(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2010-536055
(P2010-536055A)
(43)公表日　平成22年11月25日(2010.11.25)

(51)Int.Cl.		F I			テーマコード（参考）
G09C 5/00	(2006.01)	G09C	5/00		5J104
H04L 9/32	(2006.01)	H04L	9/00	675B	
G06Q 50/00	(2006.01)	G06F	17/60	140	

審査請求 未請求　予備審査請求 未請求　（全 18 頁）

(21)出願番号　特願2010-519315 (P2010-519315)
(86)(22)出願日　平成20年8月7日 (2008.8.7)
(85)翻訳文提出日　平成22年4月5日 (2010.4.5)
(86)国際出願番号　PCT/CA2008/001434
(87)国際公開番号　WO2009/018663
(87)国際公開日　平成21年2月12日 (2009.2.12)
(31)優先権主張番号　60/935,347
(32)優先日　平成19年8月8日 (2007.8.8)
(33)優先権主張国　米国 (US)

(71)出願人　510033446
メモリー　エキスパーツ　インターナショナル　インコーポレイテッド
MEMORY EXPERTS INTERNATIONAL INC.
カナダ国　エッチ４アール　２エヌ７　ケベック州　モントリオール　コヘン　ストリート　２３２１
２３２１ Cohen Street, Montreal, Quebec H4R 2N7 Canada
(74)代理人　100075199
弁理士　土橋　皓

最終頁に続く

(54)【発明の名称】透かし入り文書表示証明による確実な取引提供法

(57)【要約】
デジタル証明および承諾の先行技術の方法を採用する電子的取引は詐欺的な取引に帰着する攻撃および身元情報の悪用を被る。使用者と電子署名を求める機構との間の安全で信頼性ある経路を構築することによって電子的セキュリティを増進させて、署名や電子取引行為の完了の要求が生ずる前の取引を証明する方法が開示されている。前記安全で信頼性ある経路は、前記ユーザに、悪意あるソフトウェアによって傍受されまたは操作されることがない個人専用化装置上で、署名に対する前記機構からの要求の所定部分をユーザに提供することで、ユーザの主要なコンピュータ装置上に表示されるような要求が有効であることを証明する。

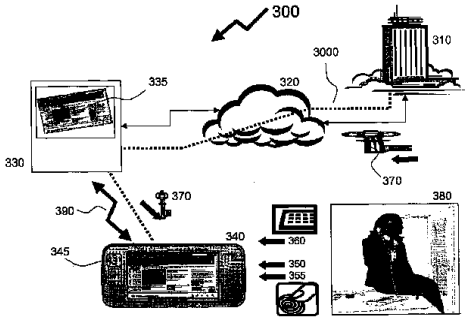


Fig. 3

【特許請求の範囲】
【請求項１】
複数の透かしを格納する記憶装置と、
取引データを受信するため、複数の透かしから第１の透かしを選択するため、証明用の第１のデータを有しかつ前記取引に関係する第１の証明データおよび前記第１のデータの改ざんを防止する前記第１の透かしに関係する第１の透かしデータを生成するため、かつ、前記選択された透かしの表示を有する第２の証明データを提供するために適切にプログラムされたプロセッサと、前記第１の証明データを目的地のシステムに送信しかつ前記第２の証明データを第２の他の目的地のシステムに送信するための少なくとも１の送信機とを有するコンピュータ・サーバ。
【請求項２】
周辺記憶装置と接続し、該周辺記憶装置内に複数の透かしの内の少なくともいくつかの記述を格納するための第１のインタフェースを有し、前記記述は、表示と共に格納され、各記述は異なる表示に応答して引き出される請求項１に記載のコンピュータ・サーバ。
【請求項３】
複数の既知の透かしからなる透かしに対する表示をそこに格納するメモリと、第２の証明データを受け取るためおよびそれに基づいて透かしの表示を決定するためのプロセッサと、前記安全処理システムのユーザへの前記表示を表示するためのディスプレイとを有する安全処理システム。
【請求項４】
デジタル的に文書に署名するためのデジタル署名プロセッサを有する請求項３に記載の安全処理システム。
【請求項５】
前記文書のデジタル署名を起動するアクチュエータを有する請求項４に記載の安全処理システム。
【請求項６】
データを送信しかつ受信する無線トランシーバを有する請求項１乃至請求項５のいずれかに記載の安全処理システム。
【請求項７】
前記トランシーバは、少なくとも他のシステムとの安全な通信を構築しかつ維持するための安全通信処理回路を有する請求項６に記載の安全処理システム。
【請求項８】
コンピュータと結合するためのコンピュータ・インタフェースを有し、前記メモリが、周辺記憶装置としても用いられる請求項３乃至請求項７のいずれかに記載の安全処理システム。
【請求項９】
第１のシステムとサーバとの間の第１の通信経路を構築し、
既知のユーザのための取引に関係するデータを第１のシステムから受信し、
前記第１のシステムに、前記取引を証明しかつ承諾する第１の証明データを提供し、
第２の他のシステムと前記サーバとの間の第２の通信経路を構築し、かつ、
前記第２の他のシステムに、前記透かしの表示の提供に使用するための第２の証明データを提供する各工程を有し、
前記第１の証明データは透かしを有し、前記第２のシステムは、既知のユーザと結びついた方法。
【請求項１０】
前記取引を承諾するためのデジタル的に署名された取引証明データを前記サーバで受信する工程を有する請求項９に記載の方法。
【請求項１１】
前記第２の通信経路は、安全な通信経路を有する請求項９及び請求項１０のいずれに記載の方法。

【請求項１２】
前記第１の通信経路は、安全な通信経路を有する請求項９乃至請求項１１のいずれかに記載の方法。
【請求項１３】
前記第２の証明データは、複数の所定の透かしから選択された透かしを表示するインデックスを有する請求項９乃至請求項１２のいずれかに記載の方法。
【請求項１４】
前記第２の証明データ及び以前に格納されたデータに基づいて前記表示を決定し、前記第２のシステムの前記ユーザ前記表示を提供する工程を有し、前記以前に格納されたデータは、前記第２のシステム内に格納された請求項１３に記載の方法。
【請求項１５】
前記透かしは画像データを有する請求項９乃至請求項１４のいずれかに記載の方法。
【請求項１６】
前記第２の証明データは、前記透かしの証明への使用のための画像データを有する請求項９乃至請求項１５のいずれかに記載の方法。
【請求項１７】
前記透かしは音響データを有する請求項９乃至請求項１６のいずれかに記載の方法。
【請求項１８】
前記第２の証明データは前記透かしの証明への使用のための音響データを有する請求項９乃至請求項１７のいずれかに記載の方法。
【請求項１９】
デジタル証明書、セキュア・ソケット・レイヤー証明書、およびITU-TX.509による証明書の少なくとも１つを有する承諾データを受け取る工程を有する請求項９乃至請求項１８のいずれかに記載の方法。
【請求項２０】
前記第２の他のシステムの前記ユーザに、前記第２の証明データに基づく前記透かしの表示を提供し、かつ、前記ユーザから前記取引のための承諾を受ける工程を有する請求項９乃至請求項１９のいずれかに記載の方法。
【請求項２１】
前記第１の証明データは、時間署名を有し、該時間署名は、遅れ検出に使用され、該遅れは潜在的に改ざんの表示である請求項９乃至請求項２０のいずれかに記載の方法。
【請求項２２】
前記第２のシステムは、無線装置、個人用電子装置および周辺記憶装置の内の少なくとも１を有する請求項９乃至請求項２１のいずれかに記載の方法。
【請求項２３】
前記第２の証明データは、前記第２のシステムの前記ユーザにより、前記透かしの内容を決定の使用のためのデータを有する請求項９乃至請求項２２のいずれかに記載の方法。
【請求項２４】
前記第２の証明データは、分野の表題を有し、該分野の内容は、それが前記ユーザに属するように、前記透かしを表示する請求項２３に記載の方法。
【請求項２５】
実行の際に、第１のシステムとサーバとの間の第１の通信経路を構築し、既知のユーザに対する取引に関係するデータを前記第１のシステムから受信し、
前記取引を証明しかつ承諾するための第１の証明データであって透かしを有するものを前記第１のシステムに提供し、
第２の他のシステムであって前記既知のユーザと結びつくものと前記サーバとの間に第２の通信経路を構築し、
前記第２の他のシステムに前記透かしの表示の提供に使用するための第２の証明データを提供することに帰着する所定のコンピュータ装置のフォーマットに応じたデータがそこに格納されたコンピュータにより読み取り可能な媒体。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、確実な取引の提供に係り、特に通信者間の信頼性ある通信経路の構築と表示された透かしの証明に関する。
【背景技術】
【０００２】
近年、電子商取引（e-commerce）が大きな注目を集めているのは、インターネット販売が25パーセント以上の率で成長したからである。それにも拘らず、２００６年には、米国内での旅行購入を除く全オンライン販売は、米国の小売販売の約6%を示したにすぎなかった。２００７年には、旅行購入を含めたこの数字は、18パーセント増加して、約2600億米ドルに達すると期待されていた。
【０００３】
電子商取引およびその成長を阻害するものは、電子商取引が多くのプライバシーおよびセキュリティ上の問題をもっているという一般の見方であり、その問題の中心となる態様は、電子伝送の送り手が事実そうであると主張する者であることを保証する信頼性のある方法がないということである。前記インターネットの非物理的性質が不信に導いている。なぜなら、消費者は生きている人間と交流せず、前記消費者は現実の製品を見ず、かつ最も重大なことには、前記ユーザはこの見もせず知りもしない売主に支払いの情報を提供するからである。
【０００４】
対面商取引では、顧客と商人は、身元確認、立証および承諾を提供する。身元確認は、顧客または売主、例えば、看板によって店の確認を可能にする処理であり、立証は、個人が主張した身元を証明する行為であって、例えば、身分証明書の第2の部分を見せることによって行い、承諾は取引が完了する最後の過程であって、例えば、クレジットカードを提供しクレジットカード伝票に署名することによって行う。さらに、顧客は売主の前に立っているので、プライバシーを確認し、身元詐称等を防止することは一般に簡単である。
【０００５】
インターネットを通しての身元確認、立証、および承諾の提供を使用するためのいくつかの解決方法は、暗号作成法の応用に大きく集中している。暗号作成法を用いることは、２つの端点の間の安全な接続を可能にして通信が傍受されずかつ改ざんされていないことを保証する。商取引の他の面は実質的に同じままである。すなわち、製品またはサービスが選択され、請求書が製品またはサービスに対して作成され、支払い方法が提供され承諾が受け付けられる。一旦完了すると、時には、取引が別の通信経路、例えば、電子メールによって確認される。
【０００６】
より技術的なセキュリティ攻撃は、「介入者」（man-in-the-middle）セキュリティ攻撃である。そのような攻撃では、あるシステムが通信経路の各末端からのメッセージを傍受し、該通信の中間に前記システムを置いていることになる。前記システムは、前記経路の各末端が前記中間の前記通信経路へアクセスできる安全な通信経路を設定している。そうであるので、介入者はデータを傍受し、記録しまたは変更することができる。最も問題なのは、介入者は一般にソフトウェア処理であり、したがって、ユーザ自身のシステム上で実行することができるであろうことである。
【０００７】
介入者セキュリティ攻撃が採用されると、メッセージの完全性の証明が、改ざんが生じていないことを保証するために重要である。メッセージの完全性の点検は一般には、メッセージの要約コードのような当初のメッセージデータを要約またはハッシュ値を計算するコードを用いて決定される。
【０００８】
メッセージの作者が偽ってメッセージの送信を否認することができないように、暗号に

よる受信の産物が否認防止を記述する。このように、前記インターネットは、人々、コンピュータおよび組織間の信頼すべき関係について十分な複雑さを見せている。

【０００９】

デジタル署名のような秘密キーおよびキー変換を含有する暗号処理が、例えば、周辺カード上で実行されることが知られている。そのような環境で取引に署名することによって、取引においてユーザは自身と他の当事者との間で交換されたデータの僅かな完全性と非公開性でもって保証されている。秘密キーは周辺カードの外部に公開される必要はない。しかしながら、周辺カードの不利益の１つは、その所有者が前記ホストシステムの誤用から保護されていないことである。例えば、ディスプレイ画面のようなユーザのインタフェースがないために、前記所有者は署名された現実の前記メッセージの内容について確信がもてないことであろう。

【００１０】

採用された他の方法は、無線適用プロトコール（ＷＡＰ）可能携帯電話や無線個人用デジタル補助装置（ＰＤＡ）のような個人専用化装置によって前記解決法を実行することであって、そのとき前記個人専用化装置は前記署名トークンを提供する。そのような個人専用化装置は秘密キーを保持しかつ所有者のために取引を署名することができる。そのような状況では、前記個人専用化装置の保持者が、適正なアクセス制御機構によって決定されたような正当な所有者または認可された代理人、これはその場合ではないが、であると想定される。この方法は、「信頼性のある通信システムおよび方法」という発明の名称を持つ米国特許第７２１６２３７号にバンストーンによってさらに拡張され、そこではデータメッセージが、パソコン（ＰＣ）のような外部装置上で生成され、それから署名のために前記個人専用化装置に提示される。バンストーンは、前記顧客が前記パソコン上と個人化用装置上の前記メッセージを比較してから、前記メッセージへの彼らの電子署名を書き添えることの承諾を発行し、それによって、例えば、前記電子商取引を完了することを教示している。他に、バンストーンは、無線電子商取引を可能にする全ての行為が前記個人専用化装置内に含まれていることを教示している。

【００１１】

しかしながら、どちらの方法にも、詐欺的行為に対する本質的なリスクが存在する。前記第１の方法では、前記メッセージがパソコン上で作成されて前記個人専用化装置に伝送される際に、前記メッセージの完全性に疑問が生じかつ前記メッセージを十分に証明する能力もまた疑問である。したがって、署名された前記データメッセージは個人専用化装置を通して伝送されるけれども、前記個人専用化装置の小さな視覚領域および一般には不便なユーザのインタフェースを用いて全体の前記文書を証明することは困難である。

【００１２】

前記第２の状況では、全ての行為は前記個人専用化装置内に含まれており、個人専用化装置の制約によって取引の証明および実行をするという不便に直面する。

【００１３】

少なくとも上記制約のいくつかを克服する方法およびシステムを提供することは利益がある。

【発明の概要】

【００１４】

発明の１の態様によれば、複数の透かしを格納する記憶装置と、取引データを受信するため、複数の前記透かしから第１の透かしを選択するため、証明用の第１のデータを有しかつ前記取引に関係する第１の証明データおよび前記第１のデータの改ざんを防止する前記第１の透かしに関係する第１の透かしデータを生成するため、かつ選択された前記透かしの表示を有する第２の証明データを提供するための適切にプログラムされたプロセッサと、前記第１の証明データを目的地のシステムに送信し前記第２の証明データを第２の他の目的地のシステムに送信するための少なくとも１の送信機と、を有するコンピュータサーバを提供する。

【００１５】

発明の他の態様によれば、複数の既知の透かしについての透かし用の表示をその中に格納しているメモリと、第２の証明データを受けかつそれに基づいて透かしの表示を決定するためのプロセッサと、前記安全処理システムのユーザに前記表示を表示するためのディスプレイとを有する安全処理システムを提供する。

【００１６】

発明の他の態様によれば、第１のシステムとサーバとの間の第１の通信経路を構築し、既知のユーザに対する取引に関係するデータを第１のシステムから受信し、前記取引を証明しかつ承諾するための第１の証明データを前記第１のシステムに提供し、第２の他のシステムと前記サーバとの間の第２の通信経路を構築し、かつ、前記透かしの表示の提供に使用するための第２の証明データを前記第２の他のシステムに提供する各工程を有するとともに、前記第１の証明データは透かしを有し、前記第２のシステムは前記既知のユーザと結びついている方法を提供する。

【００１７】

発明のさらに他の態様によれば、作動の際には、第１のシステムとサーバとの間の第１の通信経路を構築し、既知のユーザのための取引に関係するデータを前記第１のシステムから受信し、前記取引を証明しかつ承諾するための第１の証明データを前記第１のシステムに提供し、第２の他のシステムと前記サーバとの間の第２の通信経路を構築し、前記透かしの表示の提供に使用するための第２の証明データを前記第２の他のシステムに提供する工程を有し、前記第１の証明データは透かしを有し、前記第２のシステムは前記既知のユーザと睦びつく結果に導く予め定めたコンピュータ装置に応じたデータをその中に格納したコンピュータ読出し可能な媒体を提供する。

【図面の簡単な説明】

【００１８】

本発明の典型的な実施の形態が、以下の図面とともに記述される。

【００１９】

【図１】図１はバンストーンの名前での米国特許第７２１６２３７による顧客によって署名された信頼性のあるメッセージを提供する先行技術の方法を例示している。

【００２０】

【図２】図２は本発明の第１の典型的な実施の形態であって、信頼性のある経路が商取引の当事者と顧客との間に、安全な取り外し可能な記憶装置の使用を通して最初に構築されることを例示している。

【００２１】

【図３】図３は本発明の第２の典型的な実施の形態であって、前記信頼性のある経路が、前記顧客のパソコンとピアツーピア通信関係をもつ顧客の個人専用化電子装置によって構築され、それから前記商取引が主に前記顧客のパソコン上で起動されるものを例示する。

【００２２】

【図４】図４は本発明の第３の典型的な実施の形態であって、前記信頼性のある経路が、前記顧客の個人専用化電子装置によって構築され、前記取引が主に前記顧客のパソコン上で起動され、前記信頼性のある経路および取引の経路が完全に分離されるものを例示している。

【発明を実施するための形態】

【００２３】

後述する詳細な説明及び請求の範囲において、透かしという前記語句は、取引証明データ内に該データから容易に分離できないように挿入された特定の取引に無関係なデータを表すために用いられている。透かしの１例は、文書上の薄い背景画像であって、その文書上には取引の詳細が上書きされていて、取引の詳細の変更がいくつかの前記透かしの消去に導きそのため検出可能となる。透かしの他の例は、音響的取引証明データ上に上書きされた音響的な流れである。取引の詳細が音響形式で振舞うような透かしの一例は、低い音量で背景に流れている曲であって、前記取引の詳細の音響的内容の変更は、背景の曲が沈黙しまたは変更されるので検出可能である。

【００２４】
図１は、バンストーンの名前をもつ米国特許第７２１６２３７に係り、顧客による署名のための信頼されたメッセージを提供する先行技術の方法を示している。その方法は、データメッセージの完全性を証明するためのシステム１１０が、相互に通信し合う第１の装置と第２の装置との間に与えられている。前記第１の装置は個人専用化装置１１２として示され、前記第２の装置はパソコン１１４として示されている。バンストーンに係るこの実施の形態では、前記個人専用化装置１１２は、安全モジュール１１８を有する基本プロセッサ１１６によって制御される携帯電話である。前記安全モジュール１１８は、前記基本プロセッサ１１６について独立に作動するように構成され、その結果前記安全モジュール１１８の内部状態は、うまく解析して模倣することができず、かつ、または、その基本的なハードウェアとの相互作用は悪意で傍受されかつ再解釈されることはない。装置のディスプレイ１２０は、前記装置の基本プロセッサ１１６と結合し、ユーザに情報の入力を促すテキスト表示および画像表示を提供する。前記装置の基本プロセッサ１１６と接続したキーボード１２２は、情報の供給を容易化する。同様にして、前記安全モジュール１１８は安全ディスプレイ１２４及び信頼性のあるボタン１２６と通信し合う。

【００２５】
前記安全ディスプレイ１２４は、全体として安全モジュール１１８の制御下にあり、安全経路１２８によってそれと接続し、かつ前記信頼性のあるボタン１２６が安全経路１３０を介して前記安全モジュール１１８と直接的に通信し合っている。したがって、前記安全経路１２８および１３０は、論理的にどんな他の経路からも孤立しかつ異なる。前記安全モジュール１１８、前記安全入出力装置１２４および１２６、および、前記安全経路１２８および１３０は、上記安全モジュール１１８と個人専用化装置１１２のユーザとの間の信頼性のある経路を形成する。前記パソコン１１４は、外部ディスプレイ１３２を有する。立証用の前記データメッセージが前記外部コンピュータ１１４から通信経路１３６を介して前記個人専用化装置１１２に伝送され、その上前記メッセージトランシーバ１３４によって受信される。前記個人専用化装置１１２による立証用の前記データメッセージは前記パソコン１１４から通信経路１３６を介してまたはアンテナ１３４を通る無線インタフェースを通して伝送される。このようにして、前記個人専用化装置１１２はデータを受信し、かつ前記パソコン１１４上で生成したデータメッセージに署名するために使用される。作動中には、前記パソコン１１４は、署名されるべきデータメッセージ部分を有するデータを組み立て、好ましくは、前記外部ディスプレイ１３２に前記適当なデータメッセージを表示し、かつ、前記データを前記個人専用化装置１１２に前記経路１３６を介して伝送する。

【００２６】
前記基本プロセッサ１１６は前記データを前記安全モジュール１１８に伝送し、希望するのであれば、同一データを前記ディスプレイ１２０上に表示する。前記安全モジュール１１８は、前記データメッセージまたは前記メッセージの一部を、適当なフォーマットで、前記安全ディスプレイ１２４上に表示する。前記データの完全性を証明するために、前記ユーザは、前記外部ディスプレイ１３２上の前記データメッセージと前記安全ディスプレイ１２４上の前記データメッセージとを比較する。もし、２つの前記データメッセージの間に相関性があれば、前記ユーザは、署名発生器に、信頼性のあるボタン１２６の形態での前記信頼性のあるアクチュエータを駆動することによって署名の発生処理を指示する。

【００２７】
バンストーンによって提示された前記システム１１０において、前記信頼性ある経路は、前記パソコン１１４と個人専用化装置１１２との間でのみ構築され、両者は同一のユーザに属している。すると、前記信頼性のある経路は、署名された前記データメッセージ部分に対してのみ用いられている。すると、バンストーンは、前記データメッセージの内容を少し変えるという前記パソコン１１４上での介入者（MITM）攻撃から、前記ユーザを防御しておらず、その結果前記ユーザは彼らが署名している完全な前記メッセージの内容を

必ずしも知らない。前記ユーザは、改ざんを捜す場所を知らないので、前記個人専用化装置上に表示された文書を非常に注意深く検討しなければならない。大抵の携帯電話は非常に小さなディスプレイをもち多くの署名を要求する文書は長々しくかつ詳細なので、これは不便でありかつ困難である。

【００２８】

本発明の実施の形態に係る取引システム２００に関して、取引者２１０からユーザ２８０への信頼性のある経路２０００の典型的な実施の形態を図２に示す。そうであるので、前記取引者２１０との少なくとも１の取引を行おうとするユーザ２８０は彼らのセキュリティ・モジュール２４０をラップトップコンピュータ２３０に連結することで安全通信チャネルの構築を起動して、前記取引者２１０への要求を起動する。前記取引者２１０と前記ラップトップコンピュータ２３０の両者は、ワールド・ワイド・ウェブ（インターネットとして通常言及される）２２０の形態でのネットワークを通して相互に接続される。前記ユーザ２８０からの要求を受けると、前記取引者２１０は、前記ユーザ２８０に証明書２７０を発行し、該証明書は前記インターネット２２０を通して前記ラップトップコンピュータ２３０に伝送され、その上、前記ユーザのセキュリティ・モジュール２４０に伝送される。

【００２９】

前記証明書２７０は、前記取引者２１０によって発行されるデジタル文書であり、公開キーの前記取引者２１０との結びつきを立証し、かつ前記証明書２７０に設けられた前記公開キーは事実前記取引者２１０に属しているという主張の証明を可能にしている。前記証明書は、それによって第三者が、偽りの公開キーを用いて前記取引者２１０になりすますことを防止する。その最も簡単な形態では、証明書２７０は公開キーおよび氏名を含有するが、通常それは終了日、その証明書を発行した証明機関の名前、通し番号およびおそらくは他の情報を含有する。最も重要なことは、前記証明書の発行者のデジタル署名を含有している。最も広く受け入れられた証明書の様式はITU-TX.509国際標準によって定義され、他の様式も前記発明の範囲内で採用されるかもしれない。

【００３０】

前記証明書２７０を有効化する際に、セキュリティ・モジュール２４０はユーザ２８０が彼らの身元証明を提供することを要求する。示されるように、前記セキュリティ・モジュール２４０は、前記ユーザに指紋２５０とパスワード２６０の両方を提供することを要求し、前記指紋２５０は前記ユーザ２８０の前記セキュリティ・モジュール２４０での物理的存在を証明し、前記パスワード２６０は前記取引者２１０によるそれらの取引ファイルへのアクセスを提供する。前記指紋２５０およびパスワード２６０の両者を有効化するに際し、前記セキュリティ・モジュール２４０はユーザのセキュリティ・モジュール２４０およびそのユーザと取引者との間の信頼性のある経路２０００の構築を完了するのに必要な任意のキーまたはパスワード情報を前記取引者２１０に提供する。前記ユーザ２８０は、直ちに彼らのラップトップコンピュータ２３０上で彼らが行おうとしている取引にアクセスし、そこでは、取引を完了する前に、前記ユーザ２８０は、彼らのデジタル署名を承諾して取引を完了することが要求される。

【００３１】

取引が要求され、取引情報が提供されると、有効化要求が前記取引の内容の視覚的表示の形態で生成される。この時点で、前記第１の有効化要求２３５が前記ユーザのラップトップコンピュータ２３０上のディスプレイの形態でのディスプレイ上に表示され、前記ユーザのセキュリティ・モジュール２４０上のディスプレイの形態での第２のディスプレイ上に第２の有効化要求２４５として表示される。前記ユーザ２８０は、もし前記第１および第２の有効化要求２３５および２４５が正しくかつ相関性があると決定するならば、第２の指紋２５５の形態で、承諾を提供することによって彼らのデジタル署名の発行を起動する。

【００３２】

本発明の第１の典型的な実施の形態によれば、信頼性のある経路２０００は、最初に、

取引者２１０と前記ユーザのセキュリティ・モジュール２４０との間で構築され、希望するならば、指紋２６０とパスワード２５０の形態でのユーザの入力データに依存させる。次に、任意の取引は、前記ユーザに、ラップトップコンピュータ２３０の形態での前記取引を起動する彼らの主要システム上に提示される情報を提供し、その情報は前記取引者２１０によって前記ユーザのセキュリティ・モジュール２４０に提供される情報に応じたものである。そのような情報の例として、第２のデジタル証明書、電子透かし、符号化された画像、および、両方の当事者によってのみ知られた情報および署名のための文書内での関連項目の表示の事項を含むがそれに限られない。

【００３３】

電子透かし入れに対しては、例えば、主要システムに提供された文書は透かしが入れられており、該透かしの表示は前記セキュリティ・モジュール２４０を通して前記ユーザに提供される。電子透かしは、前記取引書類内に埋め込まれた透かしを有し、該透かしは、前記透かしにおける変化により前記文書内での情報の変更が人目を引くように、前記文書に一体化している。前記信頼性のある経路２０００を通して提供された情報に基づいて前記透かしの証明が実行される。例えば、前記透かしの画像は、前記信頼性のある経路２０００を通して前記ユーザのセキュリティ・モジュール２４０に提供される。

【００３４】

代わりのものとして、前記ユーザのセキュリティ・モジュール２４０に提供された前記情報は、前記取引者によって提供された前記情報の表示であって、前記ユーザに、彼らのラップトップコンピュータ２３０上におけるように表示される。例えば、前記ユーザのセキュリティ・モジュール２４０に提供される情報は、「ジョージ・ワシントン」を有し、前記取引者によって提供された情報が有効であるためにはジョージ・ワシントンの透かしを含有すべきであることを表示している。他の例として、前記情報は「トリシャの誕生日」を有しており、前記透かしは、トリシャは、家族、友人または他の人であって、その誕生日が前記ユーザに知られているものの誕生日であることを表示している。そのような方法は詐欺的な取引のための偽りのデジタル署名の使用をより困難で回避可能とするので、あらゆる取引は、複数の割り当てられた透かしの種々のものを使用することで証明することができる。希望により、前記透かしは全体的な透かしの集合から選択される。代わりに、前記透かしは前記ユーザに特有な透かしを含有する。

【００３５】

上述した実施の形態は前記モジュールに対する安全な経路を含有するけれども、透かしを決定する秘密の情報を用いまたはセキュリティのいくつかのレベルを提供するパケットの異なる伝送経路に依存することのいずれかによって、同じ方法が安全経路なしで実行可能である。

【００３６】

図３に示すように、本発明の典型的な第２の実施の形態が、取引システム３００に関して、取引者３１０からユーザ３８０までの信頼性のある経路３０００について提示されている。そうであるので、取引者３１０との少なくとも１の取引を実行しようとする前記ユーザ３８０は、ピアツーピア（サーバ機を使用せず、各コンピュータが対等な立場で接続されているＬＡＮ）リンク３９０を介してラップトップコンピュータ３３０とＰＤＡ（個人用デジタル補助）の形態でのセキュリティ・モジュール３４０とを結合することによって安全な通信チャネルの構築を起動し、それから前記取引者３１０への要求を起動する。前記取引者３１０とラップトップコンピュータ３３０の両者はインターネット３２０の形態でのネットワークを介して相互に接続する。希望する場合には、前記セキュリティ・モジュール３４０は前記取引者と、前記ピアツーピアリンク３９０によって、前記ラップトップコンピュータ３３０を介してよりもむしろ前記インターネット３２０との接続を介して前記取引者と通信する。前記ユーザ３８０からの前記要求を受信すると、前記取引者３１０は証明書３７０の形態でのセキュリティ・データを前記ユーザ３８０に発行し、前記データは前記インターネット３２０を介して前記ラップトップコンピュータ３３０に伝送され、それによってピアツーピアリンク３９０を介して前記セキュリティ・モジュール３

４０に伝送される。

【００３７】

前記証明書３７０は、前記取引者３１０によって発行され公開キーの前記取引者３１０への結びつきを裏づけかつ前記証明書３７０に設けられた前記公開キーが事実前記取引者３１０に属するという主張の証明を可能にするデジタル文書を有している。前記証明書はそれによって第三者が偽の公開キーを用いて前記取引者３１０を装うことを禁止する。

【００３８】

前記証明書３７０を有効化する際に前記ＰＤＡ３４０は、前記ユーザ３８０が彼らの身元の証明を提供することを要求する。示されたように、前記セキュリティ・モジュール３４０は前記ユーザ３８０に対して第１の指紋３５０とパスワード３６０の両方を提供することを促す。前記第１の指紋３５０は前記セキュリティ・モジュール３４０での前記ユーザ３８０の物理的存在を証明するものであり、前記パスワード３６０は前記取引者３１０による彼らの取引ファイルへのアクセスを提供するものである。希望するならば、ユーザの立証の他の形態が採用される。前記第１の指紋３５０とパスワード３６０の両方を有効化する際に、前記セキュリティ・モジュール３４０が前記取引者３１０にユーザのセキュリティ・モジュール３４０と取引者３１０との間の信頼性のある経路３０００の構築を完了するのに必要な任意のキーまたはパスワード情報を提供する。前記ユーザ３８０は、取引に関するデータを入力してラップトップコンピュータ３３０の使用に取り掛かる。一旦取引が決定されかつ該取引完了前であれば、前記ユーザ３８０は彼らのデジタル署名を提供して前記取引を完了することを要求される。この時点で、取引関連データを含有する前記第１の有効化要求３３５が前記ユーザのラップトップコンピュータ３３０上に表示され、証明データを含有する前記第２の有効化要求が前記ユーザのセキュリティ・モジュール３４０に提供される。前記ユーザ３８０は前記第２の有効化要求に基づいて決定された表示に対して前記第１の有効化要求３３５を証明し、相関性がある場合には、彼らのデジタル署名の発行を、例えば、第２の指紋３５５を提供することによって起動する。

【００３９】

前記第１の有効化要求３３５の例は、ステガノグラフィー（電子迷彩技術）、電子透かし、更なるデジタル証明書、テキストシール、画像シールおよび旋回テストによりメッセージを埋め込むことを含有するがそれに限定されるわけではない。旋回テストの例は、コンピュータと人間とを見分けるための完全に自動化された周知の旋回テスト（CAPTCHA）、帰納的旋回テスト（RTTs）、および自動化旋回テスト（ATTs）を含有する。図２に関して前述したように、前記ユーザのセキュリティ・モジュール３４０上に提供される前記情報は、希望するならば、前記取引者によって提供される前記情報の表示であり、ラップトップコンピュータ３３０に表示される。したがって、このようにして、前記セキュリティ・モジュール３４０は前記ラップトップコンピュータ３３０と同様な表示能力を要求しない。例えば、前記ユーザのセキュリティ・モジュール３４０上に提供される前記情報は、希望するならば、「ジョージ・ワシントン」であって、前記取引者によって提供された前記情報が有効である場合にはジョージ・ワシントンの透かしを含有すべきであることを表示しており、これは、小さな液晶文字ディスプレイを介して、スピーカーを介して、または１組のＬＥＤを介して、各々結びついている透かしについて達成可能である。そうであるので、前記セキュリティ・モジュールは、より単純に、低いコストで製造され、または、ＵＳＢトークン、ＵＳＢメモリスティック、ＭＰ３プレイヤー等の種々の安価な電子装置に埋め込まれることができる。

【００４０】

あらゆる取引が証明データを含有するので、そのような方法は、例えば、普通人による潜在的な取引の偽発生をより困難にする。１の実施の形態では、前記証明データは、１または２以上の複数の透かしを有する。さらに、前記透かしは希望するならば、個人または組織にとって唯一のものである。代わりに、前記透かしは、前記システムに対して包括的である。さらに、前記透かし情報は、希望するならば、定期的に改定され、かつ、前記ユーザのセキュリティ・モジュールに伝送され、必ずしも取引と関係しない他の活動中に、

または、例えば、前記ユーザが仕事中に物理的結合を通して伝送される。もちろん、各文書は種々の独特の画像で透かし入れ可能であるので、前記透かしを提示する視覚的な表示を提供することは、顕著な柔軟性を与える。

【００４１】

希望するならば、前記第２の実施の形態は、安全な通信に依存しないで実行される。例えば、透かしが用いられた場合に、前記第１の証明データ内で前記透かしを符号化して前記ＰＤＡ３４０に、セキュリティなしで前記透かしの内容の表示を伝送することが可能である。前記第１の証明データ３４５を変更することが、前記透かしの注意深い検討によって検知可能であって、普通人が前記第１の証明データ３４５および第２の証明データを成功裏に傍受するだろうことはありそうにもない。希望するならば、コードが前記ＰＤＡ３４０に移送されて、前記透かしの内容の明瞭な表示に変換される。例えば、ルック・アップ・テーブルに対するアドレスが提供され、前記ＰＤＡ３４０は前記透かしの記述子を調べる。そのような実施の形態にあっては、前記透かしの記述子は希望するならば、周期的に変更される。そうであるので、前記コードが傍受されたとしてもそれらが意味することを知ることは困難である。

【００４２】

希望するならば、前記ＰＤＡ３４０の代わりに、ＵＳＢメモリスティックのような周辺記憶装置が採用される。さらに、希望するならば、他の装置が用いられて、前記発明を実行するための適当な機能を与える。

【００４３】

図４に示すように、本発明の第３の実施の形態が、前記取引システム４００に関する前記取引者４１０からユーザ４８０までの安全な経路４０００について提示している。取引者４１０との少なくとも１の取引を実行しようとする前記ユーザ４８０は、ＰＤＡ（個人用デジタル補助）４４０の形態の安全通信装置を用いることによって安全通信チャネルの構築を起動して、前記取引者４２０に要求を起動する。前記取引者４１０およびＰＤＡ４４０はインターネット４２０の形態でのネットワークを介して連結される。前記ユーザ４８０からの前記要求を受けると、前記取引者４１０は証明書４７０を前記ユーザ４８０に発行し、前記証明書は、前記インターネット４２０を介して直接彼らのＰＤＡ４４０に伝送される。

【００４４】

前記証明書４７０は、前記取引者によって発行され、公開キーの前記取引者４１０への結びつきを立証し、かつ前記証明書４７０に設けられた前記公開キーが事実前記取引者４１０に属するとの主張の証明を可能にするデジタル文書を有する。前記証明書はそれによって、第三者が偽りの公開キーを用いて前記取引者４１０に成りすますことを防止する。代わりに、安全な通信経路を構築する他の方法を採用する。

【００４５】

前記ＰＤＡ４４０は、前記証明書４７０を有効化する際に、ユーザ４８０が彼らの身元の証明を提供することを要求する。示されているように、前記ＰＤＡ４４０は前記ユーザ４８０に第１の指紋４５０とパスワード４６０の両方を提供することを促し、前記第１の指紋４５０は前記ユーザの前記ＰＤＡ４４０での物理的存在を証明するものであり、前記パスワード４６０は前記取引者４１０に対し彼らの取引ファイルへのアクセスを提供するものである。前記第１の指紋４５０及びパスワード４６０を有効化するに際し、前記ＰＤＡ４４０は前記取引者４１０に任意のキーまたはパスワード情報を提供してユーザのＰＤＡ４４０と、そこのユーザ４８０と取引者４１０との間の信頼性のある経路４０００の構築を完了させる。希望するならば、ユーザの証明の他の方法が採用される。さらに、希望するならば、ユーザの証明が実行されない。前記ユーザ４８０は、前記取引者４１０に、引き受けられるべき取引に関係するデータをラップトップコンピュータ４３０によって提供する。取引が決定されると、前記取引が完了する前に、前記ユーザ４８０は、デジタル署名を提供する。前記デジタル署名を要求する際に、第１の有効化データ４３５が提供され、前記ラップトップコンピュータ４３０に表示され、第２の有効化データが提供され、

それとは独立に、証明情報４４５が前記ＰＤＡ４４０にいる前記ユーザに表示される。前記ユーザ４８０は、前記第１の有効化データ４３５を前記証明情報に対して証明し満たしている場合には、前記デジタル署名の発行を、例えば、個人的な識別番号を提供することによって起動する。好ましくは、前記デジタル署名及びデジタル契約は、前記ＰＤＡ４４０上で行われる。

【００４６】

本実施の形態では、前記ラップトップコンピュータ４３０とＰＤＡ４４０との間の経路は、それらの経路の部分によって種々であり、潜在的には、前記取引者４１０に非常に接近している場合を除き、重複しないことは明らかであろう。例えば、前記ラップトップコンピュータ４３０は希望により物理的に、ローカル・エリア・ネットワークまたはケーブルインターネットサービスを介して記して前記インターネット４２０に接続され、または、2.4GHzまたは5GHzで典型的に作動するＷｉＦｉまたはＷｉＭａｘのような標準によって前記インターネット４２０に対するローカル・アクセス・ポイントへ無線で連結される。それに対して、ＰＤＡ４４０は、希望によりセルラー基地局への無線リンクを介して、850MHz、900MHz、1800MHz、または1900MHzで作動するグローバル・システム・フォー・モバイル通信方式のような標準に従って、前記インターネット４２０と接続される。前記セルラー基地局は、光ファイバ・ローカル・エリア・ネットワークのような、セルラー方式の基幹ネットワークと、さらには、無線プロバイダーネットワークの経路設定ハブに接続される。この経路設定ハブから前記取引者４１０への接続は、インターネットを経由する。

【００４７】

希望するならば、取引についての前記デジタル署名の発行は、前記ＰＤＡ４４０から前記取引者４１０への前記信頼性のある経路４０００を介する証明メッセージの伝送によって、または、前記ＰＤＡ４４０から前記ラップトップコンピュータ４３０へのピアツーピア移送によって行われる。したがって、第３の典型的な実施の形態は、前記第１および第２の有効化データ４３５の前記取引者４１０から前記ユーザ４８０に対する経路の多様性を提供する。そのような経路の多様性は、介入者（MITM）攻撃のための前記第１の有効化データ４３５と前記第２の有効化データの両方の同一の当事者による傍受に対し、より大きな困難性を顕著に与える。さらに、ラップトップコンピュータ４３０上の悪意のあるソフトウェアの存在は、前記第２の有効化データ４４５に影響を及ぼさない。これは前記ラップトップコンピュータ４３０を介して伝送されるものではないからである。

【００４８】

希望するのならば、前記第２の典型的な実施の形態は、安全通信に依存せずに実行される。例えば、透かしが用いられる場合には、前記第１の証明データ４３５内で前記透かしを符号化し、それから、セキュリティなしでそこから前記透かしの内容４４５の全ての表示を決定するための第２の証明データを前記ＰＤＡ４４０に送信する。前記第１の証明データ４３５を変更することは前記透かしの注意深い検討を通して検出可能である。普通人が成功裏に前記第１および第２の証明データ４３５，４４５を傍受するだろうことはありそうもない。希望する場合には、コードの形態にある第２の証明データが、前記ＰＤＡ４４０であって、前記透かしの内容４４５の明らかな表示が変更される。例えば、ルック・アップ・テーブルに対するアドレスが提供されて、前記ＰＤＡ４４０は前記透かしの記述子を調べる。そのような実施の形態では、前記透かしの記述子は希望するならば、周期的に変更され、すると、前記コードが、傍受された場合であってもそれらが意味するものを知ることは困難である。

【００４９】

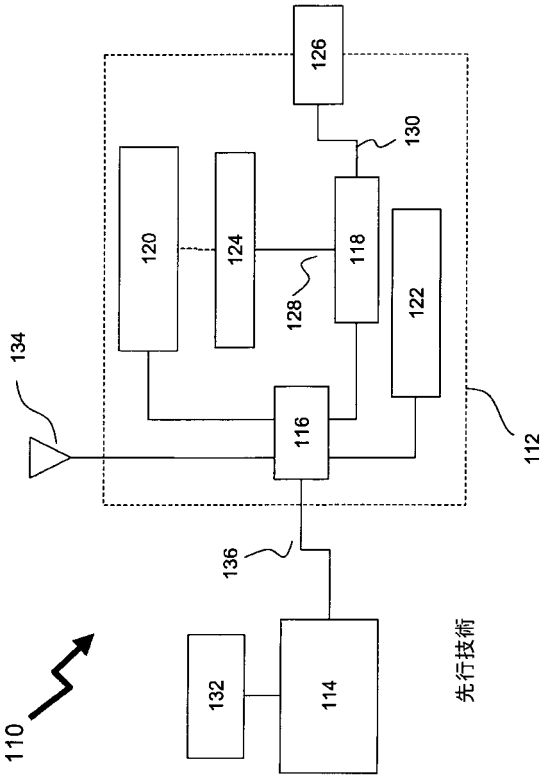
希望するならば、前記ＰＤＡ４４０の代わりに、ＵＳＢメモリスティックのような周辺記憶装置が採用される。さらに、希望する場合には、他の装置が用いられて、前記発明を実行するための適当な機能を提供する。

【００５０】

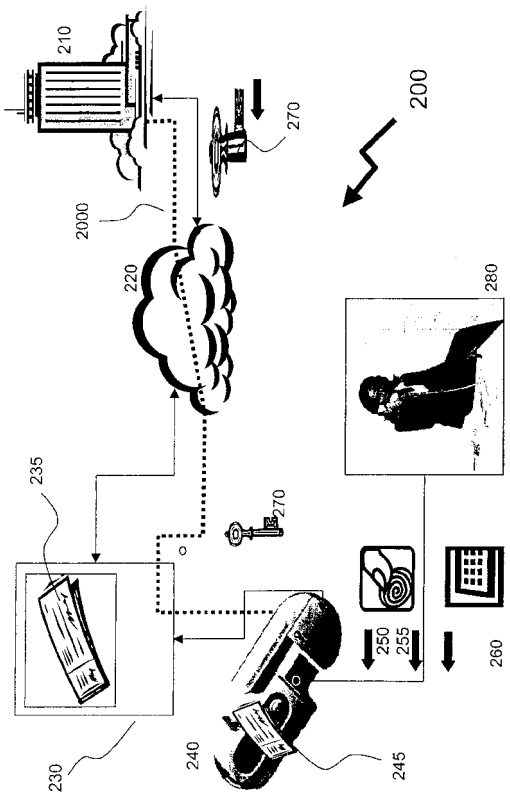
上記実施の形態は、ラップトップコンピュータについて記述しているけれども、希望するならば、システムに基づく他の適当なプロセッサが、その代わりに用いられる。

【００５１】
多数の他の実施の形態が、本発明の範囲またはその主旨を逸脱せずに想像することができる。

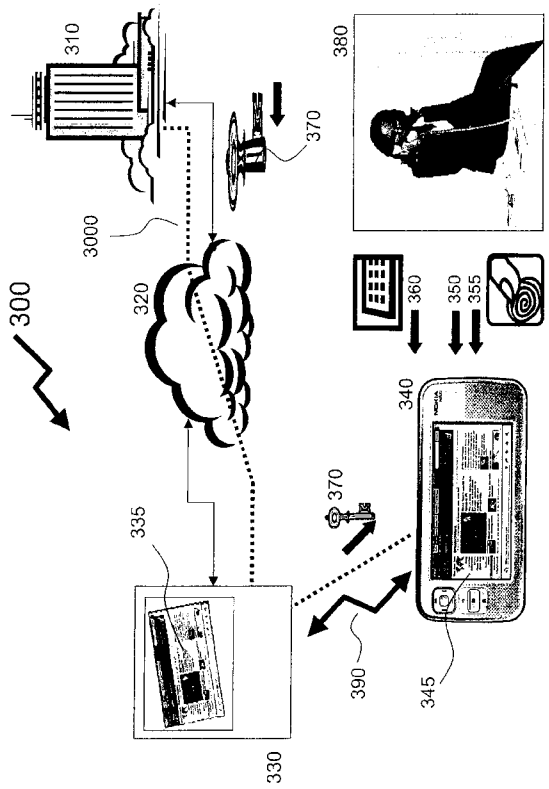
【図１】



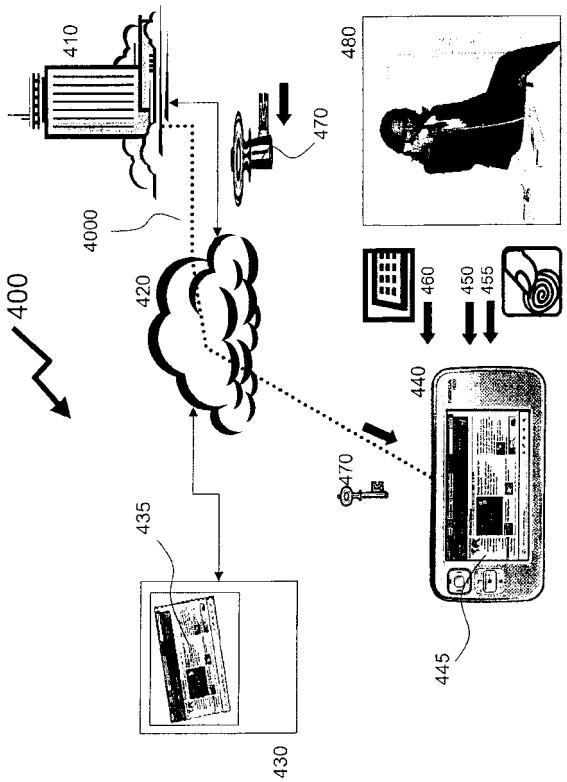
【図２】



【図３】


300
310
320
330
335
340
345
350
355
360
370
380
390
3000

【図４】


400
410
420
430
435
440
445
450
455
460
470
480
4000

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2008/001434

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***H04L 9/32*** (2006.01) , ***G06F 21/00*** (2006.01) , ***G06Q 30/00*** (2006.01)
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
All IPC (2006.01)classes using key words

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Delphion, WEST, Canadian Patent Database, Scopus
Keywords: electronic transaction, digital certificate/signature, time signature/stamp, watermark, trusted/secure communication path, embed, verification, steganography, text/image seal, CAPTCHA, identification, authentication, authorization, encryption, message digest, codes,

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	US5917913 A; Portable Electronic Authorization Devices and Methods Therefor"; WANG, Y. ; 29 June 1999 (29-06-1999) [col. 4 lines 8-65], [col. 5 lines 1-18], [col. 5 line 51 to col. 6 line 21], [col. 7 lines 1-17], [col. 8 line 65 to col. 10 line 6], [col. 11 line 50 to col. 12 line 64], [col. 12 line 65 to col. 13 line 9], [Fig. 2, 5A &6B]	3-8 1, 2, 9-25
Y A	US7216237 B2; "System and Method for Trusted Communications"; VANSTONE, S.; 8 May 2007 (08-05-2007) [col. 3 line 65 to col. 4 line 51], [col. 5 line 4 to col. 6 line 3], [Fig. 1 & 2]	3-8 1, 2, 9-25
A	US5778071 A; Pocket Encrypting and Authenticating Communications Device" CAPUTO et al.; 7 July 1998 (07-07-1998) *** whole document ***	1-25
A	US20060287963 A1; "Secure Online Transactions Using a Captcha Image as a Watermark"; STEEVES et al.; 21 December 2006 (21-12-2006) *** whole document ***	1-25

[ ] Further documents are listed in the continuation of Box C.
[X] See patent family annex.

* Special categories of cited documents :
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06 November 2008 (06-11-2008)	18 November 2008 (18-11-2008)
Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001-819-953-2476	Authorized officer Lawrence J. Engel 819- 997-2936

Form PCT/ISA/210 (second sheet) (July 2008)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CA2008/001434

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US 5917913A	29-06-1999	AU 2059701A	24-09-2001
		AU 4004300A	21-09-2000
		AU 5383198A	29-06-1998
		AU 2002247213A1	12-09-2002
		AU 2002357047A1	02-09-2003
		AU 2002367640A1	08-10-2003
		AU 2002367640A8	08-10-2003
		CA 2365644A1	08-09-2000
		CA 2403332A1	20-09-2001
		CN 1265292C	19-07-2006
		CN 1307594C	28-03-2007
		CN 1344396A	10-04-2002
		CN 1452739A	29-10-2003
		CN 1623173A	01-06-2005
		EP 1159700A2	05-12-2001
		EP 1272933A1	08-01-2003
		HK 1077386A1	12-10-2007
		JP 2003517658T	27-05-2003
		JP 2003527714T	16-09-2003
		KR 20080072742A	06-08-2008
		TW 487864B	21-05-2002
		TW 560159B	01-11-2003
		TW 565786B	11-12-2003
		US 6175922B1	16-01-2001
		US 6282656B1	28-08-2001
		US 6594759B1	15-07-2003
		US 6850916B1	01-02-2005
		US 7089214B2	08-08-2006
		US 7107246B2	12-09-2006
		US 2002023215A1	21-02-2002
		US 2002123967A1	05-09-2002
		US 2003004827A1	02-01-2003
		US 2007089168A1	19-04-2007
		WO 0052866A2	08-09-2000
		WO 0052866A3	21-12-2000
		WO 0052866A9	30-08-2001
		WO 0169388A1	20-09-2001
		WO 9825371A1	11-06-1998
		WO 02069291A2	06-09-2002
		WO 02069291A3	16-10-2003
		WO 03065318A2	07-08-2003
		WO 03065318A3	26-02-2004
		WO 03081377A2	02-10-2003
		WO 03081377A3	04-03-2004
US 7216237B2	08-05-2007	CA 2453853A1	30-01-2003
		EP 1413157A1	28-04-2004
		JP 2005509334T	07-04-2005
		US 2003014632A1	16-01-2003
		US 2007214362A1	13-09-2007
		WO 03009619A1	30-01-2003

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2008/001434

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US 5778071A	07-07-1998	AU 726397B2	09-11-2000
		AU 4147097A	06-03-1998
		CA 2263991A1	19-02-1998
		CA 2263991C	30-11-2004
		EP 0916210A1	19-05-1999
		EP 0916210A4	07-04-2004
		IL 128507D0	31-01-2000
		US 5546463A	13-08-1996
		US 5878142A	02-03-1999
		WO 9807255A1	19-02-1998
US 2006287963A1	21-12-2006	US 7200576B2	03-04-2007
		US 2007005500A1	04-01-2007

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MT,NL,NO,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(72)発明者 ローレンス ハミド
カナダ国 ケー４エー １ゼット３ オンタリオ州 オタワ ブルックリッジ クレセント ５６１
(72)発明者 ダレン エル．クラーン
カナダ国 ケー２ケー ３ジェイ２ オンタリオ州 カナタ ウィンブルドン ウェイ ２２

Ｆターム(参考) 5J104 AA09 AA11 AA16 AA32 EA04 EA08 EA16 GA03 JA21 LA06
NA02 NA38 PA10