo utilizando dados biométricos que podem mudar ao longo do tempo para uma pessoa em particular por intermédio disso potencialmente permitindo uma falha de verificação daquela pessoa fundamentada sobre uma comparação de mensurações biométricas normais contra um gabarito (*template*) previamente produzido das mesmas características, **caracterizado pelo fato** de que referido método compreende:

15 - automaticamente atualizando o gabarito previamente produzido, referida atualização automática sendo conseguida em um sistema de verificação de modo múltiplo em que referido sistema de verificação utiliza mais do que um cartão biométrico/de código **PIN**/inteligente.

20 62. O método de acordo com a reivindicação 61, **caracterizado pelo fato** de que pelo menos um método de verificação é utilizado para verificar a identidade do operador enquanto um outro método de verificação que não está presentemente sendo utilizado para propósitos de verificação do operador é utilizado para atualizar o gabarito previamente produzido depois de determinar que o processo de verificação foi bem sucedido.

25
63. O método de acordo com a reivindicação 61, **caracterizado pelo fato** de que sobre o operador adentrando o veículo um lembrete (*prompt*) é emitido requerendo

verificação de identidade utilizando código **PIN**, impressão digital e reconhecimento de rosto, e depois do que o sistema verifica a identidade do operador utilizando código **PIN** e reconhecimento de rosto e utiliza a impressão digital biométrica para atualizar o gabarito de impressão digital na base de dados.

5 **64.** O método de acordo com a reivindicação **61**, **caracterizado pelo fato** de que adicionalmente compreende armazenamento do gabarito biométrico em uma base de dados sobre o veículo.

65. O método de acordo com a reivindicação **61**, **caracterizado pelo fato** de que adicionalmente compreende armazenamento do gabarito biométrico em uma base de dados no *back-office* por intermédio disso requerendo comunicação em tempo real entre o veículo e o *back-office*.

66. O método de acordo com a reivindicação **61**, **caracterizado pelo fato** de que adicionalmente compreende armazenamento do gabarito biométrico em uma base de dados que um motorista carrega sobre sua pessoa (consigo).

20 **67.** O método de acordo com a reivindicação **66**, **caracterizado pelo fato** de que referido gabarito biométrico é armazenado em um cartão inteligente.

68. O método de acordo com a reivindicação **67**, **caracterizado pelo fato** de que adicionalmente compreende utilização de um cartão de motorista do Tacógrafo digital para armazenar referidos gabaritos de verificação, referido cartão sendo um cartão inteligente que é adequado para tal armazenamento e é algo que o motorista é forçado a utilizar por lei em algumas jurisdições e é, por consequência, sempre carregado com o motorista.

69. O método de acordo com a reivindicação 61, **caracterizado pelo fato** de que adicionalmente compreende:

5 - assegurar que o operador de um veículo é um motorista autorizado utilizando um sistema de verificação de motorista de modo múltiplo, embarcado, para verificar se um operador é um motorista autorizado;

10 - execução de um primeiro procedimento de verificação de motorista sobre um operador presente do veículo e determinar se o operador presente é um motorista autorizado ou não autorizado do veículo;

15 - execução de um segundo procedimento de verificação de motorista sobre o operador presente do veículo e determinar se o operador presente é um motorista autorizado ou não autorizado do veículo, em que referidos primeiro e segundo procedimentos de verificação de motorista são executados com um intervalo de tempo dentre eles, referido intervalo de tempo sendo dependente da natureza do trabalho sendo executado pelo operador; e

20 - exercício de uma mensuração remediadora para impedir impacto potencialmente negativo quando o operador presente do veículo é determinado ser um motorista não autorizado fundamentada sobre pelo menos um dos procedimentos de verificação executados.

25 70. O método de acordo com a reivindicação 69, **caracterizado pelo fato** de que referido segundo procedimento de verificação de motorista é diferente a partir de referido primeiro procedimento de verificação de motorista.

30 71. O método de acordo com a reivindicação 69, **caracterizado pelo fato** de que referido segundo

procedimento de verificação de motorista é o mesmo como referido primeiro procedimento de verificação de motorista.

72. O método de acordo com a reivindicação **69**, **caracterizado pelo fato** de que adicionalmente compreende 5 iniciação de referida segunda verificação de motorista imediatamente seguindo-se uma determinação que o operador presente é um motorista não autorizado em referido primeiro procedimento de verificação de motorista.

73. O método de acordo com a reivindicação **69**, 10 **caracterizado pelo fato** de que procedimentos de verificação do motorista de motorista múltiplos são executados durante uma única ação de condução do operador, referida única ação de condução se estendendo a partir de quando o operador adentra o veículo pela primeira vez quando venha a chegar 15 para trabalhar e até que o operador finalmente venha a deixar o veículo quando venha deixar o trabalho.

74. O método de acordo com a reivindicação **69**, **caracterizado pelo fato** de que uma pluralidade de procedimentos de verificação de motorista de diferentes 20 tipos é conduzida em intervalos de tempo randômicos.

75. O método de acordo com a reivindicação **69**, **caracterizado pelo fato** de que pelo menos um de referidos primeiro e segundo procedimentos de verificação de motorista é um teste de verificação passivo que não requer 25 interação consciente pelo operador em associação com a execução de pelo menos um de referidos procedimentos de verificação de motorista.

76. O método de acordo com a reivindicação **75**, **caracterizado pelo fato** de que referido teste de 30 verificação passivo compreende um escaneamento de uma

característica física do operador a partir da qual uma imagem é comparada com um conjunto de imagens de controle representativas de motoristas autorizados do veículo.

5 **77.** O método de acordo com a reivindicação **76**, **caracterizado pelo fato** de que referido escaneamento das características físicas do operador é a íris de pelo menos um dos olhos do operador.

10 **78.** O método de acordo com a reivindicação **76**, **caracterizado pelo fato** de que referido escaneamento das características físicas do operador é a retina de pelo menos um dos olhos do operador.

79. O método de acordo com a reivindicação **76**, **caracterizado pelo fato** de que referida característica física escaneada é um termograma facial do operador.

15 **80.** O método de acordo com a reivindicação **76**, **caracterizado pelo fato** de que referido teste de verificação passivo possui uma taxa de falha devida para pelo menos uma condição ambiental que previne que um escaneamento adequado da característica física do operador venha a ser obtido.

81. O método de acordo com a reivindicação **80**, **caracterizado pelo fato** de que a pelo menos uma condição ambiental é iluminação insuficiente.

25 **82.** O método de acordo com a reivindicação **69**, **caracterizado pelo fato** de que pelo menos um de referidos primeiro e segundo procedimentos de verificação de motorista é um teste de verificação ativo que requer interação consciente pelo operador em associação com a execução de pelo menos um de referidos procedimentos de
30 verificação de motorista.

83. O método de acordo com a reivindicação 82, **caracterizado pelo fato** de que referido teste de verificação ativo compreende um escaneamento de uma característica física do operador a partir da qual uma
5 imagem é comparada com um conjunto de imagens de controle representativas de motoristas autorizados do veículo, referido escaneamento requerendo que o operador venha a colocar uma porção do corpo sobre um *scanner*.

84. O método de acordo com a reivindicação 83,
10 **caracterizado pelo fato** de que referida característica física escaneada do operador é um padrão de impressão de pelo menos um dos dedos do operador.

85. O método de acordo com a reivindicação 83,
15 **caracterizado pelo fato** de que referida característica física escaneada é a geometria de mão do operador.

86. O método de acordo com a reivindicação 82,
caracterizado pelo fato de que referido teste de verificação ativo compreende emissão de uma requisição para que o operador venha a inserir um número de verificação
20 pessoal no sistema que venha a identificar o operador como um motorista autorizado.

87. O método de acordo com a reivindicação 82,
caracterizado pelo fato de que referido teste de verificação ativo compreende leitura de informação de
25 verificação severamente codificada sobre um cartão de verificação apresentado pelo operador e requerendo que o operador venha a inserir um número de verificação pessoal no sistema que venha a corresponder a um número de verificação severamente codificado lido a partir do cartão
30 de verificação.

88. O método de acordo com a reivindicação **82**, **caracterizado pelo fato** de que referido teste de verificação ativo compreende emissão de um comando para o operador falar uma sentença pré-escrita e registrando
5 referida sentença falada como um padrão de fala e comparando aquele padrão com um conjunto de padrões de fala de controle de motoristas autorizados do veículo.

89. O método de acordo com a reivindicação **82**, **caracterizado pelo fato** de que referido segundo
10 procedimento de verificação de motorista é o mesmo como referido primeiro procedimento de verificação de motorista.

90. O método de acordo com a reivindicação **82**, **caracterizado pelo fato** de que adicionalmente compreende
15 iniciação de referida segunda verificação de motorista imediatamente seguindo-se uma determinação que o operador presente é um motorista não autorizado em referido primeiro procedimento de verificação de motorista.

91. O método de acordo com qualquer uma das reivindicações precedentes **1 - 90**, **caracterizado pelo fato**
20 de que o(s) sistema(s) de verificação, procedimento(s) de verificação, teste(s) de verificação, número(s) de verificação, cartão(ões) de verificação, falha(s) de verificação, ou informação de verificação são substituídos pelo(s) correspondente(s) sistema(s) de identificação,
25 procedimento(s) de identificação, teste(s) de identificação, número(s) de identificação, cartão(ões) de identificação, falha(s) de identificação, ou informação de identificação, como pode ser o caso, ou por qualquer combinação de sistema(s), procedimento(s), teste(s),
30 número(s), cartão(ões), falha(s), ou informação de verificação e identificação, como pode ser o caso.

DESENHOS

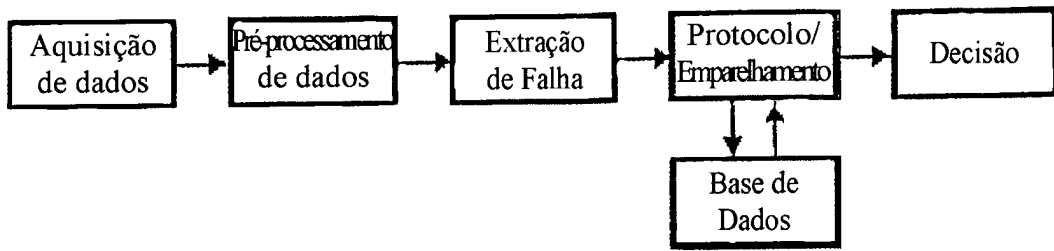


Figura 1



Figura 2











 <p>Sulco</p>	Sulco	Definido como possuindo o dobro da distância a partir do início para o fim, desde que sulcos vizinhos são largos
 <p>Finais de Fuga</p>	Finais de fuga	Dois sulcos com diferentes direções correm paralelos um com o outro por mais do que 3 mm
 <p>Bifurcação</p>	Bifurcação	Um sulco se divide, ambos os sulcos mantêm a mesma direção e são mais longos do que 3 mm
 <p>Gancho</p>	Gancho	Um sulco se divide; um sulco não é mais longo do que 3 mm
 <p>Garfo</p>	Garfo	Dois sulcos estão conectados por um terceiro sulco não mais longo do que 3 mm
 <p>Ponto</p>	Ponto	A seção de sulco não é mais longa do que os sulcos vizinhos são largos
 <p>Olho/Ilha</p>	Olho	O sulco se divide e se reúne dentro de 3 mm
 <p>Olho/Ilha</p>	Ilha	Um sulco se divide e se une novamente dentro de não menos do que 3 mm e não mais do que 6 mm. A área englobada é sem sulco
 <p>Sulco Englobado</p>	Sulco Englobado	Um sulco não mais longo do que 6 mm entre dois outros sulcos
 <p>Loop Englobado</p>	Loop Englobado	Um <i>loop</i> de determinação sem padrão entre dois ou mais sulcos paralelos
 <p>Especialidade</p>	Especialidades	Formas de sulco raras tais como sinais de interrogação e ganchos de açougueiro

Figura 3

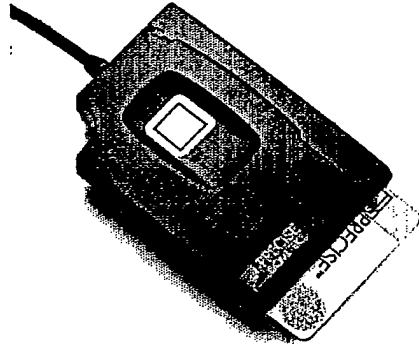


Figura 4

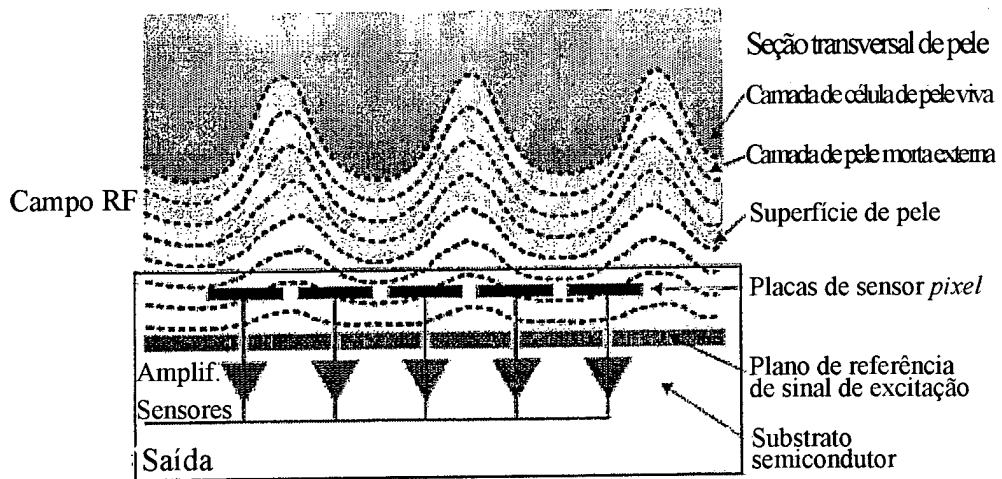


Figura 5

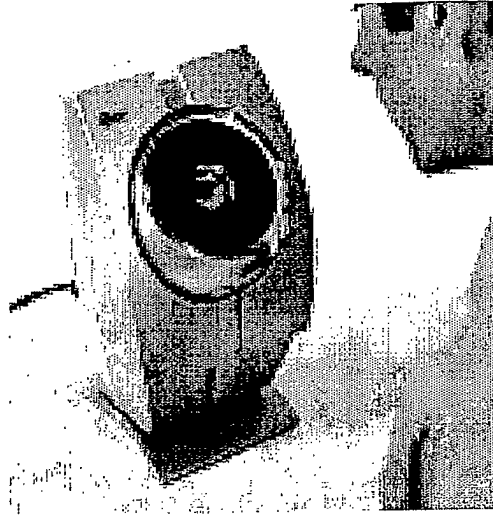


Figura 6



Figura 7

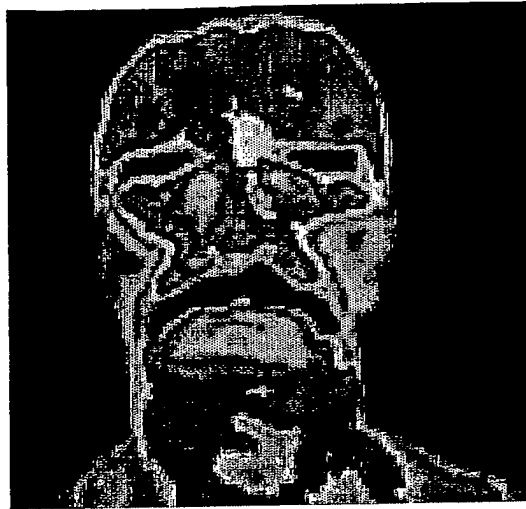


Figura 8

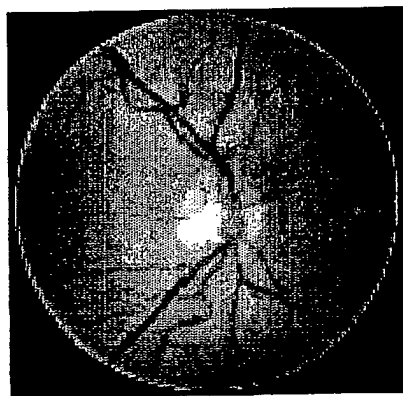


Figura 9



Figura 10

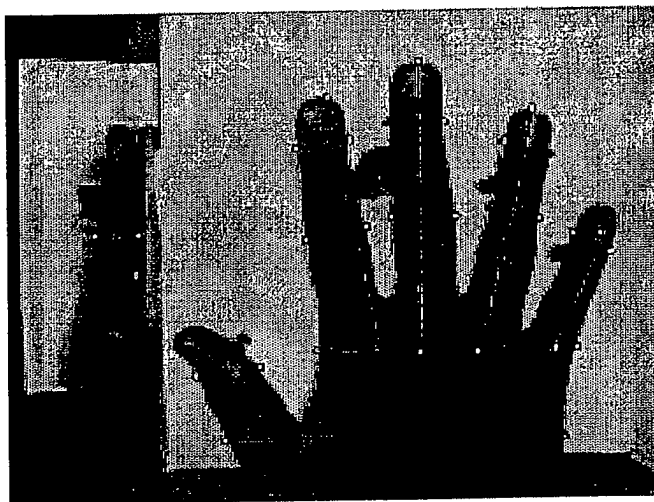


Figura 11

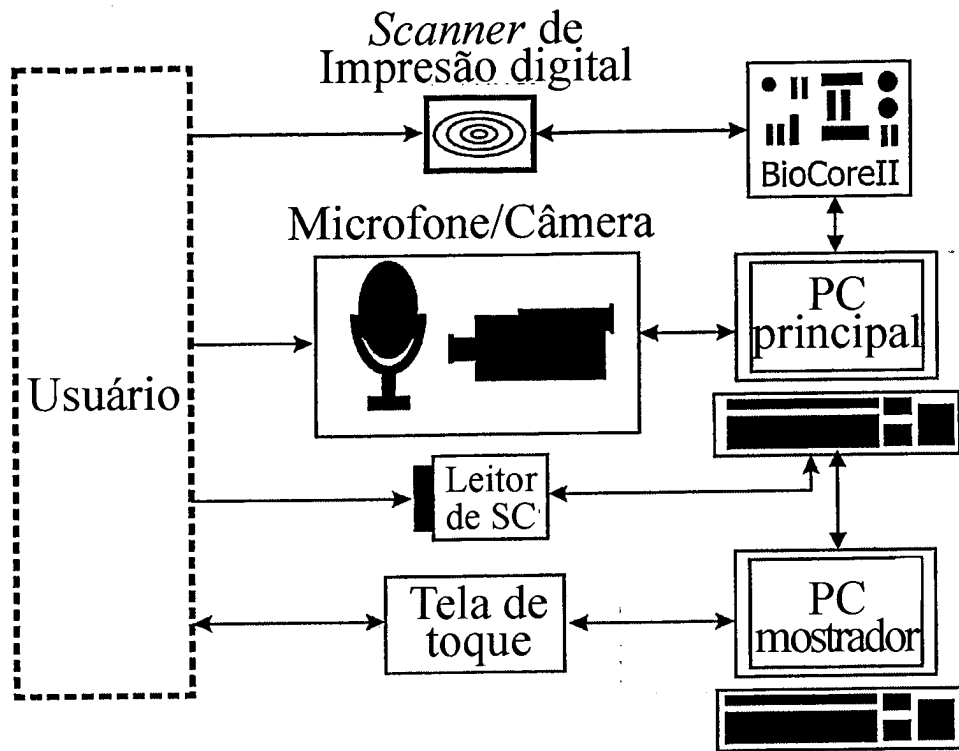


Figura 12

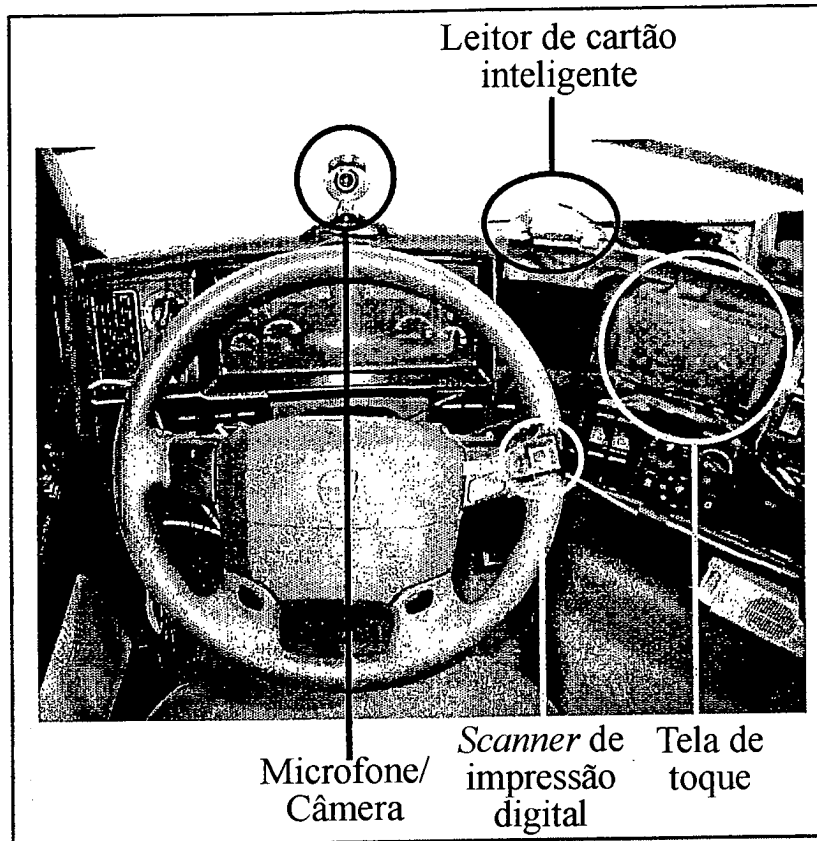


Figura 13



Figura 14

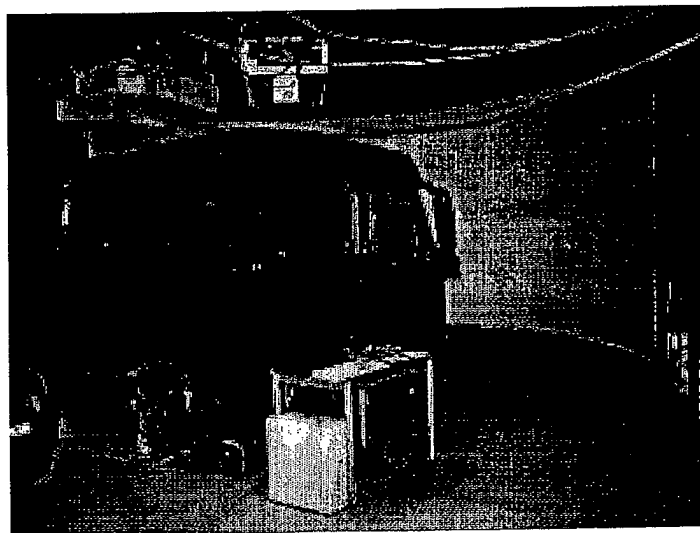


Figura 15

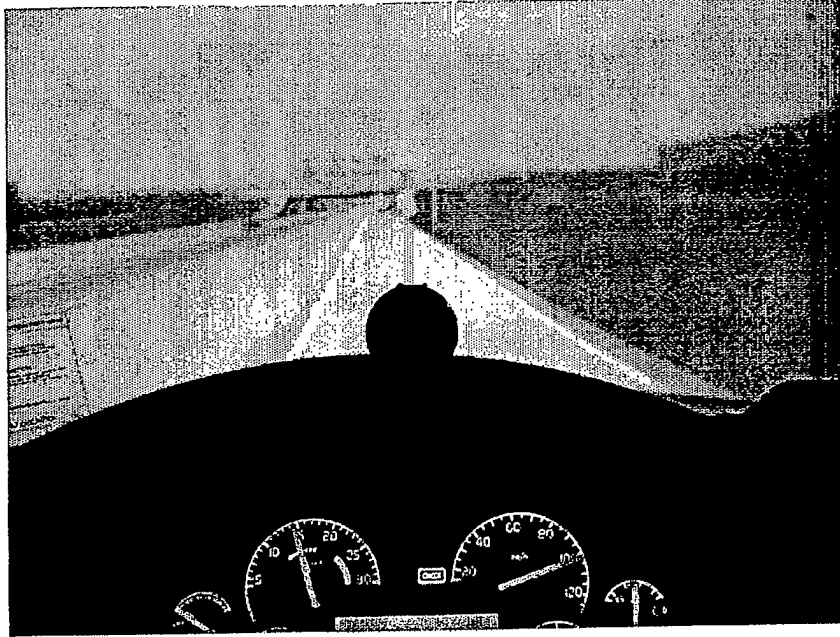


Figura 16

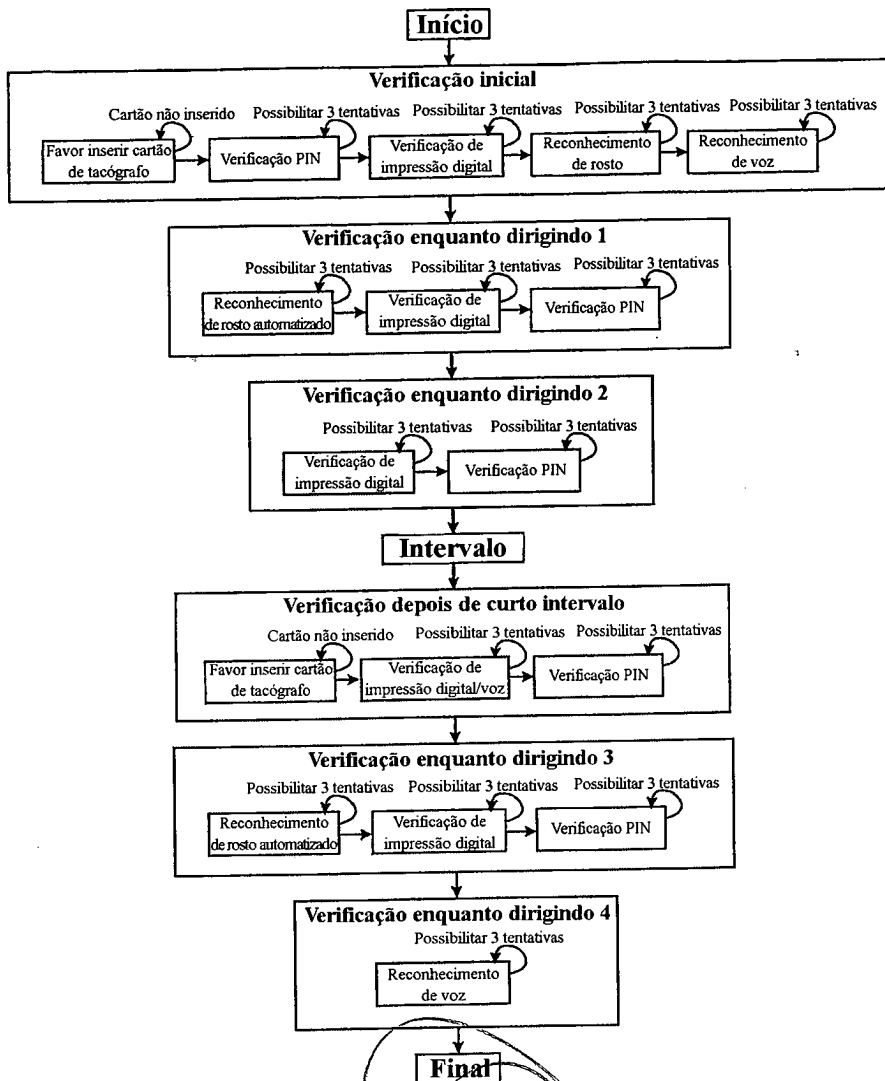


Figura 17

Resistências	Fragilidades	Oportunidades	Ameaças
Não dispendioso	Nem todos podem utilizar este método	Pode ser utilizado enquanto dirigindo	O sensor se danifica por sujeira, etc.
Bem testado	Pode ser enganado por bolores	Equipamento pequeno pode facilmente ser integrado no ambiente de motorista	Algumas pessoas poderiam se recusar a utilizá-lo desde que o método é associado com identificação criminosa
Fácil de utilizar	Poderiam haver problemas com mãos sujas ou feridas	Com mais do que um gabarito salvo o sistema pode randomicamente dizer que dedo escanear para verificação	Se o motorista está no meio do nada e vem a ter suas impressões digitais destruídas, por exemplo, por queimar sua mão
Rápido		Diversos modelos estão disponíveis desde que muitas diferentes companhias fabricam o equipamento	

Figura 20

Resistências	Fragilidades	Oportunidades	Ameaças
Muito preciso	Dispendioso	Poderia ser capaz de ser integrado com espelhos retrovisores traseiros	Pessoas podem se recusar a ter seus olhos analisados se elas acreditam ser perigoso
Rápido	Uma companhia, <i>Iridian</i> , detém todas as patentes. Todos os demais fabricantes têm que obter licença a partir dela	Poderia ser possível se utilizar enquanto dirigindo	Fabricante descontinua o negócio por alguma razão
A íris não muda ao longo do tempo			Pode ser impossível se utilizar em um veículo devido às condições de iluminação
Difícil de enganar			

Figura 21

Resistências	Fragilidades	Oportunidades	Ameaças
Rápido, tanto quanto o é a verificação. (E se você não exigir uma sentença longa a ser falada)	Voz muda ao longo do tempo	Pode ser integrado com telefone celular livre da mão ou outro equipamento controlado por voz	Voz do motorista muda devido à condições de saúde e emocionais
Não dispendioso	Algumas pessoas não confiam na tecnologia	Sistema pode randomicamente escolher sentença desejada para falar	Podem existir problemas com o ambiente ruidoso no cupê
Fácil de utilizar		Motorista pode possuir uma única senha, tomando a exigência para outro método de verificação desnecessária	
Não intrusivo		Pode ser utilizado enquanto dirigindo	
Frase falada pode ser mudada se, por exemplo, for roubada			

Figura 22

Resistências	Fragilidades	Oportunidades	Ameaças
Não intrusivo	Problemas podem ocorrer com barbas, óculos de sol, maquiagem, etc.	Câmera poderia ser integrada em espelhos retrovisores traseiros	Condições de iluminação no cupê poderiam tornar impossível tirar uma fotografia satisfatória
Não dispendioso	Um rosto de pessoa muda ao longo do tempo	Poderia ser possível utilizar enquanto dirigindo.	Rosto do motorista incha ou fica machucado por alguma razão
Fácil de utilizar			

Figura 23

Resistências	Fragilidades	Oportunidades	Ameaças
Rápido	Dispendioso	Câmera poderia ser integrada em espelhos retrovisores traseiros	Método novo, incerteza de quanta pesquisa e quanto desenvolvimento irão ser feitos
Independente de condições de iluminação	Novo e, portanto, não é extensivamente testado	Pode ser utilizado enquanto dirigindo	
Difícil de enganar			
Não intrusivo			

Figura 24

Resistências	Fragilidades	Oportunidades	Ameaças
Muito preciso	Não pode ser utilizado enquanto dirigindo	Utiliza <i>laser</i> , significando que é independente de condições de iluminação de cupê	Pessoas podem recusar utilizar o método desde que elas podem não confiar em radiação <i>laser</i>
Difícil de enganar	Necessita alinhamento próximo perfeito do olho		
Padrão de vaso de retina não muda muito ao longo do tempo	Dispendioso		
Rápido			

Figura 25

Resistências	Fragilidades	Oportunidades	Ameaças
Não intrusivo	Tem que ser utilizado em conjunção com outros recursos de verificação	Poderia ser utilizado enquanto dirigindo	Incerteza de quanta pesquisa e quanto desenvolvimento do método irão ser feitos
Rápido	Somente testado em um determinado contexto	Câmera poderia ser integrada em espelhos retrovisores traseiros	Motorista fica machucado na área em torno da boca por alguma razão
Fácil de utilizar	Incerteza de quantas companhias, se alguma, que manufacturam o equipamento	Poderia ser utilizado em conjunção com, por exemplo, verificação de rosto ou voz	

Figura 26

Resistências	Fragilidades	Oportunidades	Ameaças
Rápido	Equipamento desajeitado	Pode ser utilizado enquanto dirigindo	Somente um fabricante de equipamento
Funciona com mãos (razoavelmente) sujas	Mãos não são únicos recursos, outros recursos de verificação necessitados		
Não intrusivo			
Fácil de utilizar			
Não dispendioso			

Figura 27

Resistências	Fragilidades	Oportunidades	Ameaças
Rápido	Se alguém descobre a senha ou o <i>PIN</i> , não existe nada que possa impedir que ele ou ela venham a utilizar a senha ou o <i>PIN</i>	A maior parte do equipamento necessitado já existe nos veículos de hoje em dia	A senha ou o <i>PIN</i> podem ser esquecidos
Fácil de utilizar, tanto quanto você tenha uma boa memória	Funciona melhor quando utilizado em conjunção com outros métodos	Não é difícil de utilizar enquanto dirigindo	A senha ou o <i>PIN</i> podem ser descobertos e utilizados por outros
Sem grandes custos para integrar/utilizar o método			

Figura 28

Resistências	Fragilidades	Oportunidades	Ameaças
Fácil de utilizar na medida em que é um método bem conhecido que a maior parte das pessoas utilizou antes	Um cartão poderia estar desgastado, ou quebrado	Todo o equipamento necessitado já existe nos veículos de hoje em dia	Um cartão é fácil de se desprender, ou ser esquecido em casa
Rápido	Um cartão pode ser utilizado por diversas diferentes pessoas	A segurança pode ser aumentada pela adição de dados biométricos para o cartão, tornando difícil utilizar cartão de alguma outra pessoa	O cartão poderia ser roubado
Não intrusivo	Funciona melhor quando utilizado em conjunção com outros métodos		Mais fácil de enganar do que, por exemplo, alguns métodos biométricos
Não dispendioso			

Figura 29

Resistências	Fragilidades	Oportunidades	Ameaças
Muito rápido	Uma etiqueta <i>RFID</i> pode ser utilizada por diversas diferentes pessoas	O equipamento não necessita muito espaço, e não deveria ser difícil para integrar no veículo	Uma etiqueta <i>RFID</i> é fácil de se desprender, ou ser esquecida em casa
Independente de condições de iluminação	Funciona melhor quando utilizado em conjunção com outros métodos	Pode ser utilizado enquanto dirigindo	A etiqueta <i>RFID</i> poderia ser roubada
Não intrusivo			
Fácil de utilizar			

Figura 30

Estatísticas Descritivas

	N	Mínimo	Máximo	Médio	Desvio Padrão
Útil/Inútil	18	,00	2,00	1,2778	,82844
Agradável/Desagradável	18	-2,00	2,00	,4444	,98352
Ruim/Bom	18	-1,00	2,00	,8333	1,09813
Gentil/Aborrecido	18	-2,00	2,00	,3333	1,32842
Efetivo/Supérfluo	18	-2,00	2,00	1,0000	1,13759
Irritante/Prazeroso	18	-2,00	2,00	-,0556	1,21133
Auxiliado/Sem Valor	18	-2,00	2,00	,7222	1,22741
Indesejável/Desejável	18	-2,00	2,00	,2222	1,35280
Vigilância Aumentada/ Indução ao Sono	18	,00	1,00	,1667	,38348
Utilidade	18	-1,00	1,60	,8000	,72274
Satisfação	18	-2,00	1,50	,2361	,88895
N Válido (como lista)	18				

Figura 31

RESUMO

"MÉTODOS E DISPOSIÇÃO PARA EXECUÇÃO DE VERIFICAÇÃO
DE IDENTIDADE DE MOTORISTA"

5

A presente invenção se refere a um método para assegurar que o operador de um veículo é um motorista autorizado.

Em concordância com a presente invenção, o referido método está **caracterizado pelo fato** de que compreende:

- utilização de um sistema de verificação de motorista de modo múltiplo, embarcado, para verificar se um operador é um motorista autorizado;

15 - execução de um primeiro procedimento de verificação de motorista sobre um operador presente do veículo e determinar se o operador presente é um motorista autorizado ou não autorizado do veículo;

20 - execução de um segundo procedimento de verificação de motorista sobre o operador presente do veículo e determinar se o operador presente é um motorista autorizado ou não autorizado do veículo, em que referidos primeiro e segundo procedimentos de verificação de motorista são executados com um intervalo de tempo dentre eles, referido intervalo de tempo sendo dependente da natureza de trabalho sendo executado pelo operador;

25 - exercício de uma mensuração remediadora para impedir impacto potencialmente negativo quando o operador presente do veículo é determinado ser um motorista não autorizado fundamentado sobre pelo menos um dos procedimentos de verificação executados.

30