

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4852604号
(P4852604)

(45) 発行日 平成24年1月11日 (2012. 1. 11)

(24) 登録日 平成23年10月28日 (2011. 10. 28)

(51) Int. Cl.	F I
B60R 25/00 (2006.01)	B60R 25/00 601
G06F 21/20 (2006.01)	G06F 15/00 330F
G08B 13/00 (2006.01)	G08B 13/00 B
G06T 7/00 (2006.01)	G06T 7/00 510B
B60R 25/10 (2006.01)	B60R 25/10 619
請求項の数 91 (全 71 頁) 最終頁に続く	

(21) 出願番号	特願2008-521358 (P2008-521358)	(73) 特許権者	502196511
(86) (22) 出願日	平成18年7月11日 (2006. 7. 11)		ボルボ テクノロジー コーポレーション
(65) 公表番号	特表2009-500246 (P2009-500246A)		スウェーデン国 エス-405 08 イ
(43) 公表日	平成21年1月8日 (2009. 1. 8)		エテポリィ
(86) 国際出願番号	PCT/SE2006/000869	(74) 代理人	100098729
(87) 国際公開番号	W02007/008159		弁理士 重信 和男
(87) 国際公開日	平成19年1月18日 (2007. 1. 18)	(74) 代理人	100116757
審査請求日	平成21年5月14日 (2009. 5. 14)		弁理士 清水 英雄
(31) 優先権主張番号	60/697, 564	(74) 代理人	100123216
(32) 優先日	平成17年7月11日 (2005. 7. 11)		弁理士 高木 祐一
(33) 優先権主張国	米国 (US)	(74) 代理人	100089336
			弁理士 中野 佳直
		(74) 代理人	100148161
			弁理士 秋庭 英樹
		最終頁に続く	

(54) 【発明の名称】 ドライバID認証を実施するための方法と装置

(57) 【特許請求の範囲】

【請求項1】

車両のオペレータが認可ドライバであることを確かめるための方法であって、
オペレータが認可ドライバであるかどうかを確認するため、車載型マルチモードドライバ認証システムを利用することと、

前記車両の現在オペレータに第1ドライバ認証手順を実施して、該現在オペレータが該車両の認可ドライバであるか無認可ドライバであるかを判断することと、

前記車両の現在オペレータに第2ドライバ認証手順を実施して、該現在オペレータが該車両の認可ドライバであるか無認可ドライバであるかを判断することであって、該第1および第2ドライバ認証手順が時間間隔を間に置いて実施され、該時間間隔が該オペレータにより実施される作業の性質に左右されることと、

実施された前記認証手順の少なくとも一つに基づいて前記車両の前記現在オペレータが無認可ドライバであると判断された時に潜在的悪影響を回避する救済手段を行使することと、
を包含し、

前記認証手順の少なくとも一方が、現在バイオメトリクス測定値と同じ特徴についての予作成テンプレートとの比較に基づいて、特定人物について時間とともに変化することにより該人物の認証失敗を潜在的に許容するバイオメトリクスデータを利用することと、該予作成テンプレートを自動的に更新することとを包含する、
方法。

【請求項 2】

前記認証システムが二つ以上のバイオメトリクス／P I Nコード／スマートカードを使用して、前記第 2 ドライバ認証手順が前記第 1 ドライバ認証手順と異なるマルチモード認証システムにおいて、前記自動更新が達成される、請求項 1 に記載の方法。

【請求項 3】

前記少なくとも一つの認証手順が、時間とともに変化する更新済み顔認識バイオメトリクスデータを利用する、請求項 1 に記載の方法。

【請求項 4】

前記オペレータが前記車両に乗り込む際に、P I Nコードと指紋と顔認識とを使用する I D認証を要求する指示が出され、その後、システムがP I Nコードと顔認識とを用いて該オペレータ I Dを認証し、データベースの指紋テンプレートを更新するため指紋バイオメトリクスを使用する、請求項 1 に記載の方法。

10

【請求項 5】

前記オペレータの単一運転シフト中に多数のドライバ認証手順が実施され、該単一運転シフトが、仕事を始める際に該オペレータが前記車両に最初に乗り込む時から、仕事を終える際に該オペレータが該車両から最後に離れる時までに関及し、請求項 1 に記載の方法。

【請求項 6】

前記第 1 ドライバ認証手順の実施に基づいて前記車両のオペレータが認可ドライバであると判断されなかった時のみ前記第 2 ドライバ認証手順が実施される、請求項 1 に記載の方法。

20

【請求項 7】

前記第 1 および第 2 ドライバ認証手順の少なくとも一方が、該ドライバ認証手順の少なくとも一方の実施に関わる前記オペレータによる意識的対話を必要としない受動的認証検査である、請求項 1 に記載の方法。

【請求項 8】

前記受動的認証検査が、前記車両の認可ドライバを表す制御イメージ集合と比較されるイメージを持つ前記オペレータの身体的特徴の走査を包含する、請求項 7 に記載の方法。

【請求項 9】

走査される前記オペレータの身体的特徴が該オペレータの少なくとも一方の眼の虹彩である、請求項 8 に記載の方法。

30

【請求項 10】

走査される前記オペレータの身体的特徴が該オペレータの少なくとも一方の眼の網膜である、請求項 8 に記載の方法。

【請求項 11】

走査される前記身体的特徴が該オペレータの顔面サーモグラムである、請求項 8 に記載の方法。

【請求項 12】

前記オペレータの前記身体的特徴の適切な走査が行われるのを阻止する少なくとも一つの環境条件による誤認率を前記受動的認証検査が有する、請求項 8 に記載の方法。

【請求項 13】

前記少なくとも一つの環境条件が不十分な照明である、請求項 12 に記載の方法。

40

【請求項 14】

前記第 1 および第 2 ドライバ認証手順の少なくとも一方が、該ドライバ認証手順の少なくとも一方の実施に関わる前記オペレータによる意識的対話を必要とする能動的認証検査である、請求項 1 に記載の方法。

【請求項 15】

前記車両の認可ドライバを表す制御イメージ集合と比較されるイメージを有する前記オペレータの身体的特徴の走査を前記能動的認証検査が包含し、該走査が、該オペレータが身体部分をスキャナに載置することを必要とする、請求項 14 に記載の方法。

【請求項 16】

50

走査される前記オペレータの身体的特徴が、該オペレータの少なくとも1本の指の模様パターンである、請求項15に記載の方法。

【請求項17】

走査される前記身体的特徴が前記オペレータの掌形である、請求項15に記載の方法。

【請求項18】

前記オペレータを認可ドライバであると識別する個人認証番号を前記システムへ入力する要求を該オペレータに出すことを前記能動的認証検査が包含する、請求項14に記載の方法。

【請求項19】

前記能動的認証検査が、前記オペレータにより提示された認証カードのハードコーディング認証情報を読み取ることと、該認証カードから読み取られたハードコーディング認証番号に対応する個人認証番号を該オペレータが前記システムへ入力することを要求することとを包含する、請求項14に記載の方法。

10

【請求項20】

前記能動的認証検査が、規定フレーズを発話するように前記オペレータに命令を出すことと、該発話フレーズを言語パターンとして記録することと、該パターンを前記車両の認可ドライバの制御言語パターン集合と比較することとを包含する、請求項14に記載の方法。

【請求項21】

車両のオペレータが認可ドライバであることを確かめるための方法であって、
オペレータが認可ドライバであるかどうかを確認するため車載型マルチモードドライバ認証システムを利用することと、

20

前記車両の現在オペレータに第1ドライバ認証手順を実施して、該現在オペレータが該車両の認可ドライバであるか無認可ドライバであるかを判断することと、

前記車両の前記現在オペレータに第2ドライバ認証手順を実施して、該現在オペレータが該車両の認可ドライバであるか無認可ドライバであるかを判断し、該第2ドライバ認証手順が該第1ドライバ認証手順と異なることと、

実施された前記認証手順の少なくとも一方に基づいて前記車両の前記現在オペレータが無認可ドライバであると判断された時の潜在的悪影響を回避する救済手段を行使することと、

30

を包含し、

前記認証手順の少なくとも一方が、現在バイオメトリクス測定値と同じ特徴についての予作成テンプレートとの比較に基づいて、特定人物について時間とともに変化することにより該人物の認証失敗を潜在的に許容するバイオメトリクスデータを利用することと、該予作成テンプレートを自動的に更新することとを包含する、
方法。

【請求項22】

実施された認証手順のうち少なくとも二つに基づいて前記車両の現在オペレータが無認可ドライバであると判断された時に前記救済手段が行使される、請求項21に記載の方法。

40

【請求項23】

さらに、前記車両の前記現在オペレータに第3ドライバ認証手順を実施することと、該現在オペレータが該車両の認可ドライバであるか無認可ドライバであるかを判断することとを包含する、請求項21に記載の方法。

【請求項24】

実施された前記認証手順のうち少なくとも三つに基づいて前記車両の前記現在オペレータが無認可ドライバであると判断された時に前記救済手段が行使される、請求項23に記載の方法。

【請求項25】

前記ドライバ認証手順の各々が前記オペレータの単一運転時間中に実施され、該単一運

50

転時間が、該オペレータが運転席に乗って該車両の運転を開始する時から該オペレータが降りて該運転席を離れる時までに関及、請求項 2 1 に記載の方法。

【請求項 2 6】

前記第 1 ドライバ認証手順の実施に基づいて前記車両のオペレータが無認可ドライバであると判断された時のみ前記第 2 ドライバ認証手順が実施される、請求項 2 1 に記載の方法。

【請求項 2 7】

前記第 1 および第 2 ドライバ認証手順の少なくとも一方が、該ドライバ認証手順の少なくとも一方の実施に関わる前記オペレータによる意識的対話を必要としない受動的認証検査である、請求項 2 1 に記載の方法。

10

【請求項 2 8】

前記受動的認証検査が、前記車両の認可ドライバを表す制御イメージ集合と比較されるイメージを有する前記オペレータの身体的特徴の走査を包含する、請求項 2 7 に記載の方法。

【請求項 2 9】

走査される前記オペレータの身体的特徴が該オペレータの少なくとも一方の眼の虹彩である、請求項 2 8 に記載の方法。

【請求項 3 0】

走査される前記オペレータの身体的特徴が該オペレータの少なくとも一方の眼の網膜である、請求項 2 8 に記載の方法。

20

【請求項 3 1】

走査される前記身体的特徴が前記オペレータの顔面サーモグラムである、請求項 2 8 に記載の方法。

【請求項 3 2】

前記オペレータの前記身体的特徴の適切な走査を阻止する少なくとも一つの環境条件による誤認率を前記受動的認証検査が有する、請求項 2 8 に記載の方法。

【請求項 3 3】

前記少なくとも一つの環境条件が不十分な照明である、請求項 3 2 に記載の方法。

【請求項 3 4】

前記第 1 および第 2 ドライバ認証手順の少なくとも一方が、該ドライバ認証手順の少なくとも一方の実施に関わる前記オペレータによる意識的対話を必要とする能動的認証検査である、請求項 2 1 に記載の方法。

30

【請求項 3 5】

前記能動的認証検査が、前記車両の認可ドライバを表す制御イメージ集合と比較されるイメージを有する該オペレータの身体的特徴の走査を包含し、該走査が、該オペレータが身体部分をスキャナに載置することを必要とする、請求項 3 4 に記載の方法。

【請求項 3 6】

走査される前記オペレータの前記身体的特徴が、該オペレータの少なくとも 1 本の指の模様パターンである、請求項 3 5 に記載の方法。

【請求項 3 7】

走査される前記身体的特徴が前記オペレータの掌形である、請求項 3 5 に記載の方法。

40

【請求項 3 8】

前記オペレータを認可ドライバであると識別する個人認証番号を前記システムへ入力する要求を該オペレータに出すことを前記能動的認証検査が包含する、請求項 3 4 に記載の方法。

【請求項 3 9】

前記能動的認証検査が、前記オペレータにより提示された認証カードのハードコーディング認証情報を読み取ることと、該認証カードから読み取られたハードコーディング認証番号に対応する個人認証番号を該オペレータが前記システムへ入力することを要求することとを包含する、請求項 3 4 に記載の方法。

50

【請求項 4 0】

前記能動的認証検査が、規定フレーズを発話するように前記オペレータに命令を出すことと、該発話フレーズを言語パターンとして記録することと、該パターンを前記車両の認可ドライバの制御言語パターン集合と比較することとを包含する、請求項 3 4 に記載の方法。

【請求項 4 1】

車両のオペレータが認可ドライバであることを確かめるための方法であって、オペレータが認可ドライバであるかどうかを確認するため車載型マルチモードドライバ認証システムを利用することと、

前記車両の現在オペレータに第 1 タイプドライバ認証手順を実施して、該現在オペレータが該車両の認可ドライバであるか無認可ドライバであるかを判断することと、

前記車両の前記現在オペレータに第 2 タイプドライバ認証手順を実施して、該現在オペレータが該車両の認可ドライバであるか無認可ドライバであるかを判断し、該第 1 および第 2 ドライバ認証手順が相互に異なるタイプであってランダムな時間間隔を間に置いて実施されることと、

実施された前記認証手順の少なくとも一方に基づいて前記車両の前記現在オペレータが無認可ドライバであると判断された時の潜在的悪影響を回避する救済手段を行使することと、を包含し、

前記認証手順の少なくとも一方が、現在バイオメトリクス測定値と同じ特徴についての予作成テンプレートとの比較に基づいて、特定人物について時間とともに変化することにより該人物の認証失敗を潜在的に許容するバイオメトリクスデータを利用することと、該予作成テンプレートを自動的に更新することとを包含する、方法。

【請求項 4 2】

実施された認証手順のうち少なくとも二つに基づいて前記車両の前記現在オペレータが無認可ドライバであると判断された時に前記救済手段が行使される、請求項 4 1 に記載の方法。

【請求項 4 3】

前記ドライバ認証手順がランダムな時間間隔を間に置いて実施される、請求項 4 1 に記載の方法。

【請求項 4 4】

さらに、前記第 1 ドライバ認証手順における前記現在オペレータが無認可ドライバであるとの判断の直後に前記第 2 ドライバ認証を開始することを包含する、請求項 4 1 に記載の方法。

【請求項 4 5】

前記ドライバ認証手順の各々が前記オペレータの単一運転時間中に実施され、該単一運転時間が、該オペレータが運転席に乗って前記車両の運転を開始した時から該オペレータが降りて該運転席を離れる時まで及び、請求項 4 1 に記載の方法。

【請求項 4 6】

前記第 1 ドライバ認証手順の実施に基づいて前記車両のオペレータが無認可ドライバであると判断された時のみ、前記第 2 ドライバ認証手順が実施される、請求項 4 1 に記載の方法。

【請求項 4 7】

前記第 1 および第 2 ドライバ認証手順の少なくとも一方が、該ドライバ認証手順の少なくとも一方の実施に関わる前記オペレータによる意識的対話を必要としない受動的認証検査である、請求項 4 1 に記載の方法。

【請求項 4 8】

前記受動的認証検査が、前記車両の認可ドライバを表す制御イメージ集合と比較されるイメージを有する前記オペレータの身体的特徴の走査を包含する、請求項 4 7 に記載の方

10

20

30

40

50

法。

【請求項 4 9】

走査される前記オペレータの身体的特徴が該オペレータの少なくとも一方の眼の虹彩である、請求項 4 8 に記載の方法。

【請求項 5 0】

走査される前記オペレータの身体的特徴が該オペレータの少なくとも一方の眼の網膜である、請求項 4 8 に記載の方法。

【請求項 5 1】

走査される身体的特徴が該オペレータの顔面サーモグラムである、請求項 4 8 に記載の方法。

10

【請求項 5 2】

前記オペレータの前記身体的特徴の適切な走査が行われるのを阻止する少なくとも一つの環境条件による誤認率を前記受動的認証検査が有する、請求項 4 8 に記載の方法。

【請求項 5 3】

前記少なくとも一つの環境条件が不十分な照明である、請求項 5 2 に記載の方法。

【請求項 5 4】

前記第 1 および第 2 ドライバ認証手順の少なくとも一方が、該ドライバ認証手順の少なくとも一方の実施に関わる前記オペレータによる意識的対話を必要とする能動的認証検査である、請求項 4 1 に記載の方法。

【請求項 5 5】

前記能動的認証検査が、前記車両の認可ドライバを表す制御イメージ集合と比較されるイメージを有する前記オペレータの身体的特徴の走査を包含し、該走査が、該オペレータが身体部分をスキャナに載置することを必要とする、請求項 5 4 に記載の方法。

20

【請求項 5 6】

走査される前記オペレータの身体的特徴が該オペレータの少なくとも 1 本の指の模様パターンである、請求項 5 5 に記載の方法。

【請求項 5 7】

走査される前記身体的特徴が前記オペレータの掌形である、請求項 5 5 に記載の方法。

【請求項 5 8】

前記能動的認証検査が、前記オペレータを認可ドライバと識別する個人認証番号をシステムへ入力する要求を該オペレータに出すことを包含する、請求項 5 4 に記載の方法。

30

【請求項 5 9】

前記能動的認証検査が、前記オペレータにより提示された認証カードのハードコーディング認証情報を読み取ることと、該認証カードから読み取られたハードコーディング認証番号に対応する個人認証番号を該オペレータが前記システムに入力することを要求することとを包含する、請求項 5 4 に記載の方法。

【請求項 6 0】

前記能動的認証検査が、規定フレーズを発話する命令を前記オペレータに出すことと、該発話フレーズを言語パターンとして記録することと、該パターンを前記車両の認可ドライバの制御言語パターン集合と比較することとを包含する、請求項 5 4 に記載の方法。

40

【請求項 6 1】

現在バイオメトリクス測定値と同じ特徴についての予作成テンプレートとの比較に基づいて、特定人物について時間とともに変化することにより該人物の認証失敗を潜在的に許容するバイオメトリクスデータを利用して車両オペレータの I D を認証するための方法であって、

前記予作成テンプレートを自動的に更新し、該自動更新が、認証システムが二つ以上のバイオメトリクス／P I N コード／スマートカードを使用するマルチモード認証システムにおいて達成されること、
を包含する方法。

【請求項 6 2】

50

少なくとも一つの認証方法が前記オペレータのIDを認証するのに使用されるのに対して、オペレータ認証目的で現在用いられていない別の認証方法が、前記認証プロセスが成功だったと判断された後で前記予作成テンプレートを更新するのに使用される、請求項61に記載の方法。

【請求項63】

前記オペレータが前記車両に乗り込むと、PINコードと指紋と顔認識とを使用するID認証を要求する指示が出され、その後で前記システムが、PINコードと顔認識とを使用して該オペレータIDを認証し、データベースの指紋テンプレートを更新するため指紋バイオメトリクスを使用する、請求項61に記載の方法。

【請求項64】

さらに、前記車両のデータベースに前記バイオメトリクステンプレートを記憶することを包含する、請求項61に記載の方法。

【請求項65】

さらに、業務処理部門のデータベースに前記バイオメトリクステンプレートを記憶することにより、前記車両と該業務処理部門との間のリアルタイム通信を必要とする、請求項61に記載の方法。

【請求項66】

さらに、ドライバが自分で携帯するデータベースに前記バイオメトリクステンプレートを記憶することを包含する、請求項61に記載の方法。

【請求項67】

前記バイオメトリクステンプレートがスマートカードに記憶される、請求項66に記載の方法。

【請求項68】

さらに、前記認証テンプレートを記憶するためデジタル回転速度計ドライバカードの利用を包含し、該カードがこの種の記憶に適したスマートカードであるとともに、ある管轄区では法律により使用が強制されるため前記ドライバにより常に携帯されるものである、請求項67に記載の方法。

【請求項69】

さらに、

車両のオペレータが認可ドライバであるかどうかを確認する車載型マルチモードドライバ認証システムを利用して、該オペレータが認可ドライバであることを確かめることと、

前記車両の現在オペレータに第1ドライバ認証手順を実施して、該現在オペレータが該車両の認可ドライバであるか無認可ドライバであるかを判断することと、

前記車両の前記現在オペレータに第2ドライバ認証手順を実施して、該現在オペレータが該車両の認可ドライバであるか無認可ドライバであるかを判断し、該第1および第2ドライバ認証手順が時間間隔を間に置いて実施され、該時間間隔が該オペレータにより実施される作業の性質に左右されることと、

実施された前記認証手順の少なくとも一方に基づいて前記車両の前記現在オペレータが無認可ドライバであると判断された時の潜在的悪影響を回避する救済手段を行使することと、

を包含する、請求項61に記載の方法。

【請求項70】

前記第2ドライバ認証手順が前記第1ドライバ認証手順と異なる、請求項69に記載の方法。

【請求項71】

前記第2ドライバ認証手順が前記第1ドライバ認証手順と同じである、請求項69に記載の方法。

【請求項72】

さらに、前記第1ドライバ認証手順における前記現在オペレータが無認可ドライバであるとの判断の直後に前記第2ドライバ認証を開始することを包含する、請求項69に記載

10

20

30

40

50

の方法。

【請求項 7 3】

多数のドライバ認証手順が前記オペレータの単一運転シフト中に実施され、該単一運転シフトが、作業を始める際に該オペレータが最初に前記車両に乗り込む時から作業を離れる際に該オペレータが最後に該車両を離れる時まで及び、請求項 6 9 に記載の方法。

【請求項 7 4】

異なるタイプの複数のドライバ認証手順がランダムな時間間隔で行われる、請求項 6 9 に記載の方法。

【請求項 7 5】

前記第 1 および第 2 ドライバ認証手順の少なくとも一方が、該ドライバ認証手順の少なくとも一方の実施に関わる前記オペレータによる意識的対話を必要としない受動的認証検査である、請求項 6 9 に記載の方法。

【請求項 7 6】

前記受動的認証検査が、前記車両の認可ドライバを表す制御イメージ集合と比較されるイメージを有する前記オペレータの身体的特徴の走査を包含する、請求項 7 5 に記載の方法。

【請求項 7 7】

走査される前記オペレータの身体的特徴が該オペレータの少なくとも一方の眼の虹彩である、請求項 7 6 に記載の方法。

【請求項 7 8】

走査される前記オペレータの身体的特徴が該オペレータの少なくとも一方の眼の網膜である、請求項 7 6 に記載の方法。

【請求項 7 9】

走査される前記身体的特徴が前記オペレータの顔面サーモグラムである、請求項 7 6 に記載の方法。

【請求項 8 0】

前記オペレータの前記身体的特徴の適切な走査が行われるのを阻止する少なくとも一つの環境条件による誤認率を前記受動的認証検査が有する、請求項 7 6 に記載の方法。

【請求項 8 1】

前記少なくとも一つの環境条件が不十分な照明である、請求項 8 0 に記載の方法。

【請求項 8 2】

前記第 1 および第 2 ドライバ認証手順の少なくとも一方が、該ドライバ認証手順の少なくとも一方の実施に関わる前記オペレータによる意識的対話を必要とする能動的認証検査である、請求項 6 9 に記載の方法。

【請求項 8 3】

前記能動的認証検査が、前記車両の認可ドライバを表す制御イメージ集合と比較されるイメージを有する前記オペレータの身体的特徴の走査を包含し、該走査が、該オペレータが身体部分をスキャナに載置することを必要とする、請求項 8 2 に記載の方法。

【請求項 8 4】

走査される前記オペレータの身体的特徴が、該オペレータの少なくとも 1 本の指の模様パターンである、請求項 8 3 に記載の方法。

【請求項 8 5】

走査される前記身体的特徴が該オペレータの掌形である、請求項 8 3 に記載の方法。

【請求項 8 6】

前記能動的認証検査が、前記オペレータを認可ドライバとして識別する個人認証番号を前記システムに入力する要求を該オペレータに出すことを包含する、請求項 8 2 に記載の方法。

【請求項 8 7】

前記能動的認証検査が、前記オペレータにより提示される認証カードのハードコーディング認証情報を読み取ることと、該認証カードから読み取られたハードコーディング認証

10

20

30

40

50

番号に対応する個人認証番号を該オペレータが前記システムに入力することを要求することとを包含する、請求項 8 2 に記載の方法。

【請求項 8 8】

前記能動的認証検査が、規定フレーズを発話する命令を前記オペレータに出すことと、該発話フレーズを言語パターンとして記録することと、該パターンを前記車両の認可ドライバの制御言語パターン集合と比較することとを包含する、請求項 8 2 に記載の方法。

【請求項 8 9】

前記第 2 ドライバ認証手順が前記第 1 ドライバ認証手順と同じである、請求項 1 に記載の方法。

【請求項 9 0】

さらに、前記第 1 ドライバ認証手順における前記現在オペレータが無認可ドライバであるとの判断の直後に前記第 2 ドライバ認証を開始することを包含する、請求項 1 に記載の方法。

【請求項 9 1】

前記単数または複数の認証システム、単数または複数の認証手順、単数または複数の認証検査、単数または複数の認証番号、単数または複数の認証カード、単数または複数の認証失敗、認証情報が、場合に応じて、対応する単数または複数の識別システム、単数または複数の識別手順、単数または複数の識別検査、単数または複数の識別番号、単数または複数の識別カード、単数または複数の識別失敗、識別情報、または、場合に応じて、認証および識別の単数または複数のシステム、単数または複数の手順、単数または複数の検査、単数または複数の番号、単数または複数のカード、単数または複数の失敗、情報の組合せにより置き換えられる、前出請求項 1 乃至 9 0 のいずれかに記載の方法。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本発明は、ドライバ I D 認証を実施するための方法と装置に関連する。

【背景技術】

【0 0 0 2】

運送業界は、高価な物品の密輸および盗難に関わる問題に悩まされている。特にテロの脅威が高まっているようなので、様々なセキュリティ問題が世界中で重要なテーマとなっている。セキュリティのレベルを向上させる方法の一つは、ドライバが正規ドライバであることを確かめるため、商用トラックに認証システムを設置することであろう。

【0 0 0 3】

特許文献 1 は、盗難、強奪、攻撃が発生した場合、ドライバが個人識別番号 (P I N) を打ち込むことにより使用認可を証明できない場合に、電子エンジン制御装置を備える自動車を徐々に作動停止にする、車両の電子盗難防止装置を開示している。識別を証明するために電子セキュリティシステムにより制御される質問は、車両が使用されている間の移動時間内または経路上において適当に定められた間隔で行われる。ドライバが応答時間枠内に自分の I D を証明できない場合には、電子エンジン制御装置に干渉することにより往來に危険を与えずに、静止するまで徐々に車両の速度が落とされ、静止するとすぐに、ブレーキシステム、さらに存在するならば駆動系電子システムへの干渉によって運転または牽引により逃走することのないように車両がブロックされる。

【0 0 0 4】

特許文献 2 は、車両の認可オペレータの認証のための方法と装置を開示している。認証されるオペレータのバイオメトリクスデータが、車両の運転前および／または運転中に判断されて、基準データと比較される。測定されたバイオメトリクスデータと基準データとの間に整合が見つからない場合には、自律的作動制御システムが車両の制御を引き継ぐ。

【0 0 0 5】

特許文献 3 は、人間のオペレータと協働する、機器を制御するための装置に関連し、この機器は、メモリ手段を備えるとともに特定の認可人間オペレータに関連する許可要素と

10

20

30

40

50

対話できる機器側安全装置を具備し、機器は、許可要素との対話の後に始めて作動可能となる。

【0006】

一用途では、例えば、特定ドライバによる容認不可能な長時間運転に関して自動車を監視するため、監視すべき事象が許可要素のメモリ要素に記憶される。別の用途では、認可パイロットのみによって航空機が確実に航行されるように、航空機の制御手段が監視される。ドライバまたはパイロットの不変の身体特徴、例えば指紋が許可要素に記憶される。実際の身体特徴がセンサにより検出されて、記憶されたものと比較される。検出された身体特徴と記憶されたものとが同一である場合のみ、車両または航空機を使用することができる。

10

【0007】

特許文献4は、常時使用不能イグニッションシステムを有する自動車に使用するためのシステムを提供する。このシステムは、ドライバを識別するための、指紋リーダまたは網膜リーダなどのリーダを含む。リーダからの出力は、ドライバが車両を操作することを認可されているかどうかを判断するため、メモリに記憶された対応の生理学的データと比較される。任意で、プリセットされた規定時間内のみの車両の操作を許容するようにタイマが採用される。

【0008】

【特許文献1】独国特許出願公開第4326514号明細書

【特許文献2】独国特許出願公開第10156731号明細書

20

【特許文献3】米国特許出願公開第2004078118号明細書

【特許文献4】米国特許第5686765号明細書

【発明の開示】

【発明が解決しようとする課題】

【0009】

本発明の目的は、トラックドライバ認証のための、柔軟かつ使用が容易で非侵害的な詐称防止の方法とシステムを提供することである。別の目的は、同様の認証および／または識別の方法とシステムとを提供することである。

【課題を解決するための手段】

【0010】

30

かかる目的は、独立請求項の特徴により達成される。

【0011】

本出願は二つの目的を持つ。一つはドライバ認証のための適切な方法を発見して、検査および今後の開発に使用できる認証システムのプロトタイプを構築することである。他は、トラックドライバがこのようなシステムをどのように捉えるか、そして彼らの捉え方が、より高いセキュリティの必要性の高まりとどのように結びつくかを研究することである。本出願は、運送業界に焦点を当てている。

【0012】

11種類の可能な認証方法について研究が行われた。プロトタイプに使用する方法の選択の根拠を明らかにするため、理論的研究を補足するため、トラックドライバおよび運送業者へのアンケートおよびインタビューが実行された。

40

【0013】

検査には、1種類の標準的方法と3種類のバイオメトリクス認証方法、つまり指紋認証、顔認識、音声認識、PINコードが選択された。これらの方法は、トラック運転シミュレータで実行されるシステムに集約された。システムをユーザに使いやすくするために、グラフィカルユーザインタフェースが開発された。18人のトラックドライバが認証システムの検査を受けた。彼らの経歴、期待、意見を聞き出すため、検査の前と後に十分なインタビューが行われた。

【0014】

検査参加者の大部分はシステムに対して肯定的であった。現在はその必要性を感じない

50

としても、「将来的には」必要となると確信していた。しかし、参加者の中にはシステムに管理されていると感じるのでこれに不快感を持つ者もあった。ユーザのプライバシーを尊重するシステムを設けることと、システム的使用方法について必ずユーザが十分に説明を受けることがいかに重要であるかが明らかとなった。認証システムに使用された技術の一部は、自動車分野に適応するようにさらに開発が必要であるが、確実にエラーに強いシステムを実現することは可能であると考えられる。

【0015】

以下でさらに詳しく説明するように、ドライバ認証システムに関する上述の研究と分析の過程でいくつかの発明が行われた。

【0016】

少なくとも一つの実施例において、発明は、車両のオペレータが認可ドライバであることを確かめるための方法という形を取る。これは、オペレータが認可ドライバであるかどうかを確認するのに使用される車載型マルチモードドライバ識別システムの利用によって達成される。第1ドライバ識別手順は、車両のオペレータに対して実施され、その人が車両の認可または無認可ドライバであるかどうか判断される。通常は、評価される者が認可ドライバであるかどうかを確かめるためのだけの検査である。その人が認可されていることが識別手順で確かめられなかった場合には、無認可であると確かめられたものと推定され、そのような処置が取られる。第1識別手順の結果と関係なく、続いて第2ドライバ識別手順がオペレータに対して実施され、その人が認可ドライバであるか無認可ドライバであるかを再び判断しようと試みる。第1および第2ドライバ識別手順は時間間隔を間に置いて実施され、この時間間隔はオペレータにより実施される作業の性質に左右される。例えば、一日に数回しか停止せずに無認可オペレータがハンドルを握る機会がより少ない長距離ドライバと比較して、停止や車への乗降を頻繁に行う都市部での配達ドライバでは、識別確認の間の間隔が異なる。最後に、実施された識別手順の少なくとも一方に基づいて車両の現在オペレータが無認可ドライバであると判断された時の潜在的な悪影響を回避するため、救済（補正）措置が取られる。トラックは通常、オペレータを認可ドライバと識別できなかったことに基づいて急停止することはないが、事業所への通知などのことがらがテレマティックスにより行われるか、ドライバによる次の停止の後に車両の再始動が妨害される。

【0017】

ドライバ識別手順は相互に異なっているか類似していることが考えられる。

【0018】

第2ドライバ識別は、オペレータが無認可ドライバであるとの第1ドライバ識別手順における判断の直後に開始される。

【0019】

あるいは、第1ドライバ識別手順の実施に基づいてオペレータが認可ドライバであると判断できない時のみ、第2ドライバ識別手順が実施されてもよい。

【0020】

少なくとも一つの実施例では、識別手順の一方は、ドライバ識別手順の実施に関わるオペレータによる意識的対話を必要としない受動的識別検査である。一つの例において受動的識別検査は、車両の認可ドライバを表す制御イメージ集合と比較されるイメージを有するオペレータの身体的特徴の走査を包含する。

【0021】

第1および第2ドライバ識別手順の少なくとも一方は、ドライバ識別手順の少なくとも一方の実施に関わるオペレータによる意識的対話を必要とする能動的識別検査である。一例は、指または手をスキャナに載置することである。あるいは、能動的識別検査は、オペレータを認可ドライバと識別するシステムへ個人識別番号を入力する要求をオペレータに出すことを含む。能動的識別検査の別の形は、オペレータにより提示される識別カードのハードコーディング識別情報を読み取ることを包含する。次にシステムは、識別カードから読み取られたハードコーディング識別番号に対応する個人識別番号をオペレータがシス

テムに入力することを要求する。同様に、能動的識別検査は、オペレータが規定のフレーズを発話する命令を出すことと、発話されたフレーズを言語パターンとして記録することと、このパターンを車両の認可ドライバの制御言語パターン集合と比較することとを包含する。

【0022】

本発明の一変形例または発展例では、第1および第2識別手順は、相互に異なる二つのタイプであり、ランダムな時間間隔を間に置いて実施される。

【0023】

進歩性を備える別の面では、人的要因の専門家がこの分野で取り組んでいる課題の一つがいつどのようにしてドライバが認証されるべきかであることを踏まえた自動認証システムが開示される。商用車の使用は用途に応じて異なり、一部のドライバは一日に20回車両の乗降を行うのに対して、別のドライバはこれを一日に2、3回しか行わない。システムがドライバにとって不愉快になることなく十分に高いセキュリティレベルを維持するため、いくつかの異なる戦略が使用される。その一つは、運転中に自動認証を実施することである。例えば、ドライバが気づくことなく運転中に顔認識（認証）が実施される。これに失敗した場合には、自身のPINコードを入力するか別の方法を用いるようにドライバが指示される。認証はランダムな間隔で実施される。

【0024】

進歩性を備えるまた別の面では、ドライバが異なるタイミングで異なる方法を指示されるいくつかの認証方法を車両が具備する。方法とタイミングの選択がランダム化される場合、ドライバはいつまたはどのようにして自分を認証するのかを知る方法を持たない。いつまたはどの方法で自身の認証をしなければならないかを詐称者は決して分からないので、システムにおけるこの種の予測不能性の実行はセキュリティレベルを高める。

【0025】

進歩性を備えるさらに別の面では、バイオメトリクスシステムにおいて、認証（整合）されるのは測定されたバイオメトリクス（イメージ）そのものではなく、バイオメトリクスのテンプレートである、つまり、測定されたバイオメトリクスからテンプレートが抽出されて、データベース内の既存のテンプレートと比較されるのである。記憶されたテンプレート（またはバイオメトリクス測定値そのもの）との整合に関する問題の一つは、人のバイオメトリクスが時間とともに変化することに対して、記憶されたテンプレートがそうではないという事実である。例えば、人の指紋は傷による変化を受け、発話されたパスワードは病気または年齢による変化を受ける。この問題の解決法の一つは、テンプレートを（手動または自動で）更新することである。自動更新は、マルチモード認証システム、つまり二つ以上のバイオメトリクス／PINコード／スマートカードを使用する認証システムにおいて達成される。この時、ドライバの認証には一つ以上の認証方法が使用され、（認証プロセスが成功した場合には、）使用されていない一方法によりテンプレートを更新する。例を挙げると、ドライバは車両に乗り込み、PINコード、指紋、顔認識を用いて自身を認証するように指示される。システムはPINコードおよび顔認識を用いて彼を認証し、指紋バイオメトリクスを用いてデータベースの指紋テンプレートを更新する。

【0026】

記憶されたバイオメトリクステンプレートについての関連の面において重要な課題は、テンプレートをどこに記憶するかである。基本的に三つの選択肢がある。（i）トラック内のデータベース、（ii）事務処理部門のデータベース（車両と事務処理部門との間のリアルタイム通信が必要）、および／またはスマートカードなどドライバが携帯する（相互接続）データベース。一つのオプションは、認証テンプレートを記憶するのにデジタル回転速度計ドライバカードを使用することである。カードはスマートカードであり、ゆえにこの種の記憶に適しているが、さらに重要なのは、ドライバが（少なくともヨーロッパでは）法律によって使用を強制され、ゆえに常にドライバに携帯されなければならないということである。

【0027】

進歩性を備える別の面では、周知の識別認証システムに一般的に関連する不確実性を認めたうえで冗長化が設けられる。顔識別方法の実施は例えば照明条件により影響される。いくつかの方法（顔認識とPINコードなど）を用いて、システムにおいて冗長化が達成される。例えば、ドライバが運転中であって予定の自動顔認識が実施されると、何らかの理由（照明条件が不良であるなど）で失敗する。するとドライバは、指紋およびPINコードを使用して自身を認証するように求められる。

【発明の効果】

【0028】

最後に、上述した面の各々は、単独または組合せで、テレマティックスの分野において実行できることを評価すべきである。つまり認証システムは、事務部門に対して、または

10

【発明を実施するための最良の形態】

【0029】

本発明は、上述および他の目的と長所とともに、図示された実施例についての以下の詳細な説明から最も良く理解されるだろう。

【0030】

セキュリティ問題は全世界で高い優先順位を与えられている。これは自動車業界にも影響を持ち、商用車でドライバ認証システムを実施することによりセキュリティを高めることが可能かどうかという問題が提起されている。ここで調査される問題は、例えばどのタイプの認証を使用するかと、このようなシステムの恩恵を被るのは誰かということである。本節は、本出願の背景と目的と制約とを含む。出願の概要を提供するため、本節の最後に手引きを設ける。

20

【0031】

高まるテロの脅威ゆえに、社会でのセキュリティを向上させるため研究と開発に巨額の投資が行われている。国土安全保障省（米国）はこの活動の一例である。2001年の国際貿易センターに対するテロ攻撃の後には特に、どのように提示されるのであっても、セキュリティはますます重要となっている話題である。とりわけ米国では、多くの法律改正が

30

【0032】

高まるセキュリティ需要を示す一例は、いくつかの空港、例えばアムステルダムスキポール空港やスウェーデンのウーメオ空港で、乗客のバイオメトリクス認証の使用を試行していることである。2001年のパイロット・イヤーの後、虹彩認識を用いた自動出入国システムがアムステルダムスキポール空港で常時行われている。

40

【0033】

市場からの需要と法律改正に対応するため、より進化した識別および認証技術を用いた、従来のものよりはるかに進化したセキュリティシステムを新製品が備えることが多い。一例は、埋め込み型指紋スキャナを備えるノートパソコンである。

【0034】

密輸、テロリスト攻撃、高価な品物の盗難は、通常、盗難車が関与するシナリオである。そのため、運送業界が公共セキュリティの向上に力を注いでいる分野であることは言うまでもない。輸送の安全性とセキュリティを高める際に中心となる目的は、ドライバが、自称している本人であるかどうかを認証することである。

50

【0035】

本発明は、ドライバ認証に適しているかもしれない潜在的技術の検査ばかりでなく、二つの異なる可能性とシステムについてのドライバ意見の評価結果とを組み合わせたものである。プロトタイプの実験の前後におけるインタビューとアンケートがドライバ意見を形作っている。当事者／製造者にとって関心があるのはどのセキュリティ手段であるかということと、実用性と安全性とプライバシーについてのドライバの捉え方とこれをどのように調和させるかということとの比較も実施される。

ドライバ認証システムの利点

【0036】

トラックは様々な目的で使用される。ゆえに、多様な状況に適応できる柔軟なシステムが必要とされる。そのため、このようなシステムを設計するには多様な難題が発生する。すべての目的に合うシステムを構築するのは不可能であるが、できる限り多くの要求を満たすことが望ましい。ドライバ認証システムが有益である様々な状況を以下にいくつか挙げる。

【0037】

南米では、盗難車についての重大な問題が存在する。そのため、高価な物品を輸送する際には、すべてが良好に進行しているかどうかを確認するためにドライバが10分おきに保険会社に電話することが一般的なやり方である。車両が認証システムを装備している場合には、車両が正規ドライバにより運転されていることをシステムが保険会社に継続的に保証するので、ドライバは運転に専念できる。

【0038】

認証システムによって運送業者は、ドライバが以前に交通関連の軽犯罪の判決を受けていないことを確認できる。ドライバに関する情報を記憶するため、データベースが必要となる。このデータベースが当局に接続されたとすると、ほぼリアルタイムでファイルチェックが行われる。

【0039】

ドライバ認証と車両搭載型アルコールインタロック装置の両方を備える運送業者は、「信用ドライバマーク」を受け取る。それで客は、自分の品物が「信用」ドライバによって運搬されていることを確信する。国内道路協会および保険会社との協力によって車両保険のコストは低くなっている。

【0040】

認証システムの使用に対する報奨は、信用のある認証ドライバは計量ステーションまたは道路通行料金所をパスする権利が与えられることである。これは、ドライバの仕事を楽にするとともに輸送をより効率的にする。

【0041】

記録されたパラメータを特定ドライバと関連させる認証は、休憩なしで法定の4.5時間（欧州法）よりも長く運転しているかどうかを管理できる。この場合、ドライバだけでなく運送業者にも警告が送られる。

【0042】

スウェーデンでは、罪に問われた者が相手を非難するという事実のために却下される事件が発生している。事故や犯罪の場合、認証システムにより、特定の時に実際には誰が車両を運転していたかを捜査員は確認できる。

【0043】

車両が盗難されて認証の必要性がある場合には、システムにより盗難が明らかになるまでに詐称者は遠くには行けないだろう。車両が犯罪に使われた場合に、このことは、より短時間の措置を保証する。

【0044】

信用できる会社を選ぶための客の手間を簡単にするため、スウェーデンの客は“Service trapping”（サービス階段）と呼ばれるプロセスを利用できる。このプロセスはいくつかのランキング段階で構成される。会社のランキングが高いほど、客にスム

10

20

30

40

50

ーズに受け入れられる。ドライバ認証システムはこのプロセスの一部であり、認証された信用ドライバを擁する運送業者に高いランクを付与して、税関通過をより効率的にする。

【0045】

さらに、トラックに認証システムがある場合には、ドライバの個人的な好みに合わせてドライバ環境の設定を自動的に調節することが可能になるなど、ドライバはシステムから利益を受ける。例を挙げると、ドライバシート、環境制御、ステレオなどの設定が自動的に調節される。しかしこれは本出願の対象外である。

【0046】

本出願には二つの主要な目的がある。一つは、ドライバ認証の適切な方法を発見して、検査および今後の開発に使用できる認証システムのプロトタイプを構築することである。他の目的は、ドライバがこのようなシステムをどのように把握し、その捉え方が、高いセキュリティを求める需要の高まりとどのように合致するかを研究することである。

【0047】

これら二つの目的は、「トラックドライバ認証のための柔軟で使いやすく、非侵害的で詐称にも安全なシステムを設計するための有効な認証方法を使用する可能性を研究すること」とまとめることができる。

【0048】

ここに記載される認証方法はほぼいかなるタイプの車両にも使用できるが、本出願の中心は商用トラックおよび運送業である。

【0049】

三つのバイオメトリクス方法が実施され、プロトタイプにおいて検査を受ける。方法の選択は、作業中に読み取られた理論に主として左右されるが、価格と納入時間も決定に影響する。

【0050】

認証システムとユーザとの間の通信を容易にするためG U Iが開発された。しかし、G U Iを開発した著者は、ユーザ能力と設計についての知識を前もって所有していたので、ここではその理論には言及しない。そのうえ、本出願の中心となるのは、G U Iでなくシステムである。

【0051】

車両の認証システムは、セキュリティを高めるための多くの可能性を広げる。検討される問題のいくつかは、どのタイプの認証を使用するかと、このようなシステムにより恩恵を受けるのは誰かということである。しかし、このような認証システムを構築する時に検討すべきなのは、セキュリティ問題のみではない。ドライバのプライバシーと安全についての捉え方も検討に入れるべきである。これらの異なる視点は問題へのアプローチを多様なものにし、そのため、セキュリティ、安全性、プライバシーについての様々な見通しをここで説明する。これは、このような条件がここでは何を表すかを明らかにし、それが本出願ではどうして重要であるかを示すことでもある。

セキュリティ

【0052】

個人、企業、公共、国家セキュリティなど、異なるタイプのセキュリティが存在する。これらの面すべてが、単一の定義の付与を困難にする。だが、一般的に受け入れられている概念は、セキュリティとは望ましくない出来事が発生する可能性を低くするために取られる品質または措置だということである。

【0053】

この論点におけるセキュリティ問題は、上述したすべての用途を含む。公共セキュリティおよび国家セキュリティは、テロ攻撃の危険に関する場合に検討すべき問題である。危険物の輸送に関連するリスクも、公共セキュリティに影響する。盗難車両のリスクは企業セキュリティに関わる。最後に、個人セキュリティは、ドライバ認証システムの実行に付随するリスクを利点とともに伴う。これらの様々な問題について後述する。

プライバシー

10

20

30

40

50

【0054】

認証システムの主目的は、セキュリティのレベルを高めることである。これを行う方法の一つはバイオメトリクス方法を使用することである。問題は、個人のプライバシーを侵害することがあるので、それ自体が脅威であるということである。ゆえに、ユーザのプライバシーは、ここで検討する別の課題である。

【0055】

プライバシーとは、自分個人を守るための個人の領域を持つことであり、公的機関、雇用者、その他から覗き見されずにある事柄を秘密にしておくことのできる権利と表せる。バイオメトリクス方法は、大規模監視を行う（ジョージ・オーウェルの「1984」のような）「ビッグブラザー」の印象を与える。そうだとすれば、この方法は、個人のプライバシーを侵害しているかのように受け取られることになる。

10

安全性

【0056】

セキュリティと安全性は、非常に関連性があるとしても全く同じものではない。安全性は、不当な事柄が発生することを恐れずに人が何かをすることのできる時または場所として定義できる。ゆえに、優れたセキュリティは、安全性を認識する結果を生む。

【0057】

すべての方法の使用が安全であるとしても、侵害的であると認知する場合、または何らかの形で自分に害を与えると考える場合には、人はそれを使いたがらない。その結果、どれほど安全な方法であってもこれを信用しない人はそれを使用しないため、システムについてのユーザの捉え方を考慮しなければならない。ドライバがその方法を使用したことがあるかどうかは重要でなく、それについての意見は常に持っているだろう。しかし、その捉え方は必ずしも事実および現実に沿ったものではない。例えば、虹彩走査は最も正確な方法の一つであるとともに使用が安全な方法だと考えられているが、多くの人は眼を走査するシステムを使用するという考えは好まない。走査が眼を傷付けることを恐れる人は、このようなシステムを安全だと認めないだろう。

20

【0058】

未知の事柄はしばしば人に恐怖を与え、知識は否定的な感情を消し去るので、情報は重要である。上述したように、人は、虹彩走査は不快な認証方法であると信じる傾向があるが、SASにより行われた試験はそうではないことを証明した。ウーメオ空港で二種類の異なる認証システムつまり指紋と虹彩走査の検証を行った。乗客が頻繁に試験に参加し、半分の時間は指紋認証、半分の時間は虹彩走査を使用した。参加者の大部分はバイオメトリクスの使用に肯定的で（78%が、SASは乗客のバイオメトリクス認証を導入すべきだと考えていた）、この場合、虹彩走査が指紋認証よりも若干高い評価を受けた。これは、そのシステムが自分およびその仕事にとって有益であると利用者が納得しているはずであることを意味する。そうでなければ、使用に同意しないだろう。

30

車両正規ドライバの認証

【0059】

現在の市場には多くの異なる認証方法が存在し、その一部はすでに使用されており、他はいずれ登場する。それにも関わらず、実際には誰が車両を運転しているかについての認証は今日行われていない。その意図は、様々な認証方法のいくつかを導入して、自動車とユーザの観点の両方から見たその長所と短所を列挙することである。本節は、バイオメトリクスの導入と、様々なバイオメトリクス方法についての説明を含む。PIN（個人識別番号）、パスワード、様々なタイプのカードも、認証の方法である。これらは今日では頻繁に使用されるので、読者には周知であると推定され、ここでは簡単にのみ言及する。

40

【0060】

これらの方法すべての大まかな長所の一つは、認証を実行するためにユーザが現在の作業を中断しなければならないことである。これはユーザのリスク意識を高め、より集中して注意深くなるようにユーザに影響する。

バイオメトリクス方法の紹介

50

【0061】

バイオメトリー（生物統計学）の語はラテン語を語源とし、「生命の測定」と翻訳できる。バイオメトリーは通常、測定される生体の特徴の統計的研究を指す。他方、バイオメトリクスはむしろ、人間をその特徴を測定することにより特定するための分析に使用される。バイオメトリクス方法は、19世紀後半から識別および認証の目的に使用されている。本出願においてバイオメトリクス認証／識別方法に言及する際には、手、顔、眼など、人に固有の一つ以上の身体特徴を分析する方法を意味する。

【0062】

最適な認証方法は、使用される場所と理由に応じて変化する。しかし、どの方法を使用するかを決定する際に満たすように努力すべき基本的要件が三つある。理想的な認証方法を達成するため、測定される特徴は独自つまりその個人に固有のものあるべきであり、永久的つまり時間とともに変化するべきではなく、最後に普遍的つまり誰もが所有するべきである。方法により分析される特徴の受容可能性と入手可能性も検討すべきである。バイオメトリクス特徴は、その測定をユーザが侵害的であると受け取らない場合に受容可能である。特徴がセンサに提示しやすい場合、この特徴は入手可能であると言われる。

10

【0063】

バイオメトリクス認証方法を用いて、人が、自己を識別し、何か例えばアクセスカードを所有し、何か例えばパスワードまたはPINを記憶し、何者かであるためには、基本的に三つの方法がある。

【0064】

20

ここで説明する様々な方法の大部分は、認証と識別の両方に使用できるが、二つの語の間の区別を記すべきである。

識別：大集団の中で人が誰であるかを知るために方法が使用される際には、識別と呼ばれる。これは時に「一对多の比較」と呼ばれる。識別に使用される特徴に整合する一人の個人を見つけるために大集団内を検索することを意味する。

認証：人が、自分が主張している人物であるかどうかを分析するのに方法が使用される際には、認証と呼ばれる。これは「一对一の比較」と呼ばれる。この場合には、その人物の名前で保存されているデータと人物の特徴とを比較することのみが必要である。

【0065】

ドライバは会社に周知であると推定されるので、本出願は認証に焦点を当てる。ゆえにシステムは、ハンドルの前にいるのが本当に予定のドライバであることを認証することのみ使用される。

30

【0066】

バイオメトリクス認証方法の使用を検討に値するものにする長所はいくつかある。バイオメトリクス特徴は忘れられることがない。身体的属性は間違えられることがない。身体的属性はIDカードよりも模造が困難である。指紋パターンと他のバイオメトリクス特徴は、例えばパスワードほど容易に推測または漏洩されない。

【0067】

バイオメトリクスセキュリティシステムにまつわる問題の一つは、誰かがなんとかしてID情報を盗もうとする場合に生じる可能性のある損害の程度である。人がクレジットカードを紛失するか、侵入者警報器を切るシークレットPINを他の者が見つけた場合には、新しいカードを入手するかコードを変更することが常に可能である。しかし、人の指紋が複製された場合には、新しいものを作るのは不可能である。誰かが自分を騙る危険性が常にあるので、人は認証に指紋を使用することはもはやできなくなる。

40

【0068】

盗難の場合には、潜在的な詐称者が使用できないようにするために、関連のデータベースを更新して、盗難されたIDアイテムを登録することが重要である。2001年9月11日のハイジャック犯の一人は、5年前に米国でサウジアラビア人から盗んだパスポートを使用した。データが更新されたならば、おそらくこれは回避されただろう。2001年当時の乗客もバイオメトリクスにより自己を識別する必要があったならば、テロリストが

50

そのミッションを成功させることはもっと困難だっただろう。それでも、バイオメトリクス認証方法は決して完璧な方法ではない。詐称者は、システムを出し抜くか操作するためにデータベースまたはデータベースとスキャナとの間の接続を破壊することが可能である。ゆえに、十分に確実な解決法を見つけることが目的であるとしても、すべてのリスクを完全に無くすことは不可能である。

認証プロセス

【0069】

本節では、最も一般的な認証方法の概要を提示する。その大部分は、ユーザを登録／整合する、図1による以下の段階を用いる。

データ獲得：センサが対象物を走査する

10

信号事前処理：例えば、音声認識システムにおいて環境ノイズを除去する

特徴抽出：様々な特徴を分析して獲得データの小さな集合に基づいてテンプレートを作成する

登録／整合：テンプレートをデータベースに追加するか（登録）、すでにデータベースにあるテンプレートと比較する（整合）

決定：整合に成功すれば対象者を認可し、失敗すれば認可を取り消す

【0070】

テンプレートは主に二つの理由で作成される。一つは記憶されるデータの量を減少させることであり、他は以下の整合段階の複雑性を低下させることである。テンプレートに関する別の利点は、例えば指紋スキャナを使用する場合に、模様の写真全体は記憶されずに独自特徴のテンプレートのみが記憶される。これは指紋の複製にテンプレートを使用することを困難にする。

20

生体検出

【0071】

詐称者は、指紋スキャナをパスするために不正手段を用いるか認可ユーザから指を切断しようとするかもしれない。虹彩走査と掌形にも同じことが言える。一部の音声認識システムはテープレコーダにより、顔認識システムは認可ユーザの写真によりだまされることがある。しかしこれを回避する手段がある。バイオメトリクス認証システムは、検索されたサンプルが人間からのものであることを確認するための生体検出を備えることが可能である。生体検出は認証方法に適していなければならない。ゆえに、各方法について生体検出がどのように実施されるかを本書で提示する。

30

バイオメトリクス認証方法

【0072】

認証システムの基本的手順は、本節で前に説明した。いくつかの異なるバイオメトリクス認証方法の説明、つまりその歴史、どのように作用するか、そしてその長所と短所を提示する。

指紋認証

【0073】

指紋は、おそらく最もよく知られ広まっているバイオメトリクス識別方法である。19世紀の終わりと20世紀の初めには、いくつかの異なるタイプの識別方法が開発された。これらの方法は通常、2、3の主なパターンに関するある種の包括的分類を行う。指紋を見ると、凸部と凹部はパターンを形成し、これは不規則で固有な線の特徴とする。現在のスキャナは非常に高速かつ正確であり、この方法は日常的な使用に受け入れられるようになっている（図2参照）。

40

【0074】

模様全体の比較はたくさんの処理力を必要とし、そのためスキャナは通常、顕著な特徴、例えば凸部が途切れるか二分する箇所に焦点を当てる。これらの特徴は詳細と呼ばれる。比較を行うため、スキャナは複雑なアルゴリズムを用いて詳細を発見および分析する。基本的概念は、星の相対位置により空の一部が認識されるのと同じように、詳細の相対位置を測定することである。例えば環、円弧、渦巻を分析するためいくつかのタイプの個別指紋特徴がある（図3参照）。

50

【0075】

現在の自動検索システムは通常、データアルゴリズムを用いて行われ、走査された指紋から符号化された最新テンプレートを分類して、これを記憶されたテンプレート集合と比較する。

【0076】

無線周波数（RF）、超音波、シリコンスキャナなど他の技術も存在するが、指紋スキャナはたいてい光学式または容量性である。

【0077】

光学式スキャナは基本的に小型デジタルカメラであり、通常は指紋の反転像を撮影して、写真では凸部を暗くする。イメージと比較する前に、スキャナプロセッサは一連の検査を実施して、像が十分に良好であるかどうかを判断する。写真が暗すぎる、または明るすぎる場合には、スキャナが自動的に露出時間を変化させて新しいイメージを撮影する前に入射光線の量を増減する。

10

【0078】

容量性スキャナは、各々が凸部の幅より小さく反転増幅器に接続された小型プレートのアレイを使用する。スキャナに指が置かれると、指とプレートとが簡単なコンデンサを形成する。基準電荷がプレートに送られて、コンデンサを充電させる。プレートと指の間の距離に応じて、（凸部または凹部である場合には）、対応の増幅器が異なる電圧を提供する。これらの電圧が指紋の「イメージ」を形成する。こうして、容量性スキャナを欺くために、模様の白黒イメージが写ったただの紙を使用することが困難になる。さらに容量性スキャナは、光学式のものより小型にすることができる（図4参照）。

20

【0079】

最近開発された指紋走査技術は、低エネルギー無線信号を用いてプリントを走査するRF走査である。RFは、実際の指先表面の下にある模様を走査するために汚れ、傷、欠陥に左右されないという長所を持つ（図5参照）。

【0080】

スキャナについて論じる時に行う別の区別は、スイープスキャナとエリアスキャナとの間のものである。スイープスキャナでは指がセンサの前をドラッグされるのに対して、エリアスキャナでは指がセンサに置かれて走査が完了するまでそこに保持される。現在のスキャナの大部分はエリアセンサであるが、このモデルはいくつかの欠点を有する。センサが汚れやすい。これは走査性能に影響するばかりでなく、汚れたセンサに指を載せることに嫌悪感を持つ人もいる。潜像にまつわる問題も存在する。これは、すでに走査された模様がセンサ表面に残っていて、二番目の指紋の走査中に再起動されることを意味する。

30

【0081】

対象者が指をセンサに斜めに置くこともある。大部分のスキャナは20～30度より広い回転角には対応しない。

【0082】

センサ（特に容量性センサ）はエリア単位でコストがかかる。スイープセンサのセンサエリアはこれより小さくすることができ、そのため安価である。

【0083】

スイープスキャナも完全な解決法ではない。主な課題は正しいスイープ技術を習得するのにいくらか時間を要することと、薄片を指紋に再構成しなければならず時間がかかることである。ゆえに、特定の状況に合ったスキャナを選択する際には検討すべきパラメータが多くある。そのため、どのセンサ技術を用いるかは重要な課題である。

40

【0084】

光学式スキャナは模様の写真によって、容量性スキャナはモールドによってだまされる可能性がある。モールドはゼラチン、シリコン、Play-Doh（小麦粉ベースの粘度）で製作される。モールドを作製するためには実際の指が必要である。しかし光学式スキャナを欺く写真を得るためには、コップなどその人が触れたものがあれば人の指紋のイメージを作り出すのに充分である。ゆえに光学式スキャナを欺くのは容易である。閃光、熱

50

、蒸気、様々な粉末など、システムを欺く方法は他にも多数ある。しかし、システムを欺くためのこれらの方法は、スキャナがいわゆる生体検出を装備していれば役に立たない。

【0085】

生体検出は、体温、脈拍、血流、脈拍酸素濃度測定、電気抵抗、EGG、相対的誘電透過性、毛穴または皮膚変形、あるいはこれらの組合せを分析することにより、いくつかの方法で実行できる。生体検出方法は、多かれ少なかれなじみやすいものである。主な問題は、走査された模様が指の一部、薄いイメージ、指先に装着されたモールドであるかどうかをスキャナが判断することである。発汗を使用する新たな方法が解決法になるかもしれないが、いまだ開発過程にあり、そのため現実にはそれほど良好に機能するか知るのとは不可能である。

10

【0086】

10本の指はすべて独自の模様を持ち、こうして認証のためにどの指を使うことも可能である。一卵性双生児は似た指紋を持つかもしれないが、双生児でもそれぞれ独自の指紋を持つので同一ではない。人は毎日、25の完全な指紋を残すと言われており、指紋に関わる主な問題の一つは、複製が実に容易だということである。

【0087】

たいていの人は、指紋は指の先端にあると思っているので、最初、スキャナ上の間違っただけに指を置くが、実際に指がおかれなければならない時には、若干下にすると認証用の処理が可能なイメージが得られる。一部のスキャナは、例えば案内突起またはくぼみを用いて指の正しい位置決めを容易にするように設計されている。

20

【0088】

すべての人がこの方法を使用できるわけではないことに注意すべきである。事実、5%もが指紋スキャナで読み取ることはできない指紋を持っている。傷、たこ、他の欠陥が結果に影響し、スキャナ解像度が充分ではない薄い、または損傷した凹凸部を持つ人もいる。さらに、大部分の人はこの方法を非侵害的であると見なすが、犯罪捜査を連想させるため指紋走査に対して嫌悪感を抱く者もいる。

【0089】

あらゆる指は独自の指紋を持っていると言われるが、主なパターンのうち二つが観察者すべての98%で検出され、間違いのリスクを高める事実である。現在、伝統的な視覚的検査の代わりに自動化が行われている。指紋が採取されている中から人を識別しようとする、間違いが起こる。しかし、範囲の決められたデータベースで人のIDを認証する時には、非常に信頼できる方法である。

30

虹彩走査

【0090】

この方法の原理は、1936年に考えられたが、それでも1990年代まで適用されなかった。現存する実用的な虹彩バイオメトリクスは、1994年にJohn Daugman教授により作成されたアルゴリズムをその始まりとする。

【0091】

虹彩スキャナは、標準的なデジタルカメラを用いて眼の写真を撮る。イメージは通常、半径が120ピクセルであり、その結果、通常は一つの虹彩に8ビットのイメージとなる。写真が撮られる際に、テンプレート作成プロセスの最初の段階は、瞳孔と虹彩を位置決めすることである。その後、瞳孔がイメージから切り離された際に生じる輪が、極変換を使用して円板に変換される。次に分析プログラムがいくつかのアルゴリズムを使用し、異なる特徴に基づいてテンプレートを作成する(図6参照)。

40

【0092】

生体検出は、眼に可視光線を通して瞳孔のサイズが変化するかどうかを検出することによって実施される。かなり強力な光源、または人がスキャナに非常に接近しているかのいずれかを必要とする。そのため、トラックには適しておらず、従って本出願の対象外であるので、この生体検出についてはこれ以上説明しない。

【0093】

50

虹彩には266以上の独立した特徴がある。虹彩は、あらゆる人にだけでなくあらゆる眼についても独自である。通常は、266の特徴のうち約170が比較のテンプレートを形成するのに使用される。他のバイオメトリクス認証方法では、約15からせいぜい35の独立した重要な特徴を分析に使用するに過ぎない。ゆえに、虹彩テンプレートにはそれほど多くの特徴が見られるので、この方法は認証には非常に信頼性がある。我々の顔つきや我々の声のような身体的特徴は時とともに変化するが、虹彩は若年期の色彩変動を除くと、寿命全体を通して不変である。時間のかかるデータベースの更新が必要ないので、これは大きな長所である（図7参照）。

【0094】

方法の信頼性を証明するのは、追放された外国人の国内への再入国を防止するためのアラブ首長国連邦の虹彩認識システムである。毎日約600人の人々が走査を受け、現在データベースは355,000の虹彩で構成される。今までに1600万を超える検索が行われ、たった1件の整合ミスも検出されていない。プログラムの統計的分析は、整合ミスの可能性は800億分の1未満であるとしている。

【0095】

登録率は非常に良好である。視覚障害を持つ人の虹彩を除いてすべての虹彩が分析可能である。ほかに、3フィートまでの距離から虹彩のイメージを自動的に捕捉する用途が見られ、プロセスを非侵害的なものとしている。

【0096】

しかし、システムの中には眼の色の非常に濃い人々を走査するという問題を持つものがある。さらに、カラーまたは遠近両用のレンズには問題があり、度の強いメガネも同様である。

【0097】

虹彩走査の欠点の一つは、Iridian Technologies Inc.からのライセンスに基づいてすべての機器が製造されることである。このライセンスは機器そして方法全体を高価にする。加えて、車両でこの方法が実行される場合には、様々な証明条件がおそらく問題を引き起こすだろう。運転席が暗すぎる場合には、正しい走査は不可能であり、直射日光がカメラに入射する場合にも同じである。カメラがバックミラーに取り付けられて直射日光から保護されると、日光の問題は解決する。ドライバはミラーを定期的に覗き込むはずなので、これは運転中にスキャナを使用する可能性を高める。しかし、トラックは運転席にバックミラーを備えていないので、この解決法は乗用車により適している。そのためこの解決法は、本出願の範囲内では適用不可能である。

音声認識

【0098】

この方法は、声の違いに基づいて人を識別する。対象者がマイクロフォンに既定のフレーズを話す。システムは音声サンプルを捕捉して、例えばピッチ、抑揚および／またはトーンに基づいてテンプレートを作成する。認証についても同じ手順である。対象者はマイクロフォンに既定のフレーズを話し、システムがテンプレートを抽出して、データベースに記憶されたテンプレートと比較する。音声認識を使用する長所の一つは、ハイエンド記録再生機器がなくても詐称が困難なことである。これは、例えばディクタフォンによる記録が不可能な周波数を捕捉するマイクロフォンを音声認証システムが使用するからである。システムを欺くのに十分な形でパスワードが記録されたとしても、発話されたフレーズが変更されると無認可コピーを利用不能にする。さらに、すべての周波数を正しく複製するには、高性能再生システムが必要とされる。ハイエンド機器の需要は、生体検出の一種と見ることができる。

【0099】

音声認識の短所は、音声テンプレートは他の種類のバイオメトリクス情報よりも多くの記憶場所を要することである。結果的に、多量のデータが分析されるため、音声認証は他の方法よりも長い時間を必要とする。認証のために待たなければならないので、これは利用者には厄介である。別の問題は、健康、精神状態、疲労、加齢が人の音声特徴に影響す

る要因だということである。ゆえに、音声認証を唯一の認可方法として信頼すべきでない。

顔認識

【0100】

最近、再び注目を集めている方法は、顔認識である。パリ警察のAlphonse Bertillonは、1883年に最初の視覚的識別モデルを作成した。彼のシステムは人体測定学と呼ばれ、頭のサイズ、指の長さ、顔の長さ、眼の色、傷、髪の色のような特徴についてのいくつかの複雑な解剖学的測定を基礎とする。この方法は信頼性がなく、すぐに指紋に置き換えられた。英国では最近、犯人を識別するため監視カメラによる検査が実行されている。これらの検査から、カメラが鮮明な写真を撮っていない場合、または人が例えば付けひげやメガネで自分の属性を変えている場合には特に、この用法で人を識別するのは非常に困難であることが分かった。信頼できる識別結果が欠如しているが、この方法は認証目的では十分に機能する。

10

【0101】

その原理は単純で、上述した認証方法に使用される分析に類似している。対象者の顔のイメージが撮影され、コンピュータで分析されて、眼窩または口元の輪郭線などの主要特徴を発見する。分析の結果はテンプレートに記憶される。人を認証しようとする際には、イメージが撮影され、新しいイメージに基づいてテンプレートが作成される。新テンプレートは、データベースに記憶されたものと整合される。現在の標準的なパソコンは、データベース内の数千のテンプレートと一つのテンプレートとを1秒未満で比較できる。

20

【0102】

ガボールフィルタリングまたは固有顔など、イメージから重要特徴を抽出する技術は様々である。これらの技術はかなり複雑であり、それについて詳細に説明することは本出願の目的には本質的なものではないので、関心のある読者は、詳しい情報については当該技術で周知の参考文献を参考にすること。

【0103】

顔認識の長所の一つは、人間が互いを識別する時にするのと同じように人の顔を調べるので、人々がこの方法を快適だと考える傾向があることである。より正確な結果を達成するため、例えば唇動と音声認識とともに顔認識を使用できる。加齢、照明条件、顔の表情に対するエラー強さを得るため顔認証アルゴリズムを向上させようとする研究が行われている。

30

【0104】

しかし、現在、完全な解決法はなく、データベースは継続的な更新を必要とする。

【0105】

顔認識を検討する際に行う重要な決定の一つは、どのタイプのカメラを使用するかということである。普通のデジタルカメラか、赤外線カメラか。カメラが赤外線を使用する際には、この方法は顔面サーモグラフィと呼ばれる（次節参照）。

顔面サーモグラフィ

【0106】

顔面サーモグラフィは特殊な顔認識である。赤外線カメラの使用により、人の顔面血管パターンに基づく熱パターンが見られる。このパターンはそれぞれの人に独自であり、偽造が難しい（図8参照）。

40

【0107】

赤外線カメラは普通のカメラとほぼ同じように機能し、違いは、およそ760nm～0.5mmの間隔の電磁放射である赤外線に反応するということである。こうして、赤外線は人間の眼には見えない。可視光線も電磁放射の一形態であるが、赤外線とは波長が異なることに注意すべきである。赤外線は時に熱放射と呼ばれ、絶対ゼロ度を超える温度を持つすべての物体により発せられる。ゆえに、カメラが物体の温度イメージを撮影する。顔の形状、血流の変化のため顔の異なる部分は異なる温度を持ち、これを認証に使用できる。

50

【0108】

顔面サーモグラフィでは人の顔面熱パターンを分析するとしても、対象者が休憩しているか、運動しているか、低温の中にいる場合には大きな違いが見られない。I Rカメラはこれらの状況にかなり無反応であることが研究で分かっている。別の長所は、カメラは赤外線波長間隔で作動して可視光線には「反応しない」ので、走査は可視光線の条件に関係ないことである。

【0109】

顔認証のため普通のカメラとI Rカメラを使用する場合の比較が行われ、照明条件に左右されないでI Rカメラの方がほとんどいつも有利であった。しかし、I Rカメラについての問題の一つは、あらゆるタイプのメガネがこれに対して完全に不伝導性であるとい

10

うことである。これは、人がメガネを掛けている場合、または通常はメガネを掛けていてデータベースを更新せずに外した場合に、眼の周辺範囲が問題となることを意味する。

網膜走査

【0110】

網膜認識は1930年代に考案されたが、この方法を商業的に有効とするのに十分なほどこの技術が発展したのは1980年代になってからであった。網膜走査は、レーザを使用して網膜の血管パターンを分析する高速で非常に正確な方法である。網膜の写真が撮られると、上述した方法と同様に、イメージから抽出された特徴に基づいて通常はシステムがテンプレートを記憶する(図9参照)。

【0111】

20

血管パターンはあらゆる人に独自であり時間とともに変化しないので、網膜走査は最も正確なバイオメトリクス認証方法と考えられている。対象者が生存なくなると網膜の脈管構造は数秒以内に消滅するので、捕捉されたイメージが生きた人間から得られたものであることを保証する。網膜は走査が容易ではないが、網膜の撮像に必要な時間は指紋の撮像に必要な時間より短いことが研究から明らかである(図10参照)。

【0112】

カメラは高い解像度を持たなければならず、この方法は走査を可能にするため眼の正確な整合を必要とする。3フィートまでの距離からイメージ捕捉を行うことができる。しかし、どのような環境条件でこれらの性質が有効であるかは不確かである。

唇動認識

30

【0113】

発話中に人が唇を動かすやり方は人によって異なり、そのため唇動認識方法が開発された。人が話す時にカメラが使用されて口と周辺範囲の写真を何枚か(短時間で連続して)撮影する。コンピュータが使用されて、唇の周辺の範囲の細かい皺の動きを分析する。これらの動きは、写真に重ねられるベクトル場として表される。次に、上述した方法と同様に、ベクトル場がデータベースのベクトル場と比較される。使用される機器は、顔認識と基本的に同じである。

【0114】

唇動認識は、単一の認証方法として機能するのに十分なほど正確でない。そのため例えば音声認識とともに使用することが推奨される。

40

【0115】

唇認識の特殊なケースは笑顔認識と呼ばれる。笑っている間に行われる顔の下部の筋肉動作は人により異なる。これらの筋肉は意志による制御はほぼ不可能であり、対象者が笑わないようにしようとするなど顔の表情を維持しようとしても、見て取ることができる。市場には機能的なシステムはないので、これ以上は説明しない。

掌形認識

【0116】

掌形スキャナは、指の長さ、幅、厚み、湾曲を測定する。このシステムは、いくつかのペグを備える平坦面と光源とミラーとカメラとで構成される。掌を下向きにして手が平坦面に置かれ、指がペグにより案内される。手の側面をカメラに投影するためにミラーが使

50

用され、検索された写真が分析される（図 11 参照）。

【0117】

例えば指紋とは異なり、人の手は独自ではない。そのためこの方法は識別目的には使用できず、認証のみである。L i c h t e r m a n n e t a l . によれば、掌形認識は不恰好な機器のため自動車の目的には適していない。論文は2000年に書かれたので、5年間の開発によって機器のサイズが縮小したと信じるのは当然である。しかし、イメージを検索するため、掌形システムはカメラと手との間に約9インチを必要とする。これは、トラック搭載に機器を適するようにするには大きすぎる。

ソフトバイオメトリクス特質

【0118】

ソフトバイオメトリクス特質は、例えば年齢、性別、身長、体重、民族性、髪や眼の色である。これらのバイオメトリクスはあいまいであり、そのうちいくつかは生涯のうちで変化し、例えば指紋よりも偽造が容易でもある。そのため、ソフトバイオメトリクスは識別または確実な認証には使用できない。それでも、ソフトバイオメトリクスは他のバイオメトリクス方法を補足するものとして使用できる。体重管理は、指紋走査の補足として車両で実施される。

他の認証方法

【0119】

人々は、長い間、バイオメトリクス特徴を用いて他の人間を識別することができたが、現在、IDを確認する最も一般的な方法は、カード、応答器、パスワード、PIN（個人識別番号）によるものである。大部分の人はこれらの認証方法に慣れているが、異なる認証方法の比較を助けるため、各方法について簡単な説明をする。

パスワードとPIN

【0120】

パスワードとPINはそれほど紹介を必要としない。おそらく、本出願を読んでいる人はすべて、例えばコンピュータにアクセスする際、ATM（非同期転送モード）から現金を引き出す際、携帯電話を始動する際に、両方の方法を使ったことがあるだろう。

【0121】

主な長所は、システムがかなり単純だということである。必要なのはキーパッドとコンピュータだけである。他の長所は、使用が簡単であり、人々が慣れていて侵害的であると見なさないことである。

【0122】

欠点は、コードとパスワードが容易に複製、盗難、または忘れられることである。また、人は、犬の名前や子どもの年齢など、比較的推測が簡単なパスワードを持つ傾向がある。これは、詐称者が正しいパスワードを見つけ出して認証をパスすることを容易にする。

カード

【0123】

識別／認証目的のカードにはいくつかのタイプがある。その違いは、認証プロセスでカードがどのように使用されるかである。

【0124】

運転免許証および他のIDカードは、写真と実際の人との間の整合を誰かが視覚的に行うことを必要とする。

【0125】

アクセスカードは情報を記憶するための磁気ストリップを持ち、あるタイプでは、カードを所有している人が正当な所有者であることを認証するためPINを使用する。磁気ストリップは、ATM、アクセス端子、現金レジスタにより読み取られる。

【0126】

スマートカードは基本的に、クレジットカードのサイズのシンプルコンピュータである。カードに埋め込まれたマイクロプロセッサとメモリとを有する。これらのカードは、磁気ストリップよりも多くの情報がスマートカードのメモリに記憶されるので、標準的なク

10

20

30

40

50

レジットカードよりも多用途である。カード所有者が正当な所有者であることを認証するにはPINを使用するのが普通である。しかし、スマートカードのマイクロプロセッサは、Precise Biometricsにより開発されたMach-On-CardTM技術など、より複雑な方法を実行する可能性を広げる。この技術は、通常の手順である外部コンピュータによるのではなく、スマートカードのコンピュータにより実際の整合が行われることを意味する。

無線周波数識別 (RFID)

【0127】

RFIDは、RFIDタグと呼ばれるデバイスを使用してデータを遠隔操作で記憶および検索する方法である。これらのタグは能動または受動である。その違いは、受動タグは電源を持たないことである。代わりに、リーダデバイスから磁気誘導により電力を受け取る。これは、受動タグは実際の読取中にリーダに近接して保持されなければならないのに対して、能動タグは数メートルから読み取り可能であることを意味する。受動タグは、電源の欠如のため、能動タグよりも小型である。最小の受動タグは約0.4平方ミリメートルでシールほど薄いものに対して、最小の能動タグはだいたいコインのサイズである。

10

【0128】

RFIDタグは、カードと同じように認証目的で使用される。主な違いは、認証を行うために、タグをスキャナに向けるだけでよい（受動タグ）か、スキャナに充分近づけなければならない（能動タグ）かということである。

マルチモード認証システム

20

【0129】

マルチモードバイオメトリクス認証システムは、同時に機能する二つ以上のバイオメトリクス認証方法で構成される。一つの方法のみを使用するシステムは単モードと呼ばれる。同時にいくつかの方法を使用するので、マルチモードシステムは当然高価であるが、下記のように、二つ以上の認証方法を使用するという長所が見られる。

【0130】

マルチモードシステムがどのように機能するかをより分かりやすく説明するため、発明された例を以下に挙げる。マルチモードシステムを理解する方法の一つは、上述したバイオメトリクス認証方法のうち二つ、例えば指紋と虹彩走査で構成されるシステムを想像することである。三つの構成から選択することによって可能性が与えられる。

30

【0131】

対象者は、環境または他の要因により、その時に最も適した方法の一つを選ぶ。例えば、ドライバの手が汚れている場合には虹彩を走査し、運転席が暗い場合には指紋を走査する。

【0132】

対象者は両方の方法を相互に独立して使用し、システムが両方の結果を比較考量して決定を行う。この形態は、他人受入率 (FAR) を上げることなく本人拒否率 (FRR) を下げられることが経験的に判明している。認証方法の一つの整合が不十分である場合には、他の方法で有効な整合が得られ、対象者は認証をパスする。

【0133】

40

このシステムは、相互に独立した両方の方法に対象者がパスすることを必要とする。一つよりも二つの方法を欺くのは難しいので、これはセキュリティレベルを高める。欠点は、これらのシステムがかなり高い本人拒否率を持つ傾向にあることである。

【0134】

マルチモードシステムを使用する際には、セキュリティと利便性のいずれかが改良され、両方が同時に改良されることはない。マルチモードシステムの欠点は、認証がいくつかの作業で構成され、ゆえに長時間を要し、これが利用者にとって不便だということである。

マルチバイオメトリクスシステム

【0135】

50

前節で記載したマルチモードシステムは、いわゆるマルチシステムの特殊なケースである。いくつかの測定を使用するが、必ずしも異なる方法でなくてもよい。

【0136】

マルチ認証システムには基本的に五つのタイプがある。

マルチ整合器：マルチ整合システムは、二つ以上の異なる方法または二つの異なるアルゴリズム、例えば（指紋走査を用いた）詳細および非詳細に基づく整合で走査を分析する。

マルチセンサ：同じ物体の走査に二つ以上の異なるセンサが使用される際には、システムはマルチセンサシステムと呼ばれる。

マルチモード：マルチモードシステムは、二つ以上の異なる方法、例えば音声と顔の認識を用いる。

マルチユニット：マルチユニットシステムは、同じ性質の二つ以上のユニット、例えば人差し指と中指、左右両目を走査する。

マルチインプレッション：マルチインプレッションシステムは、同じ性質を多数回、走査し、例えば、音声認証システムのために対象者にそのパスワードを3回発話させることを必要とする。

【0137】

これらのシステムはすべて、明白な長所と短所を持っている。三つの方法を実施することが前もって決定されているので、マルチモードシステムに焦点を当てることとし、そのため他のマルチ方法についてはこれ以上説明しない。

準備作業

【0138】

ここでの二つの目的のため、いくつかの異なる作業方法が使用されており、ゆえに様々な種類の結果が得られている。本節では、作業プロセスのイメージを読者に与えるため、方法と結果と一緒に盛り込む。各段階の後にそれぞれ結果を記す。これは、プロセス中の様々な段階でどのような決定が行われたかと、これらの決定に基づいてどのように作業が進行したかを明らかにすると思われる。

アンケートの研究

【0139】

実行する方法の選択についてドライバの意見を重視するため、ドライバアンケートが早い段階で行われた。

2種類のアンケート

【0140】

アンケートは、それぞれ印象アンケートと方法アンケートと呼ばれる二つの文書に分割される。前者は、例えば作業ルーチン、バイオメトリクス方法についての知識、セキュリティについての感じ方、作業中の安全性を質問するものであった。後者は、2節で記載した各バイオメトリクス方法について短い説明をするものであった。回答者は、各方法について直感的なコメントをするように求められた。質問の中には回答に1から5のグレードを付けるように回答者に求めるものがあり、常に1は比較的否定的な回答、5は肯定的な回答であった。一方、比較的熟考する回答のみを求める質問もあった。すべての質問には、考察とコメントのためのスペースが設けられた。

【0141】

二つの異なる文書を作成した理由は、回答者が次の質問を覗き見して、異なる認証方法の説明に書かれた事柄に影響されるのを防止するためであった。アンケートは二部に分かれていたので、ドライバは次のものを受け取る前に第一部に回答するように強制された。

【0142】

アンケートは二つの方法で配布された。見解を示した最初の人達は、ガザンバーク郊外のトラック駐車場で休憩のために駐車したトラックドライバであった。多数のドライバがアンケートに答えるように依頼されたが、それに同意したのは12人のみであった。お礼として、回答者は菓子を受け取った。

【0143】

二番目に、イエーテボリの運送会社が、ドライバにアンケートを配布することに同意した。最初の経験から、配布されたアンケートと同数の回答は得られないことが分かっており、そのため、1週間の期限内に少なくとも半数を回収できると見込んで、運送会社に25部のアンケートを渡した。回答して期限内に返却されたアンケートは10部であった。

【0144】

アンケートにはスウェーデン語版と英語版があったため、スウェーデン語を知っているかどうかに関係なくすべてのドライバが質問に答えることができたはずである。ドライバの多くが、下手なスウェーデン語しか話さないか、全く話せないの、地方のトラック停車場ではこれは重要なことであった。運送会社で配布されたすべてのアンケートはスウェーデン語で書かれていた。

10

印象アンケートの結果

【0145】

回答者のうち11人が流通の仕事に就いており、10人が長距離を運転し、1人が長距離と配達の両方で運転していた。12人のドライバは自分専用のトラックを運転し、他は平均5人の他のドライバとトラックを共有していた。1年から38年間まで平均して15年間、仕事をしていた。

【0146】

8人のドライバがバイオメトリクス方法を周知であり、例えば全員が指紋認証を知っていた。これはいくつかの回答の一つに過ぎず、他の人は他のいくつかの方法にも言及していた。かつてバイオメトリクス認証方法を利用したことのあるのは1人のドライバに過ぎなかった。バイオメトリクスの経験を持たない9人のドライバは、これを認証に使うという考えに肯定的であり、4人はその概念全体に対してさらに限定的であるか反対しており、残る8人は肯定的でも否定的でもなかった。平均スコアは3.6であった。

20

【0147】

8人のドライバはバイオメトリクス認証システムの短所に気づいていたが、11人はそうではなかった。3人のドライバは質問に回答しなかった。他方、15人のドライバが長所を認め、5人は長所を認めず、2人は質問に回答しなかった。バイオメトリクスデータは保存されるべきかという質問には、15人のドライバが、車から降りる際に携行できるスマートカードに保存することを望むと回答した。5人は、運送会社に保存されるべきであると考え、2人は車内での保存を希望した。数人のドライバが二つ以上の選択肢を選び、3人は全く回答していないことにも注意すること。

30

方法アンケートの結果

【0148】

指紋認証は、圧倒的に最も高い評価を受けた。誰もが最も安価で使いやすいものであると考えた。車でバイオメトリクス認証方法を使用したくないと考える人でも、指紋は好ましいと考えた。それでも、4人のドライバは、手が汚れていると問題が起こることを懸念していた。2人の回答者は、指を失うか誘拐されて車を始動させられるというシナリオを想像したが、このような短所に気づいていても、それでも長所もあると認めた。また、他の方法について質問されると、(当該する方法でなく)指紋の使用が好ましいと答えるドライバが時々いた。

40

【0149】

他の方法に関して、肯定的と否定的な回答が混ざっていたことから、その方法が適しているかどうかについての結論を引き出すのは困難であった。6人のドライバがコメントしていたので、言及に値するのは、風邪をひくか喉の調子が悪くてもドライバが仕事するのは非常によくあることなので、音声認証には懐疑的であるということである。2人は音声認識技術で苦い経験を持っており、そのため音声認識の使用には懐疑的であった。

運送業者との電話インタビュー

【0150】

ここでのような認証システムは、ドライバばかりでなく様々な運送業者にとっても重要である。運送業者からの様々な要求についてアイディアを得るため、いくつかの電話イン

50

タビューが行われた。

電話インタビューはどのように行われたか

【0151】

イェテボリ内のランダムに選択された10社の事務所に、電話でインタビューを依頼した。そのうち3社がインタビューを受け、4社はEメールでアンケートを受け取り、これに回答して、同じように返信した。質問はドライバアンケートとほぼ同じであったが、ただ、口頭で質問が行われ、ドライバでなく会社に合うように若干調整が加えられた。質問は情報提供者に大きな声で読み上げられ、必要であれば説明がなされた。回答はインタビューアーにより筆記された。

【0152】

インタビューに適した人をつかまえるのは困難で、それに成功したとしても質問に答える時間のある人を見つけるのは難しかった。回答はかなり類似していたので、会社が何を重要と考えているかについてのヒントが得られた。情報提供者の数が少なかったので、回答は必ずしも正確な数で記されていないことに注意すること。

運送業者との電話インタビューの結果

【0153】

インタビューを受けた4社の事務所での労働条件は異なり、例えば長距離と配達が代表的であったが、危険物および高価な積荷もあった。会社規模はドライバ8人から76人までであった。会社のうち1社は、病気や予期せぬ欠勤の場合に外部の人間を使っていた。

【0154】

回答者は主として肯定的であり、会社は、アンケートを受けたドライバよりも様々な認証方法について詳しく知っているようであった。主な要求は高価であってはならないということであり、低コストで高いセキュリティを望んでいることを強調した。最大の懸念はドライバが眼や指を失う危険に合った場合には確実に役に立たないということである。最大の疑念は技術に対するものであった。「失敗の場合にはどうするのか？」が共通する質問であった。大部分は、車両の移動を不可能にするような事故その他のことがらがドライバに起こった場合のトラブルにも気づいていた。「なんとかして車を動かす方法がなければならない。」

【0155】

指紋による認証は、すべての会社がそれに肯定的であったので、最も評価の高い方法であった。2人は眼を分析する方法に強く反対した。3人目の人は、高価ではないので指紋認証がよいとコメントした。ドライバは病気であるか声がかれていても仕事に行くのが普通であるとの判断により、音声認識を用いた認証システムを信頼する人はいなかった。顔認識は指紋認証よりも高価であると考えられ、体重増加または髭がある場合とない場合に同じ人物に対応できないことを恐れていた。他の方法はいずれも楽天的な考えを得られなかった。例えば掌形は、指紋認証ほど信頼性がないと思われるので不必要であると考えられた。「指1本のみ」よりも手全体を失う危険を高めることにもなるだろう。

【0156】

情報提供者の何人かは、会社にこのようなセキュリティが必要であるとは感じていなかった。代わりに、アルコールインタロック装置の必要性を指摘した。それでも何かを選択しなければならなかったら、指紋認証を支持するだろう。1人の人は、他の者よりもアイディア全体に肯定的であり、1人はより否定的であった。顕著なのは、バイオメトリクス認証方法に対して最も否定的であった人は、いわゆるドライバスタイル識別のアイディアを好んだことである。現在の車両は多くの情報、例えば走行時間、燃費、ギヤチェンジ、制動技術を監視および記憶できる。この情報を監視することにより、ドライバの運転スタイルを観察することが可能である。これは人を認証するには充分でないだろうが、パターンが劇的に変化した場合には、誰か他の者が車両を奪ったと推定される。ドライバスタイル識別のアイディアを好む情報提供者は、眠気検出およびドライバがドラッグその他の薬物を服用したかどうかの検出と統合されるべきであると示唆している。

【0157】

会社は現時点では認証システムを必要とするとは感じていないが、車両の盗難が難しくなるならば肯定的に感じていた。

どうすれば方法が目的にかなうかについての考察

【0158】

現在、市場にはいくつかの異なる認証方法がある。それでも、本出願の目的にとって完璧な方法はない。理論研究により、トラック分野での同方法の妥当性についての考察および論考に達した。すべての方法には長所と短所があるが、それをすべて検査するのは可能でなかった。そのため、異なる方法を理論的に相互に比較考量して、検査プロトタイプでどれを実行するかを選択できるようにすることが重要であった。本節では、考察および理論的比較による結果を記す。

10

理想的方法

【0159】

どの方法を実施するかを選択の背景とするため、認証システムに最も望ましい性質を挙げた。これらの基準は、理想的なシステムはどのように機能すべきかに関する考察と創造的集団思考の際に登場するので、選択された。

使いやすさ：機器の操作に広範囲の教育が必要であるべきではない。できる限り直観的であるべきであり、できる限り自動化されるべきである。

速度：認証プロセスは長い時間かかってはならず、せいぜい数秒でなければならない。登録は短時間であるべきである。さらに、方法は多様な作業で構成されるべきではない。

20

柔軟性：システムは、シフトを変える可能性のある様々なドライバに対応するように構築されるべきである。認証されたドライバがエンジンを始動するとすぐに詐称者により車両から放り出されることを回避するため、運転中にドライバを認証することが可能であるべきである。

コスト：システムは高価過ぎてはならず、さもないとトラック所有者は購入を考えないだろう。

ユーザ受容性：システムは非侵害的であるべきである。それ以外にも、ユーザとトラック所有者は、システムは有意義であり自分達にとって有益であると感じなければならない。

セキュリティ：システムは攻撃に対して安全でなければならない。

精度：システムは十分に低いTER（総合誤差率）を達成するべきである。

妥当性：システムの方法は、スペース、照明、温度、騒音、振動、湿度など車両の様々な環境特性に適合しなければならない。

30

統合性：車両への統合が容易な機器は、コストを低く抑え、習得すべき新たな作業が多すぎることがないのでシステムの使用を容易にする。必要とされる機器は不恰好であってはならず、さもないと車両への搭載は困難だろう。

信頼性：システムは決して破壊されるか認証に失敗してはならず、さもないと無認可の人間が車両を始動させることを防止することはできないだろう。そうであると、ドライバまたは所有者はシステムを信頼しなくなる。同じ意味で、正規ドライバへのアクセスを許可し損なうことがあってはならない。

様々な方法についての見解

【0160】

40

本節は、様々な認証方法に支持または反対する注釈を含む。以下の課題と考察は、上述した理想的システムの基準に結び付けられる。これらの見解は、本出願の様々な面に影響を与えている。

指紋認証に関する見解

【0161】

指紋技術は、長年にわたって使用され開発されてきたという意味で、よく検証されている。スキャナは小型で安価とすることができ、この方法は大部分の人に非侵害的なものとして経験されている。市場では多様な銘柄が入手可能であり、所望の要件に合う製品を見つける機会が充分にあることを保証する。

【0162】

50

認証システムのセキュリティを高める方法の一つは、認証に2本以上の指を使用することであろう。これを行うには二つの異なる方法がある。システムが既定の組の指の走査を要求するか、システムが特定の時にどの指が走査されるかをランダムに要求する。これらの選択肢の欠点の一つは、当然、1組の様子が要求される場合には、詐称者は人の模様のすべてを盗もうとするだろうということである。その場合には、セキュリティの向上はユーザの安全性を犠牲にするものである

【0163】

自動車の観点について検討に値するのは、多くのドライバが手で多くの作業を行って手を汚すか摩損させ、これが走査結果に影響を与えることである。スキャナ自体が汚れた場合には、正しい走査は困難となる。スイープスキャナはタッチスキャナほど汚れやすくないので、これを用いるとこの問題は解決される。

10

【0164】

無認可の人がシステムを欺こうとする可能性が常にある。生体検出はコピー、または詐称者が指（または手）全体を盗むという恐ろしいシナリオを防止するが、完全に安全なシステムを作ることは不可能である。認可ドライバに自分の指をスキャナに載置させるため、ドラッグまたは脅しが用いられる可能性もある。要約すると、指紋走査は、車両への統合が容易である、高速、安価、非侵害的な方法である。

虹彩走査に関する見解

【0165】

虹彩走査は、正確で信頼できる安全な認証方法であると考えられている。文献によれば、およそ1メートルの距離からイメージを撮影でき、それでもイメージをテンプレートに整合させるのに十分に高い品質を得ることのできる機器が、現在、入手可能である。これは、カメラがドライバの邪魔になり視界を遮ることのないように、車内にカメラを設置することが可能であることを意味する。しかし、これらの用途が車両に適しているかどうかは不確かであり、この分野では試験が行われていないので運転中の走査が可能であるかどうかはさらに不確かである。

20

【0166】

ゆえに、虹彩走査は高速であって侵害的でないが、この方法には妥当性とともな統合性が欠如しており、ライセンスゆえに機器は高価である。

音声認識に関する見解

30

【0167】

音声認証システムは、おそらくは携帯電話ハンズフリースystemなど既存の機器を使用して、車両に容易に統合される。少なくとも、大部分の人は発話と運転を同時にすることができるという意味において、運転中に音声認証を用いることは可能なはずである。ドライバが携帯電話または他の言語通信システムを利用する場合、認証要求は数分間抑制される。ドライバがステレオを聞いている場合には、認証の間は無音とすることが推奨される。

【0168】

最新型トラックの運転席は防音されており、中に乗り込むと顕著である。防音のため、エンジン、風、周囲の往来からの背景ノイズはかなり一定である。そのため、認証中に適応フィルタを用いて音声サンプルからノイズを除去することが可能なはずである。しかし、たとえば大部分トラック運転席が十分に絶縁されていても、音声認証システムは室内のオフィスでの使用のために開発されており、ゆえに、車両環境でシステムを検査することなく適しているかどうかを判断するのは困難である。

40

【0169】

マイナス面は、人の声とアクセントは時間とともに変化するのでデータベースが常に更新を必要とすることである。さらに、健康関連および感情的な要因により人の声はすぐに変化する。このような面のためこの技術を信用しない人もいる。

【0170】

本出願の中心は、ドライバのIDを認証することであり、既定の認証フレーズの利用が

50

推奨される。各ドライバが独自のパスワードを持っていれば、フレーズそのものと音声サンプルの両方を認証に使用できる。ゆえに、音声認証は安価な方法であり、トラックでの実行が容易である。しかし、騒音の多い環境と声が時間とともに変化するという事実のため、実際の状況でどれほどうまく機能するかは不確かである。

顔認識に関する見解

【0171】

顔認識は光線条件に左右されやすいが、認証中に運転席の照明を追加することは可能なので、車両の始動前に使用する選択肢とすることができる。しかし、ドライバの邪魔になるので、運転中にこれを行うことは勧められない。照明条件は一日の間で変化し、そのため運転中に顔認識を使用できるかどうかは不確かである。夜間に撮影された写真は、認証に成功するのに十分なほど、システムに記憶されたイメージと相似していない。車両にカメラを設けると、眠気検出、運転席監視など他の多くの可能性が考えられるので、ここでは様々な光線条件が検査される。しかしこれらの可能性は本出願の目的を逸脱しているため、これ以上は調査しない。

10

【0172】

顔認識の中で時間のかかる部分はテンプレート作成である。認証中、少なくとも1枚が良好となるようにシステムは3枚以上の写真を撮る必要がある。テンプレート作成は約3～5秒を要し、これは認証プロセス全体が約10～15秒を要して長すぎることを意味する。

【0173】

興味深い付随的効果の一つは、使用されるカメラが実際に車両を運転しようとする人の写真を取るという事実である。詐称者が車両を運転する場合、認証は失敗するが、それでも写真が撮影され記憶される。これらの写真は、彼を特定しようとする際に使用される。

20

【0174】

要約すると、顔認識は、ユーザにとって使いやすく、安価で、非侵害的な方法である。だが、車両の運転席に似た環境での顔認証に関する研究を発見するのは可能でなかったため、この方法が目的にどれほど適しているかは不確かである。

顔面サーモグラフィに関する見解

【0175】

顔認識の使用に関する考えの一つは、運転中の自動認証に使用することが可能だということである。しかしこれは、光線状態の変化にシステムがあまり左右されない場合のみに可能である。上で説明したように、顔面サーモグラフィと顔認識は実際には同じである。違いは、使用されるのがどのタイプのカメラかということである。顔面サーモグラフィはIRカメラを使用し、これは、この方法が顔認識に比べて光線状態に左右されないことを意味する。

30

【0176】

検査は行われておらず、開発キットは入手可能ではないので、顔面サーモグラフィが理想的な方法に相当するかどうかの判断は難しい。

網膜走査に関する見解

【0177】

現在の網膜走査機器はサイズとコストが縮小し、ゆえに実際的問題のいくつかを解決している。大きな問題は、眼が走査されることに対して嫌悪感を持つ人がいるという事実である。また、走査中にドライバは特定方向を見なければならないので、この方法は特に運転中には車内での使用に適していない。認証に十分なほど長く一点に眼を集中させ続けるという問題を生じ、これが交通安全にマイナスの影響を与える。それゆえ、現在の技術では、これは本出願の目的に使用する方法ではない。

40

掌形認識に関する見解

【0178】

掌形認識についての主な利点は、この方法が汚れ、たこ、および（妥当な範囲内の）傷には全く左右されないことである。測定される手全体にはいくつかの特徴があるので、

50

指が汚れているかどうか、またはその人が事故で切断したかどうかは重要でない。機器は安価で認証に要するのは1秒未満であるが、不恰好な機器のためこの方法は自動車目的には不適當である。

マルチモードシステムに関する見解

【0179】

マルチモードシステムでは、異なる方法を組み合わせることにより異なるレベルのセキュリティが達成される。日常的な使用では、指紋認証で充分である。危険地域を運転するか危険物を運搬する際には、いくつかの方法（例えば指紋と虹彩走査）を用いて認証が行われることでセキュリティレベルを向上させる。

【0180】

マルチモードシステムの興味深い一面は、テンプレートデータベースの自動更新に利用できることである。3種類の認証方法、例えばPIN、指紋、顔認識をランダムに使用する認証システムを想定する。システムがドライバ認証を要求すると、三つの特徴のすべてを分析する。二つの方法が良好に完了した場合、データベースは第3のサンプルを用いて更新される。ゆえに、PINが正しく、指紋スキャナで良好な整合が見られる場合には、システムは顔の写真を撮影してテンプレートデータベースを更新する。システムがデータベース自体を継続的に更新するので、これは多量の時間を節約し、こうしてシステムのメンテナンスを軽減する。

プロトタイプ実装方法の選択

【0181】

異なる認証方法の理論的分析により、前節に挙げた見解と考察が得られた。見解とSWOT分析は、プロトタイプ実装のための認証方法の選択の主な根拠となる。

方法選択

【0182】

認証方法のみでは理想的システムの基準を満たすことはできない。どの方法を使用するか最終決定は、精度とコストばかりでなく使いやすさと欺きやすさとのバランスに基づいて行われた。理想的システムの他の基準は方法によって大きく異ならず、そのため選択の際には検討されなかった。各方法の長所と短所が、価格および納入時間とともに検討された。

選択された方法

【0183】

方法を選択しなかった理由を以下に挙げ、その後で実行される方法を選択した理由を挙げる。

顔面サーモグラフィ：IRカメラは普通のカメラよりも高価であるが、この方法は非常に正確で偽造が難しいので、詳しく検討すべき分野であることは確かである。残念なことに、認証目的の顔面サーモグラフィに関してはほとんど研究が行われておらず、著者らはこのタイプの認証のための機器を製造している会社を見つけることができなかった。

虹彩走査：虹彩走査の開発キットは、約25000ドルから35000ドルかかり、プロジェクト予算を超えている。

唇動：唇動認識には、十分に信頼できる別の認証方法が必要である。その妥当性を検査して相互に比較するには、三つの認証方法を実施するのが理想的であると考えられる。異なるセキュリティレベルを可能にするため、三つの方法すべてがそれだけで信頼できるものであるべきであって、ゆえに唇動認識は選択肢ではない。

網膜走査：網膜走査は、正確な眼の整合が必要とされるため自動車の目的には適していない。

掌形：掌形走査に必要な機器は、車へ装着するには不恰好である。

【0184】

残る三つのシステム、指紋認証と音声認識と顔認識はすべて車内搭載に適しており、妥当な価格と納入時間で開発キットを提供する製造者がいた。

【0185】

システムをできる限り統合するため、すべてのシステムが同じ根拠に基づいて互換性を持つことが望ましかった。これはサポート提供能力とともに、製造者を選択する二つの主な基準であった。

【0186】

P I Nは現在では一般的であり、この方法は携帯電話のキーパッドを用いて車両で容易に実行できる。そのため、P I N認証システムも実行された。これは、一般的認証方法とバイオメトリクス方法との比較も可能にした。

【0187】

アンケートの結果に示されていたように、回答者の多くはバイオメトリクステンプレートがカードに記憶されて、車から降りる時にこれを携行することを好んだ。テンプレート記憶装置を将来的なデジタル回転速度計と一体化させる可能性を例示するため、スマートカードリーダーもこのシステムに包含された。

10

【0188】

要約すると、プロトタイプシステムに選択された方法は、指紋、顔認識、音声認識に加えてP I Nおよびカードの認証である。

使用例

【0189】

トラックが使用される多様な作業状況とエリアにより、認証システムには様々な難題が生じる。システムがどのように使用されるかについての考察は、いくつかの使用例の考案につながった。現実的な使用例を作り上げることで、実際のドライバ認証システムの必要性の実証とともに利点を指摘する。

20

使用例の考案

これらの使用例は、実装方法を選択するプロセスにおける議論および創造的集団思考に基づいている。

すべてのバイオメトリクス方法を用いたマルチモード認証

【0190】

これは、危険物または高価な物品を運搬する、または高リスク地域を運転中の車両を対象とする最高セキュリティレベルである。ドライバは、自分が正規の人間であることを確かめるため、あらゆる方法を使用して自分のI Dを認証する。以下は、この認証がどのように進められるかについてのいくつかの例である。

30

【0191】

ドライバは、一日の仕事を始めるため車庫に来ている。車両に乗り込むと、自分のスマートカード（回転速度計用カードと一体化）をリーダーに挿入し、P I Nコードをダイヤルし、それからスキャナに指を載せる。P I Nが正しく、カードと照合して指が認証されると、システムが音声サンプルを要求する。ドライバはマイクロフォンに向かってパスワードを言う。顔認証を実施するため、通常運転位置に座るようにドライバに指示するシステムメッセージが現れる。記録されたデータは分析され、スマートカードに記憶されたテンプレートデータと比較される。認証が成功した。指名と雇用識別番号が事務処理部門に送信されて符号化される。

【0192】

ドライバは認証手順を受けるが、方法の一つには失敗する。システムメッセージは、認証失敗をドライバに伝える。上の例のように手順が続行し、少なくとも一つの方法が成功する。氏名と雇用識別番号が、認証失敗の情報とともに、事務処理部門に送信されて符号化される。

40

【0193】

長距離運転で、ドライバは運転席で昼寝をする。目を覚ますと、運転を続ける前に外へ出て脚を伸ばす。助手席のドアが開いて、詐称者が乗り込み、運転席に座る。詐称者は車両を始動させようとするが認証に失敗するため、車両は作動停止となる。即座に事務処理部門に警告が送信され、システムはハンドルの前に座っている人物の写真を撮る。この写真も事務処理部門へ送られる。

50

二つのバイオメトリクス方法を使用するマルチモード認証

【0194】

この使用例の目的は、運転席に乗り込んだ人物が正規ドライバであることを確かめることである。このセキュリティレベルでは四つの異なる状況が考案されている。以下参照。二つのバイオメトリクス認証方法のみを装備する車両を設けることが可能であることに注意。しかし、すべての方法に必要な機器をすべて用意したうえで、それぞれの場合にどれを使用するかをランダムに変えることも可能である。

【0195】

ドライバは、一日の仕事を開始するため車庫に来ている。車両に乗り込むと、自分のスマートカード（回転速度計用カードと一体化）をリーダーに挿入し、PINコードをダイヤルし、それからスキャナに指を載せる。PINが正しく、カードと照合して指が認証される。システムが音声サンプルを要求するため、ドライバはマイクロフォンに向かってパスワードを言う。記録されたデータは分析され、スマートカードに記憶されたテンプレートデータと比較される。認証が成功した。氏名と雇用識別番号が事務処理部門に送信されて符号化される。

10

【0196】

上記と同じシナリオであるが、顔認証を実施するため、音声認証の代わりに、通常運転位置に座るようにドライバに指示するシステムメッセージが現れる。記録されたデータは分析されて、スマートカードに記憶されたテンプレートデータと比較される。認証は成功した。氏名と雇用識別番号が事務処理部門に送信されて符号化される。

20

【0197】

ドライバは一つ以上の方法に失敗するが、少なくとも一つの方法には成功する。ドライバの氏名と雇用識別番号が、認証失敗に関する情報とともに、事務処理部門に送信されて符号化される。どの認証にも成功しないと、車両が作動停止となり、即座に警告が事務処理部門へ送られる。

異なるセキュリティレベルでの単一バイオメトリクス認証

【0198】

この認証は、ドライバがいくつかの方法ですでに認証された後で短時間の停止の後に、または、セキュリティレベルにより一つのバイオメトリクス方法のみで充分である場合に行われると考えられる。セキュリティレベルについてはもちろん論考が可能であるが、このような例では高、中間、低セキュリティレベルと分類される。以下では高セキュリティの例を示す。

30

【0199】

ドライバは一日のうちの多くの停止場所の一つで積荷を降ろしている。エンジンがかかったまま車両は停止している。荷降ろしが終了した後、ドライバはトラックに乗り込む。短時間の停止であるため、一つのみの認証が必要であり、どの方法にするかはランダムに決められる。この時、システムは指紋認証を要求し、そのためドライバはスキャナに指を載せ、依然として、車両を運転している者であることを認証する。システムが認証するのでドライバが出発することができ、一方、氏名と雇用識別番号が確認のため事務処理部門へ送信されて符号化される。

40

【0200】

トラック駐車場でドライバが何か軽食を買いに車を停めた。エンジンをかけたままの短い停止であり、ゆえに利用できる方法のうち一つのみが出発前の認証に必要とされる。詐称者が運転席を奪うと、認証が開始する。有効な認証が行われないので、システムはカメラで写真を撮影し、これを警告とともに事務処理部門へ送信する。トラックは作動停止となる。

【0201】

認証システムはセキュリティを高めるためのものであるが、ドライバの通常の作業に影響してはならない。できる限り簡単にするには、高レベルよりも中間セキュリティレベルの方がドライバに高い自主性を与える。

50

【0202】

ドライバは積荷を降ろすための一日の多くの停止のうちの一回を行っている。車両はエンジンがかかったまま停止している。荷降ろしが終了すると、ドライバはトラックに戻る。座るとスキャナに指を載せてIDを認証する。システムは、今回、指紋を使用しても良いかどうか、またはドライバは他の方法の一つを使用しなければならないかをチェックする。この時、システムが別のタイプの認証を必要とするので、ドライバは自分のパスワードを言うことにより自己のIDを認証するように促される。認証が成功しドライバは出発し、一方、その氏名と雇用識別番号が確認のため事務処理部門へ送信されて符号化される。

【0203】

10

ドライバは積荷の一部を降ろすために停止している。エンジンはかかったままである。ドライバは車両に戻るとPINコードをダイヤルする。ストレスがたまっているためドライバが間違った番号をダイヤルして、何度も繰り返すが、それでもコードを正確に思い出せない。認証は失敗である。システムは認証が失敗したことをドライバに知らせ、代わりに指紋走査を使用してIDを認証するように要求する。認証は成功し、ドライバは出発する。ドライバの氏名と雇用識別番号はPIN認証失敗についての情報とともに、確認のため事務処理部門へ送信されて符号化される。

【0204】

低レベルのセキュリティは、認証に一つの方法のみを必要とする。これは、車両が単一の認証方法のための機器を有するだけで充分であることを意味する。また、トラックにいくつかの方法を設け、例えば積荷、経路、休憩の長さに応じて一つの方法のみが要求されるという可能性もある。車両の認証システムはセキュリティを高めると推定される。しかし、一つの方法のみでは、いくつかの認証方法よりも不正手段が成功するリスクが高くなるのは当然である。

20

【0205】

一日の多くの停止場所の一つでドライバは積荷を降ろしている。車両はエンジンがかかったまま停止している。荷降ろしを終了するとドライバはトラックへ戻る。座って指をスキャナに乗せてIDを認証する。システムがドライバを認証するのでドライバは出発し、その氏名と雇用識別番号は確認のため事務処理部門へ送信されて符号化される。

【0206】

30

ドライバは積荷を降ろすため停止している。ドライバがその日すでに自己識別を行っているので、車両が高レベルセキュリティを備えていても一つの認証方法で充分である。やはり自分のバイオメトリクスデータが記憶されたスマートカードを所有する別のドライバがドライバに取って代わって自己のIDを認証しようとする。カードが抜き取られて新しいものが挿入されたことにシステムは気づくため、単一の認証では充分ではない。ドライバはすべての方法で自己のIDを認証し、事務処理部門へ情報が送信されて符号化され、車両を運転しているのは正規ドライバでないことが即座に判明する。

【0207】

ドライバは、トラック駐車場で軽食を買うために停止している。エンジンをかけたままの短い停止であり、ゆえに利用できる唯一の方法は、出発前に認証を要求するというものである。詐称者が運転席を奪うと、認証が開始する。有効な認証は行われないので、車両は作動停止となる。システムはカメラで写真を撮り、警告とともにこれを事務処理部門へ送信する。

40

【0208】

ドライバは車両へ乗り込む。指をスキャナに載せるが認証に成功しない。これは利用可能な唯一の方法であったため、認証失敗についての警告が即座に事務処理部門へ送信される。車両は作動停止となる。

運転中の手動認証

【0209】

考えられるシナリオは、詐称者がドライバに自分のIDを認証させた後に車両から追い

50

出すというものである。これや似たようなリスクを回避するため、ドライバは運転中にも認証されるべきである。以下は、アイデアを説明するためのいくつかの例である。

【0210】

車両は走行中である。IDを認証するためパスワードを言うようにドライバに要求するシステムメッセージが現れる。ドライバはこれを行い、認証に成功する。その氏名と雇用識別番号が事務処理部門へ送信されて符号化される。

【0211】

ドライバは長距離業務の途中である。パスワードを言ってIDを認証するようにドライバに要求するシステムメッセージが現れる。ドライバはそうするが、この日は声がかれているので認証は失敗する。ドライバはさらに2回試みるが、やはり認証は失敗するため、システムは代わりにスキャナに指を載せるように彼に要求する。今度は認証が成功する。ドライバの氏名と雇用識別番号が、認証失敗についての情報とともに事務処理部門へ送信されて符号化される。

10

【0212】

車両は走行中である。スキャナに指を載せてIDを認証するようにドライバに要求するシステムメッセージが現れる。ドライバはいずれの方法でもIDを認証することができない。顔認識のためカメラで撮影された未認証ドライバの写真とともに、警告が即座に事務処理部門へ送信される。ドライバは車両の始動前に認証されているので、ドライバの氏名と雇用識別番号が、運転中のこの認証失敗についての情報とともに事務処理部門へ送信されて符号化される。

20

【0213】

いくつかの認証方法のための機器を備える車両が走行中である。スキャナに指を載せてIDを認証するようにドライバに要求するシステムメッセージが現れる。次の3分間で認証が行われないため、事務処理部門へ警告が送信される。

【0214】

車両は走行中である。スキャナに指を載せてIDを認証するようにドライバに要求するシステムメッセージが現れる。認証に失敗し、これはこの車両での唯一の認証方法であるので、即座に事務処理部門へ警告が送信される。

運転中の自動認証

【0215】

この認証はドライバからの介入なしに行われる。これは、いくつかの長所を含む。例えば、運転中にIDが認証されてもドライバは妨害されず、詐称者はシステムが自分を認証しようとしていることすら分らない。自動認証を可能にするため、車両は顔認識機器を備えなければならない。以下は、運転中の自動認証のいくつかの例である。

30

【0216】

車両は走行中である。システムはドライバの写真を撮り、回転速度計のスマートカードのテンプレートの特徴と比較する。認証は成功し、ドライバの氏名と雇用識別番号が事務処理部門へ送信されて符号化される。

【0217】

ドライバは、いくつかの可能な認証方法を備える車両で長距離業務に就いている。システムは、回転速度計のスマートカードのテンプレートと照合してドライバを認証しようとする。認証は失敗し、そのため、スキャナに指を載せるようにドライバに要求するシステムメッセージが現れる。今度は、認証は成功する。符号化されたドライバの氏名と雇用識別番号が、認証失敗についての情報とともに事務処理部門へ送信される。

40

【0218】

上記と同様の状況では、認証に失敗するため、ドライバはスキャナに指を載せるように要求される。どの認証方法も成功しないと、顔認証のためカメラで撮影された未認証ドライバの写真とともに直ちに事務処理部門へ警告が送信される。

【0219】

車両は走行中である。自動認証が失敗し、スキャナに指を載せてIDを認証するように

50

ドライバに要求するシステムメッセージが現れる。その後3分間以内に認証が行われず、そのため、顔認証に失敗したと追加方法による認証が行われなかったことについての情報とともに、警告が事務処理部門へ送られる。

プロトタイプシステムの設計と実装

【0220】

認証方法が選択され、機器が到着すると、システムを構築する番である。システムは反復的開発プロセスを使用して開発され、結果的に本節に提示される設計となった。実装された認証システムの概要を明らかにし、このようなシステムのための必要ソフトウェアを、実装についての記載とともに説明する。

ハードウェア

10

【0221】

ハードウェアの製造者は主として三つの基準つまりコストと納入時間と互換性とから選択された。本節の第一部ではハードウェアについて記し、第二部では実装の結果について記載する。

システムのハードウェア

【0222】

このプロジェクトに使用された機器を挙げ、以下に説明する。

【0223】

使用された指紋認証システムは、スウェーデンのPrecise Biometrics ABのBioCoreIIである。これは組込みシステムであって、キットにハードウェアが含まれていた。

20

【0224】

顔認証システムは、リトアニアのNeurotechnologija Inc.のVeriLook SDK 1.1である。カメラのLogitech QuickCam 4000 Proは、Neurotechnologija Inc.からの推薦により選択された。

【0225】

音声認識については、ロシアのSpeechPro Inc.のVoiceKey SDKのライセンスが購入された。顔認証カメラは、インターネット会議に使用するために組み込まれたマイクロフォンを有していた。マイクロフォンは音声認証システムに使用できるので、これは有益であった。しかし、時間が足りないので、このシステムでは音声認識は実行されなかった。

30

実装された認証システム

【0226】

以下は実装された認証システムの概要であり、矢印は異なる部分が相互にどのように通信を行うかを示す(図12参照)。

SCリーダ: ISO7816規格のスマートカードリーダ

指紋スキャナ: 指紋イメージをBioCoreIIへ送信するRF指紋スキャナ

カメラ: USBを介してメインPCに接続される標準的VGAウェブカメラ

Mic: カメラに組み込まれたマイクロフォン

40

BioCoreII: 組込み型指紋認証システム。指紋スキャナから指紋イメージを受け取る。メインPCに対してテンプレートを送受信して、実際の指紋認証プロセスを処理する。

メインPC: 指紋スキャナ(BioCoreIIを介して)とマイクロフォンとカメラからデータを収集するPC。コンピュータはまた、テンプレートデータベースと、結果を比較考量するためのアルゴリズムとを保有して、認可を許可/拒否する。

ディスプレイPC: ディスプレイPCはGUIを使用し、トラック運転台の中央コンソールに搭載されたタッチスクリーンに情報を提示する。

タッチスクリーン: トラック運転台のダッシュボードに搭載されたタッチ式7インチワイドスクリーンTF Tモニター。情報および指示を表示するとともに、PIN認証中にはキー

50

パッドとして機能する。

機器の配置

【0227】

シミュレータにシステムを実装する前に、機器の配置について論考された。指紋スキャナをギヤシフトレバーに設けるという考えがあったが、シミュレータにはそれがないので、スキャナはハンドルに設けられた。顔認識システムは、あらゆる方向に5度を超えない角度から検索された写真を必要とする。こうして、機器類の上またはフロントガラス上のルーフのいずれかというカメラ配置の二つの可能性が考えられた。後者の配置では、システムはうまく作動せず、カメラは機器類の上に配置された。ダッシュボードはスクリーンがぴったりとはまる開口部を有していた。またこの取り付けにより、キーパッドの配置は

10

ソフトウェア

【0228】

3社の製造者すべてがC++環境用の開発キットを提供しており、そのためこの開発プラットフォームが選択された。実際的手段（例えばコードそのもの）は本出願の目的または結果にとって重要でなく、そのためこれ以上詳細には記載しない。

グラフィカルユーザインタフェース（GUI）

【0229】

GUIの目的は、ユーザとシステムが相互に通信できることである。本節では、設計段階とともに結果が提示される。

20

GUIの開発

【0230】

最初に、低f iのプロトタイプが紙にスケッチされ、検査中に見せられる各メッセージに1枚の紙が用意された。言葉のメッセージとイラストの両方があり、メッセージの一部は二つまたは三つの種類があった。スウェーデン語が検査参加者の母国語であると推定されたので、言葉のメッセージはすべてスウェーデン語であった。メッセージを補助する適当な音声の研究も行われた。GUI設計の経験がほとんどまたは全くない5人のVTEC従業員の反応を見るため、彼らに低f iのGUIが個別に示された。最初に1種類のメッセージを、検査で現れる順に見せられた。二番目に別の種類を見せられ、どちらを使用するか意見を述べるように求められた。

30

【0231】

次に、GUIによる作業と検査状況に多くの経験を持つ人に低f iのGUIが示された。検査シナリオとGUIについて話し合われ、二つの注釈が加えられた。次にGUIがMacromedia Director MXに実装された。

実装されたGUIの結果

【0232】

認証手順のあらゆる段階は、言葉のメッセージ（スウェーデン語）とイラストと音声を含んでいた。ドライバの注意をスクリーンに引き付けるため、二つの異なる音声を使用した。最初のものは、新しい作業が要求されていることまたは直前の作業がうまく行われたことを示すものとして使用された。二番目の音声は認証が失敗するかエラーが発生した場合を示すのに使用された。さらに、絵が、成功の場合には緑色に、失敗では赤色に変わった。以下はGUIの二つの例である（図14参照）。

40

運転シミュレータ

【0233】

システムプロトタイプの実験中にできる限り現実的な状況を可能にするために、シミュレータが必要であった。VTECは、この検査のために提供されたシミュレータを有する。このシミュレータは、大型アーチスクリーンに投影する3台プロジェクタを有する。このタイプの配置は、実際に移動している感じを強めて、1台のみのプロジェクタと平面スクリーンとを使用する場合よりも妥当な形でドライバが周囲を認知できるようにすること

50

である。V o l v o F H I 2 の運転台が、部屋の中央、スクリーンの正面に置かれた。シミュレーションエンジン音の出るスピーカをオンにすることが可能であった。

【0234】

このシミュレータは最近まで自動車の検査に使用されており、そのため運転台とシミュレータとはまだ充分には同期化されていなかった。検査にあまり適していない性質が他にもあり、著者らはこれを変更することができなかった。例えば、内部においてドライバはスロットルとブレーキは扱えたが、パーキングブレーキとクラッチとギヤシフト、そしてクルーズコントロールも備えていなかった。タンクは常に空であり、回転速度計も走行距離計も、トラックを表すように調節されなかった。パーキングブレーキがなかったため、ドライバが停止して車両から出る必要がある場合には、シミュレータをオフにする必要があった。ブレーキが押下されている限りシミュレータは動かないが、（運転席を出る時など）ブレーキを解除すると、シミュレーション車両はゆっくりと前方へ移動し続けた（図15, 16 参照）。

10

検査前の準備

【0235】

トラック内部に認証システムを設けるというアイデアでは、このようなシステムがいつ使用されるか、何のために使用されるか、どれほどの頻度で認証が行われるべきかについていくつかの疑問が生じる。仮定的疑問のいくつかは、シミュレータ検査の使用によって回答可能である。他はさらなる研究と確認検査を必要とする。

【0236】

20

検査の準備は主として四部、つまりインタビュー質問を用意すること、シミュレータのシナリオの概要を作成すること、十分に適切な数の検査対象者を見つけること、パイロット検査を実施することで構成される。前に述べたように、いつどのように認証が行われるべきかに関する疑問が準備作業中に生じた。（他の疑問のうち）これらの疑問に回答するため、インタビューと検査シナリオの概要が作成された。

インタビュー

【0237】

検査の準備をする際に、インタビューに合うようにアンケート質問が調整された。前のアンケートの結果との比較を可能にするため、多くの質問が似たようなものにされた。

インタビュー質問の考案

30

【0238】

二つのインタビューが用意された。最初はシミュレータ検査の前に実施されるもので、二番目のより網羅的なインタビューが後で行われた。検査中にドライバが意見を変えたかどうかを確かめるため、前のインタビューの質問のいくつかが繰り返された。

【0239】

再定義、追加、削除されるべき質問があるかどうかを確かめるため、二人の行動科学者によって質問が読み上げられ、コメントが加えられた。

質問

【0240】

40

最初のインタビューは、ドライバの作業ルーチンについての質問から始まった。質問は、セキュリティなどの問題とそれがドライバに何を意味するかに関するものであった。バイオメトリクスについてのドライバの知識を調査した後で、すぐ反応できるように、検査に使用される様々な方法について紹介された。ドライバはまた、認証システムの長所または短所に気づいたかどうかを質問された。

【0241】

二番目のインタビューは検査経験についての質問であった。ドライバは、様々な方法にランクを付け、考えられる長所または短所について自分の意見を述べるように再び求められた。

【0242】

質問の多くは常に1から5までのランクが付けられ、1は否定的な意見、5は肯定的な

50

意見を表す。

検査シナリオ

【0243】

シミュレータへの実装に必要なものを見つけて何の検査が可能であるかを知るため、検査シナリオの概略が作成された。

シナリオの概略作成

【0244】

これらの見解は、検査シナリオの作成中にインスピレーションとして機能した。シナリオの概略は創造的集団思考法および論考を通して作成され、問題のいくつかの面が含まれる最終検査シナリオとなった。停止中と運転中の両方の方法をできる限り多く検査することが望ましかった。同時に、短い検査時間中にあまりに多様な作業を含む危険性を回避するため、シナリオはできる限り現実的なものとすべきである。さもないと、検査参加者は自分のIDを極めて頻繁に認証しなければならないと感じてしまい、これは実生活ではあり得ないことである。その結果得られたのは、バランスがよくて網羅的なシナリオであった。

10

検査シナリオ

【0245】

検査シナリオは、詳細な初回認証で始まる。次にドライバは、運転中の指紋認証が要求される前にシミュレータに慣れるための時間を与えられるべきである。シミュレータでの時間のほぼ半分が過ぎた後で、「コーヒーストップ」が設けられた。休憩の後、ドライバは指紋と音声のいずれかを使用して短い認証を受けなければならなかった。検査が終わる前に別の運転中認証が要求され、今度は音声認証であった。運転中、一方は開始時に、他方は休憩後に、二種類の自動認証が行われた。失敗した場合に、ドライバは代わりに指紋認証を要求されるが、成功した場合には検査中にそれについて知らされることはなかった（図17参照）。

20

検査対象者の募集

【0246】

検査のためのトラックドライバの募集は、外部の会社に外注された。20人のドライバを選ぶように依頼され、長距離と配達ドライバが混合していることが望ましいとも言われた。募集の間、ドライバは、実用性とユーザ受容性が評価される運転シミュレータ検査に参加すると告げられた。募集中に検査についての大まかな情報を与える目的は、異なる背景と予想を持つドライバをうまく混ぜて受け入れることであった。

30

パイロット検査

【0247】

システムの改善とシナリオおよびインタビューの調整を可能にするため、実際の検査前にパイロット検査が行われた。

【0248】

パイロット検査で回答される予定の質問は、例えば次のようであった。

- シナリオは現実的か。作業が多すぎるまたは少なすぎるか、時間が長すぎるまたは不十分ではないか。別の順序で進めるべきか。

40

- GUIの設計はよいか。何をすることが常に明白か。音声は特定の瞬間に聴き取り可能であり適切であるか。

- カメラの配置は受容できるものか。指紋センサおよびキーパッドに簡単に届いたか。マイクロフォンに直接ではなく何もないところに向かってパスワードを言うことはやりにくいと感じるか。

- インタビュー質問は重要で順序正しく行われているか。質問が多すぎるまたは少なすぎることはないか。

- 検査の時間が長すぎるか、さらに作業を加えることはできるか。撮影され、運転席で検査監視者に観察されるのは快適に感じるか。

パイロット検査の手順

50

【0249】

トラック運転の様々な経験を持つVTECの従業員が参加を依頼された。その中で、行動科学者はインタビューについて意見を述べるように特に依頼された。全部で6人の男性が参加した。そのうち3人は、検査手順全部と両方のインタビューと受容性アンケートとシミュレータシナリオを経験した。他の3人は、インタビューは受けずにシステムに登録しただけで、シミュレータについて指示を受けてシナリオの検査をした。顔認証の要件を確かめるため、様々な光線条件の検査が行われた。

パイロット検査の結果

【0250】

パイロット検査は、安定性と実用性を高めるためと検査をできるだけ確実かつ網羅的にするため、システムの修正を含む。PIN認証中にスクリーンに現れるただのアステリスクの代わりに、ユーザが数字をダイヤルする時に聴覚で聞き取れるフィードバックを受けるように、第3の音声が増加された。インタビュー質問のいくつかは、より明確になるように調整された。

【0251】

暗すぎる場合には参加者は（顔認識のために）登録されず、シミュレータスクリーンからの光線だけでは登録に充分でないことが明らかになった。他方、部屋の照明はシミュレータのイメージの質に影響するので、照明は強すぎてはならない。運転席内の光線を明るくして実験すると、余分な照明は反射を起こすのでメガネを掛けた人には問題が生じた。最終的に、すべての検査対象者のシステムへの登録と認証を可能にする照明の配置が見つかった。これらの光線実験中の興味深い所見は、登録の時よりも部屋の光線が弱い状態で（メガネを掛けていない）一部の人を認証することが可能であるということである。

検査

【0252】

本節では、プロトタイプシステムの最終検査について説明する。第一部で、検査とインタビューがどのように行われたかを説明し、第二部では結果を示す。

検査手順

【0253】

検査状況をできるだけ明確にするため、上述したシミュレータで認証システムが検査された。残念なことに2人のドライバがキャンセルしなければならず、そのため招かれたドライバのうち18人のみが参加でき、すべて男性だった。ドライバは一度に1人ずつ検査とインタビューを受けた。

シミュレータ検査の前

【0254】

ここからはドライバとも呼ばれる検査参加者は、到着すると、検査監視者に迎え入れられる。彼は自分の権利と義務、例えば匿名性は保証されること、いつでも検査を中断できることを口頭と書面の両方で通知された。仕事について最初にインタビューされてからシミュレータを運転し、それから検査経験について再度インタビューを受けると告げられた。検査監視者は、インタビューを記録することの許可を求めた。

【0255】

発明者の1人はすべての検査中に検査監視者となった。他は技術者として働き、登録およびビデオ記録に責任を持った。

第1回インタビュー

【0256】

検査段階は、ドライバの通常の勤務日、作業ルーチン、セキュリティについての意見、バイオメトリックスについてどのような知識と経験を持っているかについてのインタビューで始まった。第1インタビューはおおよそ20分続き、シミュレータの隣の会議室で行われた。検査監視者はドライバの回答を書き取るか、解釈して質問のタイプに応じて1（否定的な値）から5（肯定的な値）までランクを付けた。ランク付け質問への回答があいまいである場合には、ドライバは1と5の間の点数をつけるように求められた。ドライバが

質問を誤解していると思われる場合には、検査監視者によって説明された。

登録

【0257】

最初のインタビューの後、検査参加者はシミュレータに案内され、座って、シートとハンドルとを通常の快適な運転位置に調節するように求められた。登録が始まる前に、技術者はカメラがドライバの明瞭な写真を撮影したかを確認し、必要であれば、ドライバはハンドルを下げるように求められる。

【0258】

ドライバがPINを与えられてから登録段階が開始する。彼は指紋のどの部分をスキャナに載せるかを指示される。スキャナはハンドルに設けられているので、参加者は右手の親指を使用しなければならず、他の指は走査に適した位置にはなりにくい。正しい配置に慣れるため、スキャナに親指を何回か載せるチャンスが与えられる。その後、指紋が登録される。それから技術者は、運転しているかのようにまっすぐ前方のシミュレータスクリーンを見るようにドライバに要求するが、これは顔認識テンプレートを回収するためである。音声認証では、ドライバは、コンピュータによる分析を可能にするため最低3秒続くフレーズが必要であると言われる。またマイクロフォンがカメラに組み込まれていると告げられるため、パスワードを大声で言うだけでよい。ドライバは「私の名前は（名）（姓）です。」というパスワードを与えられた。上述したように、音声認証の機能はシミュレーションに過ぎない。

シミュレータ説明

【0259】

登録が完了すると、ドライバはスマートカードを渡され、これは検査中の彼個人のデジタル回転速度計カードであると言われる。次に車両から降りて、シミュレータと検査シナリオについての説明を受けるように言われる。

【0260】

ドライバは、検査中に写真を撮られることと、不快に感じたらいつでも検査を中断する完全な権利を持つことを告げられる。通常は車で気分が悪くなることなく、シミュレータでは一部の人の吐き気を催すことがあると言われる。ドライバの注意は、この時には大通りの中央で停止しているシミュレタイメージに向けられた。ドライバは、検査監視者が運転席内で横に座って道を案内すると言われた。しばらく大通りを走行してから、右に曲がり、村に着くまで走り続けると説明される。村で休憩のために停車してから、さらに2分間の運転が続くシナリオとなる。ドライバは、そこにある機器について、足りない機器（「運転シミュレータ」で言及）とともに説明される。実際に運転したのは20分であるが、午後にシナリオが終わると想像するようにドライバは言われる。

【0261】

短い説明の後、ドライバは検査を始めるため運転台に再度乗り込むように求められる。検査監視者は、反対側から車両に乗って、ドライバが席に着きドアを閉めると、シミュレーションを開始する。

シミュレータ検査

【0262】

ドライバは運転席に座った。検査観察者反対側から車両に乗り込み、ドライバがドアを閉めるとシナリオを開始させる。スマートカードを挿入すると初回認証が開始される。この第1回認証は四つの方法で構成され、システムが次の方法に進む前に、各方法で3回失敗することが認められた。ドライバが最初の三つの方法のうち少なくとも二つに合格すると、初回認証全体が成功したと考えられた。第4の方法は、検査中にシミュレーションされるだけの音声認識である。

【0263】

すでに説明したように、検査は大通りのシミュレーションで始まった。しばらくしてから、検査監視者は第1回運転中認証を起動させるが、これは自動顔認識である。失敗しなければ、ドライバはこの認証について知らされないことに注意すること。自動認証が失敗

10

20

30

40

50

した場合、システムは指紋認証を使用して I D を認証するようにドライバに求める。これも失敗した場合には、システムはドライバに P I N をダイヤルするように求める。

【0264】

検査参加者は運転を続け、しばらくしてから、検査監視者は、第2運転中認証である次の段階を起動させる。指紋を使用して I D を認証するようにドライバに求めるシステムダイアログが現れた。認証が失敗した場合には、ドライバは P I N 認証を要求された。

【0265】

またしばらく運転した後、道路は小さな村に達し、ここでドライバはコーヒープレイクのため片側に寄せるように要求された。(これは、ドライバが車両に乗り込んでシナリオを開始させた時からおよそ12～13分であった。)ドライバと検査監視者とはトラックから降りて別の部屋へ行き、ここでドライバは何か軽食を提供された。これには二つの目的があった。第一は、再び運転しようとする時に短い認証を開始する短い休憩をシミュレーションすることであった。第二は、検査の第一部でのコメントと反応をすぐ検査監視者に伝える機会をドライバに与えることであった。他の自動システムとの統計的比較を可能にするため、休憩中に受容尺度[56]がドライバに手渡された。参加者の母国語はスウェーデン語であったので、皆、スウェーデン語版の受容尺度を受け取った。尺度は、五つは実用性を、四つは満足度を反映すると考えられる9対の対照的な単語で構成される。実用性と満足度に関する回答をそれぞれ追加することにより、これから平均が計算され、-2と+2の間で実用性と満足度に点数をつけた。評価されるのはシミュレータではなく認証システムのみであると検査監視者は説明した。ドライバが書面による指示を読んでも受容尺度を理解できない場合には、検査監視者がさらに説明してからドライバに1人で回答を埋めさせた。

【0266】

一部のドライバはコーヒープレイクのために降りる際に「回転速度計カード」を携行したが、大部分はリーダーに残したままであった。休憩後にドライバが運転席に再び座ると、検査監視者によってシナリオが続けられた。ドライバがカードを残していた場合には、システムはすぐに認証手順を開始した。ドライバがカードを携行していた場合には、認証を始める前にカードを要求することによってシステムが開始する。最初の10人の参加者については、システムはドライバに指紋を使用して I D を認証するようにドライバに要求し、残りの8人には音声認証が使用された。この単一の認証が失敗した場合、ドライバは P I N をダイヤルするように求められた。認証要求からおよそ6秒後に「音声認証が成功した」と G U I がアナウンスするようにシナリオはプログラムされていた。参加者がシミュレーションに気づくことを回避するため、十分な早さでパスワードを言わなかった場合には検査監視者によって気づかされた。

【0267】

しばらくしてから、道路は町に通じ、検査監視者は、最後に述べた第1回認証に類似した第2回運転中自動認証を起動させる。システムが認証に成功しなかった場合には、ドライバは失敗を告げられ、代わりに指紋を使用して I D を認証するように求められる。この認証も失敗した場合には、ドライバは P I N をダイヤルするように言われる。

【0268】

参加者は運転を続け、検査監視者は最後の認証手順である運転中の音声認証を起動させる。この認証の直後にドライバは、車を寄せて停止するように求められた。

フォローアップインタビュー

【0269】

検査の後、ドライバはまた会議室へ案内されて再びインタビューを受けた。第2回インタビューは、各認証方法、G U I、シナリオを挙げて、検査全体についてのドライバの体験を尋ねるものであった。

【0270】

ドライバは第1回の初回認証と運転中認証の体験(それぞれ指紋走査と音声認識)について尋ねられた。自動認証が成功している場合には、ドライバはその存在について知らさ

れた。このような方法の使用と、自動認証が失敗した場合に別の種類の認証を行うという考えについて意見を出すように促された。自動認証によってうまく認証されなかったドライバは、運転中にまた別の種類の認証をしなければならなかった体験について尋ねられた。運転中に自動認証をすることについての意見も述べるように促された。検査中に行われた様々な方法と認証の比較を可能にするため、ドライバはそれぞれの場合について同じ質問を受けた。認証／方法が複雑であるか簡単であるか、時間がかかるか短時間であるか、不合理であるか妥当であるか、退屈であるか面白いのか、つまらないか興味深いのか、不必要か必要かどうか、繰り返される質問にランク（1～5）が付けられた。

【0271】

ドライバは、セキュリティと認証システムの車両への実装についての考えを質問された。検査により意見が変わったかどうかを確かめるため、検査の前と後にそれについての考えを述べるように促された。1回の検査が終了する前に、何か追加したいかどうか、検査に何か欠けているかどうか、質問があるかどうかドライバに尋ねられた。

検査の結果

【0272】

本節は、検査参加者の紹介で始まる。以下、第1回インタビューとシミュレータ検査とシミュレータ検査に続く詳細なインタビューの結果について提示する。すべてのインタビューはスウェーデン語で行われ、ここに示される引用は著者による翻訳である。

【0273】

参加者の平均年齢は41歳であり、標準偏差は11歳であった。最年少の参加者は23歳、最年長は60歳であった。参加者は3年間から40年間まで、平均して18年間、トラックドライバとして働いていた。4人のドライバは長距離運転のみ、6人のドライバは主としてイエーテボリ地方で運転し、残る8人は様々な距離を運転していた。

第1回インタビューの結果

【0274】

「セキュリティ」が何を意味するかの質問について、大部分のドライバは安全な車両の話をした。質問が犯罪行為に対するセキュリティに明確化されると、大部分のドライバは長距離ドライバが車内に備えているガス警報機の話をした。安全でも危険でもない点数を入れた一人を除いて、すべてのドライバが勤務中、安全であると感じていた。平均点は4.78で、標準偏差は0.55であった。10人のドライバによれば、人が運転する環境または地域が安全の感じ方に影響するかもしれないということだった。3人は、環境とともに時刻も要因であると考えていた。3人のドライバによれば、安全の感じ方に影響する他のことがらがあり、それは例えばどの種類の荷物を運搬しているかである。ドライバのうち2人は、全く安全だと感じており、安全の感じ方に影響する要因を思いつかなかった。

【0275】

1人を除いて全員が、特定の物品または地域へのアクセスのために勤務中にカードを使用していた。カードを使用していない一人は、アクセスのためにPINを使用していた。8人のドライバは、カードとPINの両方を使用していた。

【0276】

11人のドライバは、1人またはそれ以上の他のドライバと車を共有していた。他は自己所有の車両だったが、何人かは、病気の場合には他の人がその車両を運転し、また誰か別の人に自分の車を貸すこともあると述べた。

【0277】

インタビュアーの手助けなしでバイオメトリクス方法に言及できたのは、2人のドライバのみであった。2人は、指紋認証を例として与えられても、他の方法は思いつかなかった。それにもかかわらず、3人のドライバはバイオメトリクス方法で認証／識別を受けたことがあり、誰もこれに反対していなかった。バイオメトリクスを使用したことのない人たちの点数は、1（否定的）から5（肯定的）までの尺度で平均4.20であり標準偏差は1.42であった。彼らのうち11人は肯定的で、全員が5点を付けた。1人のドライ

10

20

30

40

50

バの点数は1、2人の点数は2、最後の1人の点数は3で否定的でも肯定的でもなかった。

【0278】

バイオメトリクス認証方法の使用の欠点として考えられるものについて尋ねられて、6人のドライバはリスクに気づいていた。他方、2人のドライバはバイオメトリクスの可能性または長所にも気づいていた。10人のドライバは、長所と可能性のみに目を向けていた。残りの2人は質問に回答しなかった。

検査シナリオの結果

【0279】

18回の検査全体を通して、システムは良好に機能した。本節では結果について簡単に論じる。結果はどれくらいの頻度で参加者が認証の合格に成功したかについて述べているに過ぎないことに注意すべきである。著者らは、他人受入率についてシステムを簡単に調べた。一つの例も発生していなかった。

初回認証

【0280】

初回認証は、実装された認証方法すべてで構成される。すべての参加者について少なくとも一つの方法は成功したため、全員がエンジンの始動を承認された。

【0281】

18人の参加者全員がPIN認証に成功した。1人は一度間違ったコードをダイヤルしたが、二回目の試行では成功した。

【0282】

指紋認証は14人の参加者について成功した。これら14人の参加者のうち1人は、2回以上の試行が必要だった。参加者の一部は、システムが模様を発見できなかった場合に親指をどこに載せるか案内された。（理論について上述したように、指が正しく置かれないうちの多くはよくある問題である。）

【0283】

11人の参加者について、顔認識に成功するには1回の試行で充分であった。合計で16人の参加者について顔認識は成功した。

【0284】

音声認識のシミュレーションが行われ、すべての参加者が合格したが、何人かは何を言うかを思い出させる必要があった。

【0285】

参加者の1人は、指紋認証によっても顔認識によっても認証されなかったが、PINが正しかったので承認された。他の参加者のうち2人は、指紋認証によっても認証されなかった。このような場合に顔認識では、認証の成功に達するまで2回の試行が必要であった。残りの参加者のうち3人の認証では顔認証でも指紋認証でも問題が発生したが、それでもすべての方法が2回以上試みられたので、全員が認証に成功した。

第1回運転中認証（自動的顔認識）

【0286】

システムは、参加者のうち13人を自動的に認識した。自動的に認識されなかった人たちのうち2人は、指紋認証も失敗したのでPINをダイヤルしなければならなかった。

第2回運転中認証（指紋認証）

【0287】

指紋認証は13人のドライバについて成功し、そのうち10人が最初の試行で合格した。残りは最初の試行でPIN認証に合格した。

受容尺度の結果（コーヒープレイク中）

【0288】

コーヒープレイク中に回答されたアンケートから、システムは満足できるものというよりは便利なものとして認知されていることが分かった。実用性と満足度に関する各参加者の平均点（-2と+2の間の尺度）については、以下を参照すること（図18参照）。

10

20

30

40

50

【0289】

尺度はシステムの実用性についての五つの質問と満足度についての四つの質問を表すと考えられるので、すべての満足度質問とすべての実用性質問についてドライバがそれぞれ同じような点数を入れているかどうかを確かめるため、回答の計算が行われた。この計算にはCronbachのアルファが使用された。この場合、受容尺度の信頼度統計は、実用性については0.787、満足度については0.698の点数であり、これはドライバが質問を意図通りに理解したことを示す。

【0290】

すべての質問が少なくとも一つは最高ランクを受け、ほとんどすべてが少なくとも一つの最低ランクを付けられたので、意見は参加者の間で様々であった。システムが役に立たないと感じたドライバはいなかったが、3人は悪い方の点数を入れ、3人は良くも悪くもなかった。実用性は平均点が0.80で標準偏差が0.72であり、満足度は平均点が0.24で標準偏差は0.89であった。何人かのドライバはシステムをいらいらすと感じた。言葉によるコメントでは、いらいらさせるのは特に運転中の認証であったことを示していた。ゆえにシステムはあらゆる人にとって好ましいわけではないが、否定的回答よりも肯定的回答の方が多かった。

短時間休憩後の認証（指紋／音声認証）

【0291】

最初の10人の参加者は、休憩後に車両を始動する前に指紋認証を使用した。10人のうち9人は認証され、そのうち8人は最初の試行で認証された。うまく認証されなかった参加者は、認可のためコードをダイヤルしなければならなかった。PIN認証は最初の試行で成功した。

【0292】

残る8人の参加者は音声認識を使用した。何人かのドライバは何を言うかを検査指導者に教えられなければならなかったが、この認証は全員が合格するようにシミュレーションされていた。

第3回運転中認証（自動的顔認証）

【0293】

自動的認証は参加者のうち15人の認証に成功し、そのうち12人は最初の試行で認証された。次の指紋認証は、残る3人の参加者のうち2人について最初の試行で成功した。3番目の人は、指紋認証も失敗したのでPINをダイヤルしなければならなかった。彼は最初の試行でPINにより認証に成功した。

第4回運転中認証（音声認証）

【0294】

第4回運転中認証は音声認識であり、シミュレーションされていたので、すべての参加者が合格した。

フォローアップインタビューの結果

【0295】

このインタビューでは、バイオメトリクスと認証方法に関連するより一般的な質問とともに、様々な方法について明確な質問が行われた。加えて、ドライバはGUIおよびこれに関連する音声についても尋ねられた。そのすべてを本節に提示するため、本節はいくつかの部分に分かれている。

システムへの最初の反応

【0296】

検査後のドライバからの最初の反応は、主として肯定的であった。9人のドライバは検査を現実的だと感じた。7人のドライバは未来の映像であると考えた。1人のドライバは検査を非現実的だとし、残るドライバは質問に明確な回答をしなかった。

GUIおよびその音声

【0297】

1人を除いてすべてのドライバはGUIに最高点（5）を付けた。この人は3のランク

10

20

30

40

50

を付けたので、G U I は 4 . 8 9 の平均評価を得点した。1 2 人のドライバは G U I に関連する音声に気づいた。「正解の時と不正解の時の差すら分かった。」と 1 人のドライバは言った。音声を入れることの是非についての質問に対する回答として、ドライバは平均 4 . 5 と評価し、標準偏差は 1 . 2 4 であった。音声に気づいていた 1 2 人のドライバのうち 1 0 人は 1 か 5 の点数を付けたので、ドライバは音声を好むか好まないかのいずれかであると思われる。平均点は 3 . 3 8、標準偏差は 1 . 8 9 であったため、音声に役に立つのかわずらわしいのかを判断するのは難しい。

【0298】

ドライバは自分で G U I を扱い、前もって何の指示も与えられていなくてもすべきことを自発的に行った。時には、始動に熱心で、G U I が開始する前にカードを挿入すべきかどうかを検査監視者に尋ねたが、このような場合に、通常は、検査監視者が回答する間もなく最初のメッセージが示された。1 人は 3 番目の数字を間違えてダイヤルしてから検査監視者に向かって、「間違った番号をダイヤルしてしまった。どうすべきか?」。検査監視者が正しいと思うことをするように彼を促すと、間違った数字を消すための正しいボタンを本能的に使用して、通常通りに続けた。

初回認証

【0299】

すべてのドライバは、走行を開始する前の初回認証は簡単であると感じた。使いやすさの平均点は 4 . 8 9 で標準偏差は 0 . 3 2 であった（2 人は 4、残りは 5 と評価した）。1 0 人のドライバは、この認証を行うのは妥当だと考えた。1 人は妥当であるか不合理であるか分からなかった。残る 7 人は不合理であるか、少し不合理であると考えた。必要性についての質問では、平均点は 3 . 1 4、標準偏差は 1 . 8 0 であった。すべての質問を要約すると、この第 1 回認証の平均点は 3 . 7 1 であり、標準偏差は 0 . 6 8 であった。

自動的顔認証

【0300】

カメラを使用して自動認証が行われたと告げられると、大部分のドライバはよい考えだと思った。カメラにより認証されずに指紋認証を行わなければならなかったドライバは、きわめて妥当だと考えた。それと知らずに認証された人々は、失敗した場合には指紋認証を受けなければならないという考えにほとんど肯定的であった。

【0301】

システムが認証に失敗した 4 人のうち 1 人は、システムに否定的であった。他の人に関しては、認証の成功／失敗とシステムについてのドライバの感じ方との間の相関関係から結論を引き出すことはできない。そのうち 1 人は、システムが自動認証を試みたという事実も、システムが自動認証に失敗したので他の認証をしなければならないことも気にしなかった。また別の人はシステムが認証を自動的に行うならばそれが良いが、成功しなかった場合には、正しく座って認証ができるようにドライバに警告すべきだと言った。4 番目の人は運転中の認証はいずれも好まず、自動的なものも好きではなかった。「運転中に起こることは少なければ少ないほどいい。」

運転中の指紋認証

【0302】

ドライバが指紋走査を行わなければならない第 1 回運転中認証は、第 1 回認証ほど簡単であるとは見なされなかった。運転中指紋認証は平均点が 3 . 1 9 で標準偏差は 1 . 6 7 であった。この認証は、妥当よりは不合理と感じられる傾向があった。1（不合理）から 5（妥当）までの尺度では、運転中指紋走査は平均点が 2 . 9 4、標準偏差が 1 . 8 6 であった。この認証が必要かどうかの点数は 3 . 1 1、標準偏差は 1 . 7 8 であった。合計点数としてこの運転中指紋認証は 3 . 1 9 であり、標準偏差は 0 . 3 8 であった。

休憩後の認証（指紋／音声）

【0303】

コーヒープレイクの後、最初の 1 0 人のドライバは指紋で認証を行い、他の 8 人は音声認証を用いた。どの方法を使用しても、すべてのドライバはこの認証は簡単であるに点を

10

20

30

40

50

入れた。二つの方法を一緒にすると、この認証の点数は4.17で不合理よりも妥当であり、標準偏差は1.50であった。必要性は3.78と評価され、標準偏差は1.83であった。すべての質問が含まれて両方の方法が追加されると、この認証の点数は4.12であり標準偏差は0.68だった。

【0304】

休憩後に指紋認証を使用した人たちは、妥当に近い平均4.60と評価し、標準偏差は0.97であった。必要性の点数は平均4.40で標準偏差は1.35であった。1人の人は指紋認証に失敗したため、PINもダイヤルした。彼は、システムが妥当であるかについてだけでなく使いやすさにも5点を入れたが、必要性の質問には3点を入れた。

【0305】

休憩後に音声認証をしなければならなかった人たちは、この認証が不合理(1)であるか妥当(5)であるかについて、平均3.63の点数を付け、標準偏差は1.92であった。この質問の平均は3.00で標準偏差は2.14であったので、必要とも不必要とも評価されなかった。ドライバの何人かは、パスワードを思い出さなければならなかった。これは、この認証がシミュレーションであると参加者が気づくことを回避するためだけに行われた。

運転中音声認証

【0306】

第2回運転中認証がシミュレーションされ、一部のドライバはパスワードを言う時に若干のミスをしたが失敗は全くなかった。初回認証後に音声認証を使用したことのないドライバの一部はパスワードを思い出す必要があった。休憩後に音声認証を使用したドライバはすべて、システムにすぐに回答した。ドライバ全員が5点を入れ、例外がなかったので、この認証は簡単だと考えられた。この認証を行うことが妥当であるか不合理であるかについての質問では、平均評価は3.41、標準偏差は1.84であった。平均点が2.71で標準偏差は1.99であったので、最も必要のないと考えられた認証であった。すべての質問を要約すると、この認証の点数は3.65、標準偏差は1.08であった。

方法全般

【0307】

認証方法全般、指紋、音声、顔またはコード認証の使用についてドライバが感じることを質問された際には、音声認証は4.61の最高点を集め、標準偏差は0.66であった。指紋と音声認証はともに、信用性については最高の評価を受けた。これらはともに4.28の最高点を得た。指紋の標準偏差は1.23、音声は1.27であった。信用性の質問では、顔認証の平均点は3.67、コード認証は3.72であった。標準偏差はそれぞれ1.61と1.60だった。

【0308】

ドライバの一部は、指紋スキャナとGUIのスクリーンのいずれの配置も好まなかった。道路から目を離すことを望まず、代わりに音声指示を行ってGUIがハンドルに近接するか機器類に統合されることを提案した。別の提案は、運転席の右側に指紋を載せることであった。

【0309】

インタビューの終わりに、ドライバは、検査を受けた認証方法に、最も好感を持つものには数字の1を、次には数字の2をというように好感度の順に評価するように促された。参加者の半数は指紋認証を選んだ。顔認証と音声認識とPINとはそれぞれ3人の参加者に選ばれた。この好感度点数の平均評価に関しては、指紋が最も一般的で顔認識が二番目になったが、それでも音声認識はそれほど後ではなかった。カードを挙げたのは2人のドライバのみであった。1人はPINの次に二番目に良い方法だと考えたが、他の人は、他の方法すべてより下の最下位の評価を付けたに過ぎなかった。回転速度計カードとして提示されたので、カードを認証方法と見なさなかったことも考えられ、そうすれば誰もこれを挙げなかった理由を説明できる。

【0310】

参加者の1人は指紋認証を最も信頼できないと確信していたが、気づきさえしなかった
ので顔認識が一番であると見なした。別の参加者は、使用が最も困難であると感じて
いたが、指紋を選んだ。顔認識は最も簡単な方法であると分かっていたが、正面にカメラ
があるのは不快だと感じたので、好まなかった。

認証問題全般

【0311】

10人のドライバは、この種のシステムを車両に設けることを好ましいと考えた。しか
し、すべての方法が必要だと考えるのは2人のみで、8人のドライバは一つの認証方法
で充分だと考え、1人は方法を全く必要とせず、残りのドライバは二つ以上の様々な方法
を推奨したが、すべてを推奨したわけではなかった。システムに望ましい方法の平均数は1
.72で標準偏差は1.32であった。

10

【0312】

検査前に、バイオメトリクス認証を行う短所を認めていなかった人のうち5人が、検査
後に短所を見つけた。検査前に短所に気づいた人のうち4人が、検査後には別の回答をし
た。検査前に長所に気づいた1人は、後では長所を挙げなかった。5人のドライバは検査
後に、前には気づかなかった長所を見出した。

【0313】

この検査前にバイオメトリクスを使用したことのなかった15人の参加者は、第1回イ
ンタビューでバイオメトリクス認証方法に肯定的であるか(5)否定的であるか(1)を
尋ねられた。シミュレータ検査の後、試験後の現在はバイオメトリクス認証方法につ
いてどう思うかを再び尋ねられた。6人の参加者は検査前よりも検査後に否定的な点数を付
け、3人の参加者はより肯定的な、6人の参加者は前と同じ点数を付けた。これらの回答を
下の図に示す(図19参照)。

20

【0314】

点数に関して、15人のドライバのうち11人がバイオメトリクスに肯定的であり(点
数4~5)、2人が否定的であり(点数1~2)、2人は肯定的でも否定的でもなかった
(点数3)。

【0315】

顕著なのは、参加者の数人が、前より高い評価をしなかったけれども検査前よりも検査
後に自分がより肯定的になったと述べたことである。

30

【0316】

参加者は検査後に、前に付けた点数を言うように要求されたので、何人かは実際に入
れた点数よりも低い評価を下したと推定される。

【0317】

すべての参加者のうち4人は、他の状況よりも車両にバイオメトリクスを設けること
に肯定的であった。他の4人は反対で、バイオメトリクスはOKだが車内は良くないと考え
た。残りのドライバは、車内でのバイオメトリクスとバイオメトリクス全般に同じ点数を
付けた。平均点では、車内の認証システムは3.78で標準偏差は1.35であった。バイ
オメトリクス全般の点数は平均で3.76、標準偏差は1.48であった。

【0318】

ドライバの一部は車両での認証システムのアイディアに肯定的であったが、日常業務で
はこれを必要としないと言った。彼ら自身が犯罪または攻撃に会ったことがないという事
実は、ドライバからのコメントに頻繁に見られた。これらの問題について考えるように強
制されると、インタビュー質問に回答するのが容易になったと考えた。作業中は安全だと
感じているので、その問題に自分を関連付けるのは難しいと言った。技術全般の結果は4
.3であった。

40

【0319】

本節では、技術に関して検査中に行われた所見を示す。

指紋認証システム

【0320】

50

指紋システムは検査全体で良好に機能した。2, 3の場合にシステムが無反応となったが、これは、BioCore IIシステムではなくメインPCのCOMポートの問題によるものと思われる。十分に良好なイメージを回収するために何回かの試行が必要とされることがあったが、参加者は登録段階では失敗しなかった。参加者全員が指紋を使用して自分を認証することに少なくとも1回は成功した。

顔認証システム

【0321】

顔認証システムは、指紋認証のシステムよりも動作がより安定している。顔の登録に失敗した参加者はいなかった。しかし、参加者の1人は野球帽を脱ぐまで登録されなかった。帽子が顔に影を作り、これがシステムにとっては複雑であったと考えられる。

10

【0322】

メガネについてもいくつかの問題が発生した。ガラスの反射によりカメラに写らないからである。ある場合には、顔認識でドライバの眼の位置を突き止めるのに成功しなかったため、登録段階が繰り返されなければならなかった。このドライバはメガネを掛けており、検査中に3回の顔認証すべてに失敗した唯一の人であった。

音声認識システム

【0323】

音声認識は検査中にシミュレーションされ、そのためこのシステムの機能性について述べるのは不可能である。

結果の分析と要約

20

【0324】

参加者は認証システムに対して否定的というよりは肯定的であり、車内でバイオメトリクス認証を使用するという考えには主として肯定的であった。指紋認証は上述のように大部分の参加者が好感を持っているものであり、最高の平均評価も得ている。また大部分の参加者が知っていたのもこの方法であった。さらに例を挙げることでできた人は映画で見たことがあると言い、眼のおよび顔／音声認識の話をしたが、それでも、他の方法に言及した人でさえこれらの方法は未来的であると感じていたようである。未来的な印象が好ましい方法の選択に影響したことが考えられる。

【0325】

何人かの参加者は顔認識に肯定的であったが、他はシステムに管理されていると感じ、カメラが好きではないことを忘れてはならない。1人のドライバはこう言った。「この仕事には自由がありそれを好んでいる。すべきことをしている限りは自分のやりたいようにやり、他の人間には関係ない。このシステムだと、もう自分で管理しているのではないと感じる。運転する時としない時を自分に命令するのはシステムだった。」この参加者と別の人は、ドライバ認証が法制化されたら転職を考えると行った。残りの参加者はそれほど極端ではなかったが、このようなシステムを使用するのには慣れていないとコメントした。訓練の機会と情報によって、システムについての肯定的な受容は高まるかもしれない。

30

【0326】

受容に成功するのにいかに情報が重要であるかについての別の例は、何人かの参加者が運転中認証の必要性について質問したことである。しかし、検査指導者と参加者がインタビューの後にそれについて話し合った時には、参加者は運転中の認証について尋ね、検査指導者は次の例を挙げた。「認証されており、荷物に装着する必要のあるワイヤを見つけてエンジンを始動させたトラックドライバを想像する。ドライバが運転席を出てワイヤを固定すると、詐称者が席を奪って車両から追い出そうとする。」参加者は、それは考えたことがなかったと言ったが、車両を始動させた後で飛び降りることはあり得ると述べた。なぜ運転中にドライバが認証されるべきかについての説明によって、参加者は、指紋認証により邪魔されたくはなかったが、それが妥当であると感じた。運転中には顔または音声認識が高く評価された。

40

【0327】

商用車での認証システムは、ユーザのプライバシーを考慮して開発されるべきである。

50

そうであれば、大部分の参加者はアイディアには肯定的であるので、おそらくきちんと受け入れられるようになるだろう。

結論

【0328】

検査を受けたシステムはプロトタイプであって、システムは実生活での使用に十分なほど安定していない。両コンピュータの代わりに組込み制御システムと組み合わされた、自動車の目的に特に適した認証方法により、安定かつ安全な、エラー強さを持つシステムがおそらく達成される。運転中の自動認証が推奨されるが、照明感度についての問題が残っている場合には音声認識が二番目に優れていると思われる。これは、音声認識がドライバの注意をそれほど集める必要がないからであるが、車内での使用に実際に適しているかどうかを判断できるようになる前に方法を検査しなければならない。

10

【0329】

PIN認証は技術的観点からは適した方法であるが、PINは覚えなければならない別のコードであるので大部分のユーザはバイオメトリクス認証を好む。この方法は停止中には適度に機能するが、コードをダイヤルする間に一部のドライバは車のコントロールをほぼ失うので、運転中に使用することは勧められない。同じことが指紋走査にも当てはまり、ドライバ自身がコメントしていたことである。

【0330】

結果で述べたように、一部のドライバはこのように指紋スキャナを配置することは好まなかったが、それを別にすれば、この認証方法は高速で信頼性がある。ユーザが訓練を受けていれば、トラックドライバを認証する目的にはおそらくかなり適しているだろう。参加者の大部分が仕事から直接検査を受けに来た（ゆえに、自分の車に乗り込んだ場合と同じような指走査の確認状況である）がすべての参加者が登録および認証されたので、手が汚れていてもトラブルが生じるとは思われない。現在のように親指のみが認証に使用されるのではなく、右手のどの指でも容易に走査できるようにスキャナは配置されるべきである。正しい位置が分かるように指のガイドを備えることが好ましい大型スキャナであれば、ユーザの認証を容易にするだろう。検査参加者の間では指紋認証が好まれたが、誰もが走査に十分なほど明確な指紋を持つわけではないので、認証システムの唯一の方法とすべきではない。

20

【0331】

顔認識技術は、光線に左右されすぎるので、これらのタイプの用途についてはまだ完成していない。しかし、顔認証は高い点数を取り、ドライバの大部分は自動認証に肯定的であった。これは、ユーザの観点から見て顔認証が好まれていることを示す。何人かのドライバは運転中ずっとカメラに向かっているのは不快だと感じているので、常に監視下にあるわけではないとドライバに確信させることが重要であろう。しかしこのドライバの管理とそのプライバシーとの間でどのようにバランスを取るかは、まだ今後の研究に委ねられる。

30

【0332】

何人かのドライバは音声認識システムに肯定的であったが、いつでも成功するようにシミュレーションされていたので、どうすれば実際にトラック分野に適するかに関する結論を導き出すのは可能でない。同様の音声認識システムについての苦い経験のため多くのドライバは最初これを信用していなかったのが特に、この模擬認証は誤った信用を彼らに与えた。

40

【0333】

GUIの音声役に立つかただ不愉快であるかについてのドライバの捉え方は大きく異なっていた。そのため、ユーザが音声をオンオフできるようにすべきであると考えられる。

【0334】

質問を受けた運送業者の間に見られる最悪の懷疑は、技術に対するものであった。「失敗したらどうするのか」が共通の質問であった。ドライバが車両を動かすことができなく

50

なるような事故、その他の何かが発生した場合のトラブルに大部分が気づいていた。「なんとかして車両を動かす方法がなければならない。」また検査参加者は、事故の場合に車両を動かす解決法の重要性を強調していた。さらに検査参加者は、短い通知で車両ドライバを交代できることが必要だとしていた。これらの問題に考えられる解決法は、6.10節の「自動車の面」で述べる。

【0335】

結果を要約すると、自動車環境に適した認証システムを考案することは可能であると考えられる。それでも、すべてのリスクを消し去ることはほとんど不可能であることを忘れてはならない。例えばIRAは、主要な作戦では当局に知られていない人間しか使用しない。自爆テロでも航空機ハイジャックでも、手段は多くのテロ攻撃に共通する。また別の例は、世界貿易センターへの攻撃を実行したテロリストの数人が自分のIDを使用したということである。そのため、すべてのドライバが認証されても、その車両がテロ行為に決して使用されないと保証することは不可能であろう。予防措置を取ったにも関わらず不測の事態が発生したという例は数多く見られる。それにも関わらず、トラックの認証システムはおそらく詐称者およびテロリストを萎縮させ、それがドライバと運送業者の両方、長い目で見れば社会全体にとって有益となろう。

今後の研究

【0336】

ここで論じた発見は、このアイディアの多様な側面およびドライバ認証の可能性をさらに研究するための多様な示唆を与えた。作業プロセス中に多くの質問が出されたが、本出願ではそれらすべてに妥当な時間内で回答することは可能でなかった。このシミュレーションシステムとインタビューによりドライバの意見についてアイディアが得られたが、それでもより確実な条件下でシステムを検査することが重要である。ゆえに今後の研究では、システムを実際のトラックに実装して検査することが考えられる。以下は、検討しなければならない様々な当該質問の例である。

指紋認証

【0337】

何人かのドライバがセンサの配置を不快に感じたので、より良い配置を見つけることが興味深いだろう。

【0338】

汚れ、傷、たこなどがシステムの性能にどのように影響するかを調査するため、確認条件の下でシステムが検査されなければならない。

顔認識

【0339】

今後の研究では、システムを実際のトラックに設置して確認条件で検査することが提案される。どの状況でシステムが機能するかを検査するため、検査中にドライバが撮影されて運転席内の光線条件が測定されるべきである。これらの検査は、運転席内にカメラを設けることがどれほど適しているかを確かめるためのユーザとの十分なインタビューで補足されるべきである。ドライバの一部は検査中にカメラが自分の方を向いているのは不快に感じたが、他の人は全く気にせずに自動認証のアイディアを非常に歓迎していたので、これは重要な問題である。このようなシステムは、どのように使用されるかについての制約を必要とし、そのためこのようなカメラ監視状況について新たな法律を制定することが必要になるだろう。

【0340】

サーモグラフィの開発がさらに進むと、認証システムにこの方法を使用することを検討すべきである。その際には、好ましくは実際のトラックで一日のシフト時間での様々な状況においてこの方法を検査する必要があるだろう。

【0341】

可視波長間隔と赤外線波長間隔との間の境界には、いわゆるNIR間隔が発見されている。顔面サーモグラフィにまつわる問題は、市場には現実的な認証システムがなく、光線

10

20

30

40

50

条件に左右されるので標準的な顔認識を使用するのは問題があるということである。N I Rカメラを使用することにより、ドライバには見えないがカメラには写るN I Rダイオードでドライバの顔が照射されるので、これらの問題の両方を解決することが可能かもしれない。

音声認識

【0342】

最初は、実験的音声認証システムを検査することが望ましい。結果が満足できるものであれば、実際のトラックでエラー強さについてシステムが検査されるべきである。これは、シミュレータ内のノイズレベルが特に変化しないからである。フィルタリングによってノイズを除去できることが多く、V o i c e K e yシステムを（妥当なリミット内で）実際のノイズレベルに適応させる。しかし、実際のトラックでのノイズ変動がこれらのリミット内であれば検査されなければならない。

10

【0343】

空中に向かって大声で話すことはドライバにとって嫌な感じなので、ドライバシートの付近にマイクロフォンを実装することが必要かもしれない。マイクロフォンが電源スイッチを装備している場合には、システムがいつドライバを「聞く」ことができるかを制御しているとドライバは感じるができる。何人かのドライバが検査中に口にした嫌な感じを別にすれば、これは運転中に使用するのに適した方法だと思われる。指示が音声でも与えられれば、自分とシステムとの会話のようなものなので、音声認証を行うことがドライバにとってより自然に感じられるだろう。

20

【0344】

今回のプロトタイプで使用された文章の代わりとなるシステムからの言葉による指示とともに、映像と音声のみをG U Iに設けることは興味深いだろう。各個人が自分に最も適したシステムとすることができるよう、ドライバが音声指示と音声をオンオフすることが可能であるべきである。

様々な状況での適切な措置

【0345】

ドライバが自分のI Dを認証した時には何が起こるべきか。認証とそれに続く事象に関するシナリオがいくつか可能であり、以下では使用例についてさらに論じる。

【0346】

検討および論考しなければならない問題は、認証が全く成功しなかった場合には何が起こるべきかである。初回認証（エンジン始動の前）を考えると、主として四つの可能性がある。車両の始動が不可能である。車両が通常通りに始動して出発することが可能であるが、ある距離を走った後、歩行速度まで速度が低下してそれ以上に速度を上昇させることができなくなる。車両は通常通りに始動し走行するが、所有者に警告が送信されて、適切な予防措置を取るようにする。認証失敗が車両のボードにログされるが、それ以上の措置は取られない。

30

【0347】

様々な状況を相互に比較考量することは常に困難である。ドライバが正規の人間でなくても、または認可ドライバでなくても車両が動く場合には、望ましくない目的に車両が使用されるリスクが高まる。

40

【0348】

それでも、認可ドライバがいなければ車両を動かすことが不可能な場合には、ドライバを載せたまま車両をハイジャックするリスクが高くなる。社会とドライバのどちらが最も高い優先順位を与えられるべきかは、車両が運搬している積荷の種類と、認証失敗の瞬間に車両がどこに位置しているかに応じて変わる。

【0349】

ドライバが走行中にI Dを認証できなかった場合にはどうすべきか。このプロセス中にもこの質問について論じたが、適切な回答を得るにはいくつかの検査が実施されなければならない。最初の二つの例で車両が停止するか歩行速度まで減速するという変形では、可

50

能性は頭上の弾丸の地点と全く同じである。

認証をいつ行うべきか

【0350】

いつ認証を要求するかも重要な問題である。自由に走行できると仮定すると、無限のシナリオが考えられ、どこかで線を引かなければならない。著者らが提案するのは、ドアが開けられて誰かが運転席に座ったことをシートセンサが報告する時にドライバが自分のIDを認証しなければならないというものである。シートセンサはシートベルト装着信号を起動させるものであり、大部分のトラックはドアが正しく閉じられているかどうかをチェックするセンサを備えているため、これは実装がかなり容易である。

【0351】

運転中にドライバIDを認証したい場合には、どれほどの頻度で行われるべきか。我々のアンケートでは、長距離ドライバが我々に語ったところによれば、彼らは最高で4.5時間連続して運転することもあれば、2時間の走行で8回停車することもある。停車の間に走行する時間または距離は、セキュリティと利便性を相互に比較考量して検討しなければならない。

【0352】

認証の要求はドライバを邪魔することがあるので、あまりに頻繁に行われるべきではないと考えられる。さらに、ドライバが積み込み／積み降ろしのために停車する場合には、車両から降りることが大いにあり得、その場合には降りる前に再度認証が行われなければならない。

【0353】

理想的であるのは、自動的顔認識の場合のようにドライバからの行為を伴わずに運転中認証が実施される場合である。しかしそれでも、自動認証に失敗した場合にはドライバはなにか他の方法で認証されなければならないという事実のため、認証はあまり頻繁に行われるべきではない。

付加的可能性

【0354】

今回のプロトタイプについて設けられたものよりさらに高いセキュリティレベルを設けることが可能である。積荷と、どの地域を車両が走行しているかについての情報を認証システムが持っている場合には、システムが自動的にセキュリティレベルを調節することができる。例えば、ケープタウンの金輸送車は、ラップランド森林の建築現場に砂利を届ける時よりも高いセキュリティレベルを必要とする。

【0355】

使用例で提案したように、マルチモードシステムは認証のために一つのバイオメトリクス方法のみを必要とすることも可能である。必要とされるのがどの方法かはランダムに選択されるため、ドライバはすべてに登録される必要があるが、一度に一つしか使用しない。このランダム化により、詐称者は認証に何が必要であるかを確信できず、様々な特徴すべての偽造サンプルを準備するのに多大な労力を払うことになる。

【0356】

様々な方法がランダムに検査される際の別の利点は、常に一つのみを使用していて、指を失うか、それほど極端でないにしても何かが起こったために突然切り換えなければならない場合よりも、ドライバの慣れが早いことである。

【0357】

認証が全体として成功した場合には、これはデータベースの一つのテンプレートを更新する可能性を与えることになる。例を挙げると、ドライバが最近、カード、PIN、指紋を使用して認証されたと仮定する。これらの方法すべてに成功した場合には、システムは新しい顔写真を撮影して名簿を更新する。ドライバが例えばひげを伸ばしているか剃ったばかりである場合、または登録後にドライバの体重が増減した場合には、これは認証を容易にする。

【0358】

この段階で生じたアイデアは、掌形と指紋走査とを組み合わせることであった。現在のデジタルカメラの解像度は、指紋ばかりでなく指の測定値も分析するのに十分に詳細な掌のイメージを撮影するのに十分に高い。

データベース配置とシステム管理

【0359】

上述したすべての方法では、登録プロセス中に作成されるオリジナルテンプレートを記憶するデータベースを必要とするので、データベースの配置に関する研究が行われなければならない。このデータベースは認証中の比較に必要である。プロトタイプでは、データベースは運転席隣のコンピュータに記憶された。現実には、事務処理部門、車内、スマートカードと、基本的に三つの異なる配置が考えられる。

10

【0360】

どの配置が最も優れているかはいくつかのパラメータに左右され、実例ごとに検討されなければならない。それでも、無認可の人間が車両を始動させるのを防止するのにシステムが使用される場合には、バイオメトリクス装置とデータベースとの間の通信が決して故障してはならないことは明らかである。さもないと、車両とデータベースとの通信問題のために認可ドライバがどこかで立ち往生することになってしまう。

事務処理部門の配置

【0361】

事務処理部門とは、例えば運送業者のオフィスのコンピュータにテンプレートデータベースが配置されることを意味する。

20

【0362】

認証システムはリアルタイム更新を必要とし、そのため車両とデータベースとの間のリンクが必要とされる。ドライバが病気で誰か他の人がその仕事を担当する場合には、新しいドライバを正規ドライバとして受け入れるようにシステムが更新されなければならない。前に言及したように、FBIのデータベースに入っている人間が危険物を運搬するトラックを運転することを米国政府は回避しようとしている。FBIのデータベースは変更されるため、認証システムのリアルタイム更新が望ましいだろう。

車内配置

【0363】

車内配置とは、テンプレートがトラック内のコンピュータに配置される場合である。これは無線通信によって生じる問題を抑制するが、代わりに盗難またはシステム侵入に対する保護は、事務所部門に配置する場合ほど強力でない。最も簡単な解決法ではあるが、各車両に1台のデータベースを必要とするのでおそらく最も高価であろう。

30

スマートカード配置

【0364】

スマートカード配置とは、テンプレートがスマートカードに記憶されて、ドライバが車から降りる時にこれを携帯できる場合を指す。システムをパスするためにスマートカードを持っていく必要があるため、これはセキュリティを高める。また、ドライバ自身が自分のバイオメトリクステンプレートを持つという事実は、プライバシーの印象を強める。

【0365】

データベースがカードと事務処理部門のいずれかに保管される場合の利点の一つは、特定車両に制約されないということである。エンジン故障などでドライバが車両を換える必要がある場合には、自分自身のスマートカードを携帯しておりデータベースに登録されている限り、すべてのドライバがすべての車両を運転できるので、問題にはならない。データベースのダイナミック更新が非常に重要であろう。

40

【0366】

2005年8月5日から、全EU内のすべての新車はデジタルタコグラフを装備しなければならない。現在のタコグラフは単純な紙製ディスクであって、データが操作されることは珍しくない。デジタルタコグラフは、速度や停車の間の運転時間などのデータを自動的に記録するスマートカードである。スマートカードは、記録されたデータをドライバが

50

操作することをはるかに複雑にし、長期的に見ると、デジタルタコグラフは全車両に標準装備されるものである。デジタルタコグラフは、テンプレートに使用できるバイオメトリクススマートカードへの統合の可能性を広げる。このようにして、ドライバは1枚のカードを必要とするだけだが、車両パラメータと認証のテンプレートの両方が一緒に記憶される。タコグラフからのデータがドライバに属する（ドライバが認証されていると仮定して）ことが保証されるので、これはセキュリティをさらに一層高める方法かもしれない。

【0367】

ドライバが自分のカードを紛失した場合には、詐称者が自分を登録してそのテンプレートをカードに保存する可能性が生じる。しかし、必要なのはどの方法が使用されるかを知っていることだけではないので、これは難しいだろう。テンプレートの構造が分かって、カードに組み込まれた符号化を通過できなければならない。カードに何かを記憶するには、この特定のカードのオペレーティングシステムについての知識も持たなければならない。オペレーティングシステムは、製造者により大きく異なっている。

システム管理

【0368】

データベース配置についての論考に関連するのは、システムをどのように管理するかについての考察である。一部の運送業者は多数の車両とドライバを抱えており、システムの管理が手に負えない場合には、認証システムを管理するためだけに追加要員を採用せざるを得ない。その意味で、データベースの車内配置は勧められない。これは、各ドライバが自分の運転すべき各車両に登録されなければならないか、彼のテンプレートがこれら車両のデータベースにダウンロードされなければならないかのいずれかだからである。

【0369】

テンプレートデータベースを事務処理部門に配置する場合には、一つの選択肢は、整合を行うため車内のメモリにテンプレートを一時的にダウンロードすることである。他の選択肢は、認証中に走査されたテンプレートを整合のために事務処理部門に送ることである。受け入れが不十分な地域に車両が進入する危険、または無線接続が故障する可能性のため、これは勧められない。テンプレートから実際の特徴を再現するのは不可能なはずであると言われたとしても、自分のバイオメトリクステンプレートが送られることを知るのはユーザにとって不快かもしれない。

【0370】

テンプレートがカード、例えばデジタルタコグラフカードに記憶される場合には、これらの問題は発生しない。代わりに、ドライバが自分のカードを紛失するリスクがある。しかし、タコグラフカードを挿入せずに車両を運転することは禁止されるため、おそらくドライバはカードの取り扱いに注意するだろう。

テレマティックス

【0371】

システムが事務処理部門と通信できるようにするために、テレマティックスが必要である。現在のトラックの大部分は、何らかの種類の通信システムを装備している。それは、基本的なアナログ無線通信から先進のシステムまでいろいろである。ここで中心となるのは認証システムそのものであるもので、トラックとオフィスとの間でデータを伝達するのが可能であると単純に仮定する。

【0372】

氏名、雇用ID、様々な認証結果についての情報が事務処理部門に送られることが推奨される。接続不良のリスクのため、ドライバについてのテンプレートも多量の情報（例えば公共セキュリティ番号）も送られるべきでないと考えられる。

【0373】

接続故障のリスクのために他に推奨されるのは、情報が悪人の手に渡るリスクを下げるために情報を符号化された状態で送信することである。データ符号化のための製品は市場に多数見られる。大部分のシステムでは、符号化キーにしたがってデータを処理する。それからデータは、同一の符号化キーを有して情報を復号する受信者へ送られる。

情報配信

【0374】

データをどこへ、誰に送信するべきか。トラック所有者は情報を所有するが、これに関わろうとする他の関係者もいる。このような関係者は、例えば保険会社、国内道路協会、警察、消防署である。情報の更新、保管、配信に責任を負うべき者について検討しなければならない。

重要な自動車技術面

【0375】

自動車技術の観点から発生する可能性のある複雑なシナリオがいくつかある。例えば、
- 車両がレンタルで 사용되는場合には、システムに人を登録することは削除するのと同様に容易でなければならない。利点は、受付で登録された人のみによって車両が運転されていることをレンタル会社が確信できることである。

10

- 車両が誰かにレンタルされる場合には、簡単な迂回手段または登録／削除手順が必要である。

- 車両が修理工場での点検を必要とする場合には、修理工場の整備士を登録する代わりにシステムを迂回する簡単な方法がなければならない。可能な解決法は、タコグラフカードまたは他の認証なしで例えば5 km/hでトラックを移動できるようにすることである。

- ドライバが怪我その他で車両を運転できない場合、緊急時に動かす方法がなければならない。解決法は前の弾丸の地点で提示したようなものである。

- 認証システムを必要としない誰かに車両が販売される場合、これを取り外すことが可能でなければならない。

20

- 製造または輸送中の車両の取り扱いも検討すべき問題である。これは、修理工場での点検時と同じような方法で解決できる。

【0376】

システムを市場に出す前に、これらの面は十分に検討されなければならない。またエンジン始動のためイグニッションキーの代わりにバイオメトリクス方法が使用される場合にも、電源、エンジン始動、ステアリングロックを扱う方法を考慮しなければならない。

方法の反省

【0377】

第1回ドライバアンケートでは、トラック停車場で用紙が配布された。自分の仕事とドライバ認証システムの可能性についていくつかの質問に回答できるかどうかをドライバは尋ねられた。システムに強く反対しているか非常に肯定的である人のみが回答を希望し、残りは質問に回答する時間を取るのに十分なほどの関心を持っていないというリスクがある。

30

【0378】

イェーテボリの運送業者で配布された用紙にも同じことが言える。配布された用紙の半分のみが回収され、どんな人が回答する／しないを選び、それはなぜかという疑問が生じた。これらの資料は、オフィスに従業員への説明書とともに置かれた。何か質問がある場合、ドライバには詳しい情報／説明を尋ねる人がいなかった。

【0379】

40

方法と機器の両方の選択は、時間とともに資金の欠乏によって制限され、そのため使用された機器が入手可能な最高のシステムであるかどうかは確かではなかった。さらに、比較的経験のないプログラマによってソフトウェアが実行され、これはシステムの性能に影響を与えた。

【0380】

上述したようにシミュレータはシナリオに完全には適しておらず、時間が足りなかったため、調整をすることが可能ではなかった。参加者の何人かはシミュレータの性能についてコメントした。これが認証システムについての判断に影響を与えたかもしれない。シミュレータがもっと確実なものであったならば、おそらく検査の結果はもっと正確であっただろう。

50

【0381】

約30分間に6回の認証と、シナリオはかなり集中的であった。もっと長い検査を行う方がよかっただろうが、時間の制約のためそれは可能でなかった。

【0382】

検査へ参加することを選んだドライバは新しい技術に特に関心があり、そのため平均的なトラックドライバよりも肯定的であるということが考えられる。登録段階ですべての参加者が正確に同じ情報を与えられたわけではなく、これが彼らの態度に影響したことも考えられる。

【0383】

登録中、参加者は顔認識カメラでの明瞭な撮影のためハンドルを下げるように求められた。検査中、何人かは運転時にハンドルを再び上げた。その時に検査を中止することは可能でなかった。これは顔認証システムの性能に影響したかもしれない。

【0384】

本出願で使用された多くの単語と略語は読者には知られていないかもしれないため、頻繁に登場したものを挙げておく。

人体測定学：（人類学的）分類と比較に使用するための人体測定の研究。

自動車技術：自動車産業に関連する技術の総称。

バイオメトリクス：対象者に固有の身体特徴の分析を使用する方法の総称。

誘電体：誘電体は様々な性質を持つ絶縁材料である。

E C G：心電図の短縮形。心臓の電気信号の測定。

F A R：誤認証率の短縮形。システムがどの程度の頻度で詐称者を認可ユーザと見なすかを示す。F A RとF R R（以下参照）は関連性が高い。高いF A Rは低いF R Rを意味し、その逆も成り立つ。

科学捜査：犯罪と裁判についての研究に関連する事柄に使用される総称。

F R R：本人拒否率の短縮形。システムがどの程度の頻度で認可ユーザを拒否するかを示す。F R RとF A R（上記）は関連性が高い。高いF R Rは低いF A Rを意味し、その逆も成り立つ。

I R：赤外線短縮形。可視赤色光線よりも波長の長い光線であるため人の眼には見えない。

詳細：指紋の特徴で、例えば凸部が終わるか二つに分かれる場合。

モックアップ：シミュレーションおよび検査の目的で実験室に置かれる車両の一部、一般的にはドライバ環境。

N I R：近赤外線短縮形。

酸素測定法：パルス酸素測定法は、酸素が飽和したヘモグロビン（Hb）の百分率を監視する簡単で非侵害的な方法。

透過率：電界に置かれた時に媒体が変化してどれほどのエネルギーを吸収するかについての測定。

P I N：個人識別番号の短縮形。

凸部：指紋の顕著な線。

スマートカード：クレジットカードのサイズまたはさらに小型のカードに組み込まれた小さくて安全な暗号プロセッサ。一例は、G S M携帯電話用のS I Mカードである。

T E R：総合誤差率の短縮形であり、F A RとF R Rの合計。

サーモグラフィ：I Rカメラを使用した熱の差の測定。

凹部：指紋の凸部の間のくぼみ。

S W O T（新製品の強み・弱み・販売機会・脅威）分析表

図20 - 認証方法としての指紋

図21 - 認証方法としての虹彩走査

図22 - 認証方法としての音声認証

図23 - 認証方法としての顔認識

図24 - 認証方法としての顔面サーモグラフィ

10

20

30

40

50

図 2 5 - 認証方法としての網膜走査

図 2 6 - 認証方法としての唇動走査

図 2 7 - 認証方法としての掌形認識

図 2 8 - 認証方法としてのパスワードおよび P I N 走査

図 2 9 - 認証方法としてのカード

図 3 0 - 認証方法としての R F I D

図 3 1 - v a n d e r L a a n s 受容尺度による統計

すべてのバイオメトリクス方法を使用するマルチモード認証

使用例：最高セキュリティレベルでのマルチモード認証（すべてのバイオメトリクス方法）

10

参考：

目的：ドライバが正規ドライバであることを確かめるために認証が行われる。車両は最高セキュリティレベルに分類されているため、ドライバは、利用可能なバイオメトリクス認証方法をすべて使用する。

関係するもの：認証システム、ドライバ、事務処理部門

前提条件：車両がロックされているか、最近ロック解除された。

できごとの主な流れ

【 0 3 8 5 】

ドライバが車両に乗り込みキーを回すと、彼が正規ドライバであることを確かめるためいくつかの方法を使用してシステムが認証を要求する。ドライバは方法の一つで自己を認証することによって開始し、認証が完了するまで次へ次へと続ける。ドライバが認証されると情報が事務処理部門に送信されて符号化され、ドライバは車両を発進できる。

20

できごとの別の流れ

【 0 3 8 6 】

ドライバが車両に乗り込みキーを回すと、彼が正規ドライバであることを確かめるためいくつかの方法を使用してシステムが認証を要求する。ドライバは認証方法のうち一つ以上に成功しない。一つの方法で 3 回失敗した後、他の方法で認証が続く（または失敗したのが最後の方法でなければ終了する）。方法の少なくとも一つが成功すると、情報は事務処理部門へ送信されて符号化され、ドライバは車両を発進できる。ドライバについての認証情報とともに、事務処理部門は認証失敗についての情報も受け取る。

30

できごとの別の流れ

【 0 3 8 7 】

ドライバが車両に乗り込みキーを回すと、彼が正規ドライバであることを確かめるためシステムがいくつかの方法を使用する認証を要求する。ドライバは第 1 認証方法に成功せず、3 回の失敗の後、次の方法でシステムが続行する。どの方法も成功しないと、即座に警告が事務処理部門に送信される。

特殊な要件

【 0 3 8 8 】

人がドアをロック解除した時に、システムは情報を受け取るべきである。車両と事務処理部門との間で情報を送信できるようにするため、システムはテレマティックスを必要とする。

40

例 1

【 0 3 8 9 】

ドライバは車庫に着いて一日の仕事を開始する。車両に乗り込むとスマートカード（タコグラフのカードと一体化）をリーダに挿入し、P I N コードをダイヤルしてから、指をスキャナに載せる。P I N が正しく、カードと照らし合わせて指が認証されるため、システムは音声サンプルを要求する。ドライバはマイクロフォンに向かってパスワードを言う。顔認証を実施するため、通常運転位置に座るようにドライバに指示するシステムメッセージが現れる。記録されたデータは分析され、スマートカードに記憶されたテンプレートデータと比較される。認証が成功した。氏名と雇用識別番号が事務処理部門に送信され符

50

号化される。

例 2

【0390】

ドライバは車庫に着いて一日の仕事を開始する。車両に乗り込むとスマートカード（タコグラフのカードと一体化）をリーダーに挿入し、PINコードをダイヤルしてから、指をスキャナに載せる。声によりIDを認証しようとするが、今日は風邪をひいているため失敗する。認証失敗についての合図がドライバに伝えられる。顔認証に成功して手順は続行する。氏名と雇用識別番号が、音声認証の失敗とともに事務処理部門に送信されて符号化される。

例 3

【0391】

長距離走行においてドライバは運転席で昼寝をする。眼を覚ますと、運転を続ける前に外へ出て脚を伸ばす。乗員がドアを開け、詐称者が乗り込んで運転席を奪う。詐称者は車両を始動させようとするが、認証に成功せず、車両は作動停止となる。即座に警告が事務処理部門に送られ、システムはハンドルの前に座っている人間の写真を撮る。この写真も事務処理部門へ送られる。

二つのバイオメトリクス方法を使用するマルチモード認証

使用例：中間セキュリティレベルでのマルチモード認証（二つのバイオメトリクス特徴）
参考：

目的：ドライバが正規ドライバであることを確かめるために認証が行われる。車両の分類つまり中間セキュリティレベルに対応するため、ドライバは二つのバイオメトリクス特徴を使用して自分のIDを認証する。

関係するもの：認証システム、ドライバ、事務処理部門

前提条件：車両がロックされているか、最近ロック解除された。

できごとの主な流れ

【0392】

ドライバが車両に乗り込みキーを回すと、彼が正規ドライバであるかを確かめるためシステムはいくつかの方法を使用する認証を要求する。ドライバは方法の一つにより自己を認証することで開始し、認証が完了するまで次へ次へと続ける。ドライバが認証されると、情報が事務処理部門へ送信されて符号化され、ドライバは車両を発進できる。

できごとの別の流れ

【0393】

ドライバが車両に乗り込みキーを回すと、彼が正規ドライバであるかを確かめるためシステムはいくつかの方法を使用する認証を要求する。ドライバは一つ以上の認証方法に成功しない。一つの方法で3回失敗した後、他の方法で認証が続けられる（または失敗したのが最後の方法でなければ終了する）。少なくとも一つの方法に成功し、情報は事務処理部門へ送信されて符号化され、ドライバは車両を発進できる。ドライバについての認証情報とともに、事務処理部門は認証失敗についての情報も受け取る。

できごとの別の流れ

【0394】

ドライバが車両に乗り込みキーを回すと、彼が正規ドライバであるかを確かめるためシステムはいくつかの方法を使用する認証を要求する。ドライバは第1認証方法に成功せず、3回の失敗の後、システムは次の方法で続ける。どの方法も成功せず、即座に事務処理部門へ警告が送られる。

特殊な要件

【0395】

人がドアをロック解除した時にシステムは情報を受け取るべきである。車両と事務処理部門との間で情報を送信できるようにするため、システムはテレマティックスを必要とする。

例 1

10

20

30

40

50

【0396】

ドライバは車庫に着いて一日の仕事を開始する。車両に乗り込むとスマートカード（タコグラフのカードと一体化）をリーダに挿入し、PINコードをダイヤルしてから、指をスキャナに載せる。PINが正しく、カードと照らし合わせて指が認証される。システムは音声サンプルを要求し、ドライバはマイクロフォンに向かってパスワードを言う。記録されたデータは分析され、スマートカードに記憶されたテンプレートデータと比較される。認証が成功した。氏名と雇用識別番号が事務処理部門に送信され符号化される。

例 2

【0397】

ドライバは車庫に着いて一日の仕事を開始する。車両に乗り込むとスマートカード（タコグラフのカードと一体化）をリーダに挿入し、PINコードをダイヤルしてから、指をスキャナに載せる。PINは正しく、カードと照らし合わせて指が認証される。顔認証を実施するため、通常の運転位置に座るようにドライバに指示するシステムメッセージが現れる。記録されたデータが分析され、スマートカードに記憶されたテンプレートデータと比較される。認証が成功した。氏名と雇用識別番号が事務処理部門に送信され符号化される。

10

例 3

【0398】

ドライバは車庫に着いて一日の仕事を開始する。車両に乗り込むとスマートカード（タコグラフのカードと一体化）をリーダに挿入し、PINコードをダイヤルしてから、指をスキャナに載せる。声によりIDを認証しようとするが、今日は風邪をひいているため失敗する。氏名と雇用識別番号が、音声認証の失敗についての情報とともに事務処理部門に送信されて符号化される。

20

例 4

【0399】

ドライバは車庫に着いて一日の仕事を開始する。車両に乗り込むとスマートカード（タコグラフのカードと一体化）をリーダに挿入し、PINコードをダイヤルしてから、指をスキャナに載せる。ドライバの顔の写真が撮られるが、休暇中にひげを伸ばしていたため認証は失敗する。氏名と雇用識別番号が、顔認証失敗についての情報とともに事務処理部門へ送られて符号化される。

30

【0400】

今回開示される発明の実施例について上述した。特許保護を求めるこれらの特徴は、上記の請求項に記載される。

【図面の簡単な説明】

【0401】

【図1】最も一般的な認証方法においてユーザを登録／整合する段階。

【図2】不規則で断続的な線の特徴とするパターンを形成する凸部と凹部とを持つ指紋。

【図3】分析のためのいくつかのタイプの明確な指紋の特徴、例えばループ、円弧、渦巻

。

【図4】指を走査するための容量性スキャナ。

40

【図5】実際の指先端表面の下模様を走査するためのRF方法。

【図6】虹彩スキャナ。

【図7】走査された網膜。

【図8】顔認識のための顔面サーモグラフィ。赤外線カメラを用いた、各個人に固有の人の顔面血管パターンに基づく熱パターン。

【図9】網膜認識のための網膜写真。

【図10】網膜の撮像。

【図11】掌形スキャナは指の長さ、幅、厚さ、湾曲を測定する。

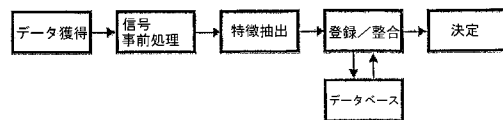
【図12】実装された認証システムの概要。矢印は異なる部分がどのように相互に通信するかを示す。

50

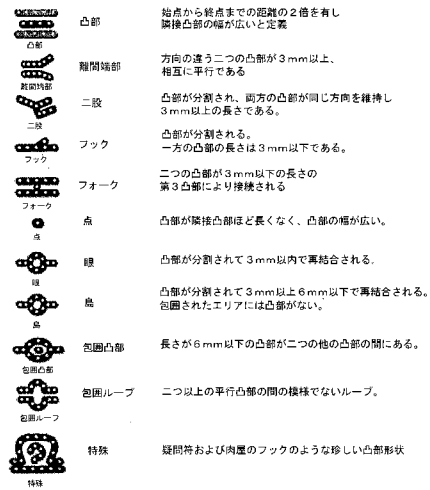
- 【図 1 3】トラック運転席に搭載されるシステムの一部の写真。
- 【図 1 4】グラフィカルユーザインタフェースの二つの例。
- 【図 1 5】シミュレータの写真。
- 【図 1 6】シミュレータの写真。
- 【図 1 7】運転中の指紋または音声および別の認証を用いた初回完全認証とコーヒープレイク、その後の短縮認証とを含む検査シナリオ。
- 【図 1 8】実用性と満足度に関する各参加者平均点の図。
- 【図 1 9】検査前後の参加者回答を表す図。
- 【図 2 0】認証方法としての指紋に関する表。
- 【図 2 1】認証方法としての虹彩走査に関する表。 10
- 【図 2 2】認証方法としての音声認証に関する表。
- 【図 2 3】認証方法としての顔認識に関する表。
- 【図 2 4】認証方法としての顔面サーモグラフィに関する表。
- 【図 2 5】認証方法としての網膜走査に関する表。
- 【図 2 6】認証方法としての唇動走査に関する表。
- 【図 2 7】認証方法としての掌形認識に関する表。
- 【図 2 8】認証方法としてのパスワードおよび P I N 走査に関する表。
- 【図 2 9】認証方法としてのカードに関する表。
- 【図 3 0】認証方法としての R F I D に関する表。
- 【図 3 1】 v a n d e r L a a n s 受容尺度による統計に関する表。 20

【図 1】

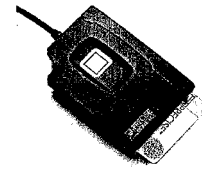
【図 2】



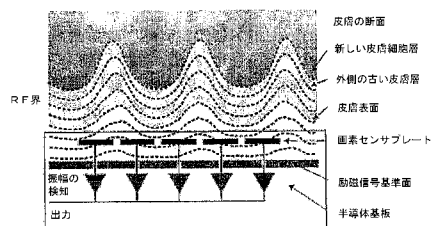
【図 3】



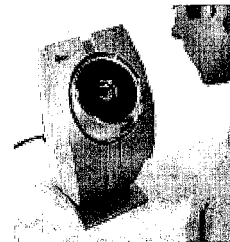
【図 4】



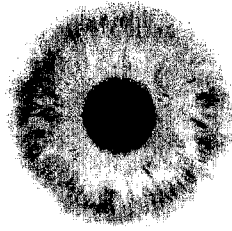
【図 5】



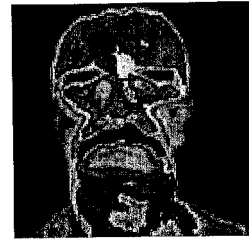
【図 6】



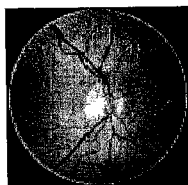
【図 7】



【図 8】



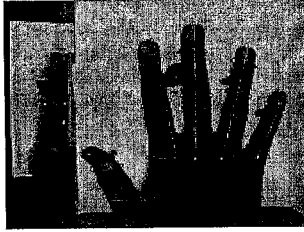
【図 9】



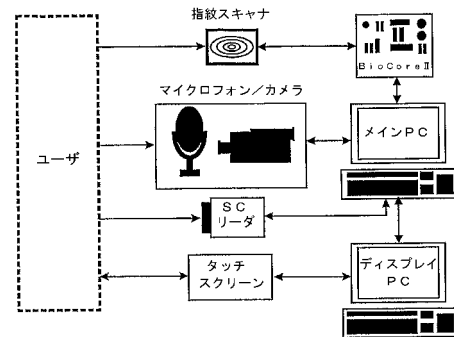
【図 10】



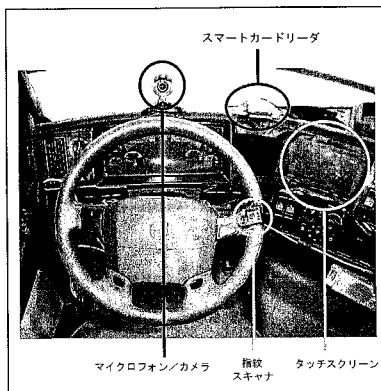
【図 1 1】



【図 1 2】



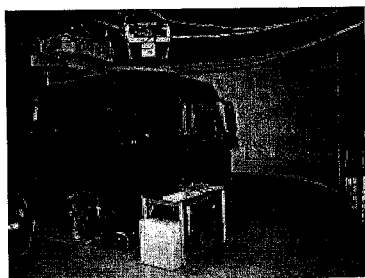
【図 1 3】



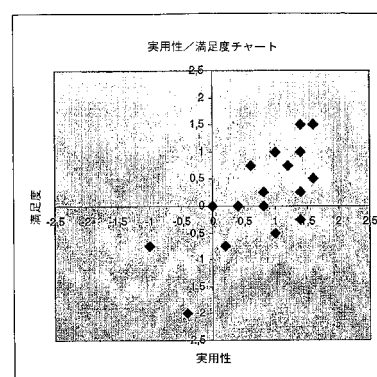
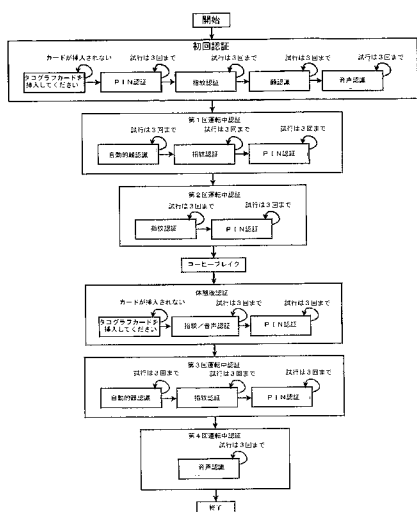
【図 1 4】



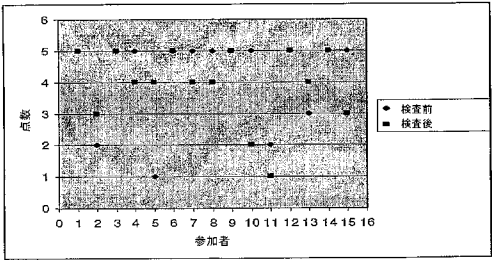
【図 16】



【図 18】



【図 19】



【図 20】

強み	弱み	販売の機会	脅威
安価である	誰もがこの方法を 使用できるわけではない	運転中に使用できる	汚れなどでセンサが 故障する
充分に検査されている	モールドによって だまることができる	小型の機器でドライバ 乗換への統合が容易	犯人特定と関連付けられる 方法なので使用を拒む人も ある
使いやすい	手の汚れまたは湿度により 問題が生じるかもしれない	複数のテンプレートを保存 することで認証のための 指が圧着されるかき システムがランダムに指示 できる	ドライバが人混み離れたところ にいて手を洗われるなどで 指紋が損傷した場合
高速である		多様な会社が機器を製造 しているのいくつかの モデルが入手可能である	

【図 21】

強み	弱み	販売の機会	脅威
非常に正確である	高価である	バックミラーへの 一体化が可能である	危険だと感じている 場合には車の分析を 嫌がるかもしれない
短時間である	一企業の technology が すべての特許を所有している。 他の製造者はすべて 同社からライセンスを 取得しなければならない	運転中の使用が 可能かもしれない	製造者がなんらかの 理由で製造を中断した
虹彩は時間とともに 変化しない			照明条件のため 車内での使用は不可能
だましにくい			

【図 22】

強み	弱み	販売の機会	脅威
話話に聞ければ (長いフレーズの発話を 必要としなければ) 短時間である	音声は時間とともに 変化する	携帯電話ハンズフリー または他の音声制御機器 への統合が可能である	健康および精神的条件 によりドライバの声は 変化する
安価である	この技術を採用しない 人もいる	望ましい発話フレーズを システムがランダムに 選択できる	運転席内の騒音環境 では問題がある
使いやすい		他の認証方法の要求を 不要にする一つの独自の パスワードをドライバが 持つことが可能である	
非侵襲的である		運転中に使用できる	
例えば盗難のために 発話フレーズを変更できる			

【図 2 3】

強み	弱み	販売の機会	脅威
非侵襲的である	熱、めがね、化粧などで問題が発生する	バックミラーにカメラを一体化できる	運転席内の照明条件が良好な写眞の撮影を不可能にする
安価である	人の顔は時間とともに変化する	運転中の使用が可能かもしれない	何らかの理由でドライバの顔が隠れるか顔を覆うことがある
使いやすい			

【図 2 4】

強み	弱み	販売の機会	脅威
短時間である	高価である	カメラをバックミラーに一体化できる	新しい方法であり、どの程度の研究と開発が行われるかが確かでない
照明条件に無関係である	熱いときや眩しいときなどがあるかもしれない	運転中に使用できる	
だましにくい			
非侵襲的である			

【図 2 5】

強み	弱み	販売の機会	脅威
非常に正確である	運転中に使用できない	レーザを使用し、運転席の照明条件に左右されないことを意味する	レーザ照射を信賴していないのでこの方法の使用を拒む人がいるかもしれない
だましにくい	取のほほ完全な場合が必要		
網膜撮影パターンは時間とともにそれほど変化しない	高価である		
短時間である			

【図 2 6】

強み	弱み	販売の機会	脅威
非侵襲的である	他の認証手段とともに使用されなければならない	運転中に使用できる	この方法の研製と開発がどの程度行われているかが確かでない
短時間である	ある状況でのみ検出される	バックミラーにカメラを一体化できる	何らかの理由でドライバの顔の周辺を隠蔽するかもしれない
使いやすい	鏡像を製造する会社があつたとしてもどれほど多くかは確かでない	例えば顔または音声認証とともに使用される	

【図 27】

強み	弱み	販売の機会	脅威
短時間である	見た目の悪い機器である	運転中に使用できる	機器の製造者は一社のみである
「おそろく」手が汚くても機能する	手は独自ではないため他の認証手段が必要である		
非侵襲的である			
使いやすい			
安価である			

【図 28】

強み	弱み	販売の機会	脅威
短時間である	誰かがパスワードまたは PIN を見つけた場合には、その使用を止める方法がない	必要な機器の大部分はすでに現在の車両に存在する	パスワードまたは PIN は忘れられることがある
記憶力がよければ使いやすい	他の方法とともに使用されると最も良好に機能する	運転中の使用が困難でない	パスワードまたは PIN が盗取にばれて使用されることがある
方法の統合／使用のコストは高くない			

【図 29】

強み	弱み	販売の機会	脅威
大勢分の人々が前使用したことのある周知の方法なので使いやすい	カードが盗竊または偽造されることがある	必要な機器はすべて現在の車両に備わっている	カードは紛失するか家に忘れてきやすい
短時間である	他人からの盗う人間によってカードを使用できる	カードにバイオメトリクスデータを追加して他人のカードの使用を困難にすることによりセキュリティが高まる	カードが盗竊されるかもしれない
非侵襲的である	他の方法とともに使用されると最も良好に機能する		例えば何らかのバイオメトリクス方法よりもましに使いやすい
安価である			

【図 30】

強み	弱み	販売の機会	脅威
未知に短時間である	RFID タグは他人からの盗う人間によって使用できる	機器はスペースをあまり必要とせず車両への統合が困難ではない	RFID タグは紛失するがまたは家に忘れてきやすい
照像条件に左右されない	他の方法とともに使用されると最も良好に機能する	運転中に使用できる	RFID タグは盗竊されることがある
非侵襲的である			
使いやすい			

【図 3 1】

記述統計

	N	最低	最高	平均	標準偏差
役に立つ／役に立たない	18	,00	2,00	1,2778	,82844
快適である／不快である	18	-2,00	2,00	,4444	,98952
悪い／良い	18	-1,00	2,00	,8333	1,09819
いい感じである／怪な感じである	18	-2,00	2,00	,3333	1,32842
効果的である／余分である	18	-2,00	2,00	1,0000	1,13769
いらいらする／好ましい	18	-2,00	2,00	-,0556	1,21133
助けになる／無益である	18	-2,00	2,00	,7222	1,22741
望ましくない／望ましい	18	-2,00	2,00	,2222	1,35280
警戒心を覚める／電気を誘う	18	,00	1,00	,1667	,38346
実用性	18	-1,00	1,80	,6000	,72274
満足度	18	-2,00	1,60	,2391	,86895
有効N (リストに関して)	18				

フロントページの続き

(51)Int.Cl.			F I		
G 0 9 C	1/00	(2006.01)	G 0 9 C	1/00	6 4 0 E
H 0 4 L	9/32	(2006.01)	H 0 4 L	9/00	6 7 3 D
A 6 1 B	5/117	(2006.01)	A 6 1 B	5/10	3 2 0 Z

(72)発明者 ラルッソン, ペッテル
スウェーデン国 エスイー-4 4 2 5 4 イッテルビイ スヴェルドガタン 3

(72)発明者 ハゲルマン, アンドレアス
スウェーデン国 エス-5 8 2 3 7 リンコピング オルンガタン 1 1

(72)発明者 ビョーク, ハンナ
スウェーデン国 エス-3 7 1 4 3 カルスクロナ ボクヴェーゲン 2

審査官 関 裕治朗

(56)参考文献 特開2 0 0 3-1 3 8 6 0 8 (J P, A)
特開2 0 0 3-1 7 8 0 3 2 (J P, A)

(58)調査した分野(Int.Cl., D B名)

B60R 25/00
B60R 25/10
G06F 21/20
G06T 7/00
G08B 13/00
A61B 5/117
G09C 1/00
H04L 9/32