(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3768249号
(P3768249)
(45)発行日　平成18年4月19日(2006.4.19)　(24)登録日　平成18年2月10日(2006.2.10)

(51)Int.Cl.		F I		
G09C 5/00	(2006.01)	G09C	5/00	
G06K 7/10	(2006.01)	G06K	7/10	P
G06K 17/00	(2006.01)	G06K	17/00	V

請求項の数 27　(全 12 頁)

(21)出願番号　特願平5-315847
(22)出願日　平成5年11月22日(1993.11.22)
(65)公開番号　特開平7-36383
(43)公開日　平成7年2月7日(1995.2.7)
審査請求日　平成12年11月21日(2000.11.21)
審判番号　不服2004-13283(P2004-13283/J1)
審判請求日　平成16年6月28日(2004.6.28)
(31)優先権主張番号　979018
(32)優先日　平成4年11月20日(1992.11.20)
(33)優先権主張国　米国(US)

(73)特許権者　591142781
ピットニー、ボウズ、インコーポレーテッド
ＰＩＴＮＥＹ　ＢＯＷＥＳ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国コネチカット州、スタムフォード　（番地なし）
(74)代理人　100064285
弁理士　佐藤　一雄
(74)代理人　100077609
弁理士　玉真　正美
(74)代理人　100088889
弁理士　橘谷　英俊

最終頁に続く

(54)【発明の名称】物その他の実体を識別する方法および識別カードを製造する装置

(57)【特許請求の範囲】
【請求項１】
ａ）物その他の実体を走査して、前記物その他の実体の画像を表す第１の信号を発生する過程と、
ｂ）前記画像を識別カードの第１の部分の上にプリントする過程と、
ｃ）前記第１の信号を圧縮して前記画像の圧縮された表現を有する第２の信号を発生する過程と、
ｄ）前記第２の信号を暗号化する過程と、
ｅ）前記暗号化された第２の信号を２次元バーコードとして符号化して符号化された表現を得て、前記暗号化された第２の信号の符号化された表現を前記識別カードの第２の部分に組み込む過程と、
ｆ）前記第２の信号の前記符号化された表現を前記識別カードから読み出す過程と、
ｇ）前記第２の信号を復号する過程と、
ｈ）前記復号された第２の信号を解読する過程と、
ｉ）前記解読された第２の信号を展開して前記画像の展開された表現を得る過程と、
ｊ）前記展開された第２の信号を表示装置へ入力して、前記画像の前記展開された表現を表示する過程と、
ｋ）　前記第１の部分における前記画像を呈示する過程と、
を備える、物その他の実体を識別する方法。
【請求項２】

請求項１に記載の方法において、前記第１の信号をデジタル信号へ変換する過程をさらに備える方法。
【請求項３】
請求項２に記載の方法において、公開鍵暗号化システムの暗号化鍵、Ｅｉ、を用いて前記第２の信号を暗号化する、方法。
【請求項４】
請求項３に記載の方法において、前記暗号化鍵、Ｅｉ、に対応する解読鍵、Ｄｉ、を、前記公開鍵暗号化システムの第２の暗号化鍵、Ｅ１、で暗号化する、方法。
【請求項５】
請求項４に記載の方法において、前記暗号化された解読鍵、Ｅ１［Ｄｉ］を、前記第２の部分に組み込む前に、前記暗号化された第２の信号へ付す、方法。
【請求項６】
請求項５に記載の方法において、前記暗号化された第２の信号の解読は、解読鍵Ｄ１を用いて前記暗号化された鍵、Ｅ１［Ｄｉ］を解読する過程をさらに備える、方法。
【請求項７】
識別カードを製造する方法であって、
ａ）物その他の実体を走査して、前記物その他の実体の画像を表す第１の信号を生ずる過程と、
ｂ）前記画像を前記識別カードの第１の部分の上にプリントする過程と、
ｃ）前記第１の信号を圧縮して前記画像の圧縮された表現を有する第２の信号を発生する過程と、
ｄ）前記第２の信号を暗号化する過程と、
ｅ）前記暗号化された第２の信号を２次元バーコードとして符号化して符号化された表現を得て、前記暗号化された第２の信号の符号化された表現を前記識別カードの第２の部分に組み込む過程と、
を備える、方法。
【請求項８】
請求項７に記載の方法において、前記第１の信号をデジタル信号へ変換する過程を更に備える、方法。
【請求項９】
請求項８に記載の方法において、公開鍵暗号化システムの暗号化鍵、Ｅｉ、を用いて前記第２の信号を暗号化する方法。
【請求項１０】
請求項９に記載の方法において、前記暗号化鍵、Ｅｉ、に対応する解読鍵、Ｄｉ、を、前記公開鍵暗号化システムに対する第２の暗号化鍵、Ｅ１、で暗号化する、方法。
【請求項１１】
請求項１０に記載の方法において、前記暗号化された解読鍵、Ｅ１［Ｄｉ］を、前記第２の部分に組み込む前に、前記暗号化された第２の信号へ付す、方法。
【請求項１２】
ａ）識別カードにより識別すべき物その他の実体の画像を表す第１の信号を発生するための走査手段と、
ｂ）前記走査手段に応答して前記画像を前記識別カードの第１の部分にプリントするプリント手段と、
ｃ）前記第１の信号を圧縮して前記画像の圧縮された表現を有する第２の信号を発生する圧縮手段と、
ｄ）前記第２の信号を暗号化する暗号化手段と、
ｅ）前記暗号化された第２の信号の２次元バーコード表現を前記識別カードの第２の部分に組み込む符号化手段と、
を備える識別カードを製造する装置。
【請求項１３】

請求項１２に記載の装置において、前記第１の信号をデジタル信号へ変換するアナログ－デジタル変換器を更に備える装置。
【請求項１４】
請求項１３に記載の装置において、公開鍵暗号化システムの暗号化鍵、Ｅｉ、を用いて前記第２の信号を暗号化する手段を更に備える装置。
【請求項１５】
請求項１４に記載の装置において、解読鍵、Ｄｉ、が第２の暗号化鍵、Ｅ１、で暗号化され、前記暗号化された解読鍵、Ｅ１［Ｄｉ］が、前記第２の部分に組み込まれる前に、前記暗号化された第２の信号へ付される装置。
【請求項１６】
請求項１４に記載の装置において、前記暗号化鍵、Ｅｉ、と前記暗号化された解読鍵、Ｅ１［Ｄｉ］を中央局から受けとる手段を更に備える装置。
【請求項１７】
識別すべき物その他の実体の画像を第１の部分の上に有し、前記画像の圧縮された表現を有する暗号化された信号の２次元バーコード表現を第２の部分の上に組み込んで有する識別カードの有効性を確認する方法であって、
ａ）前記信号の前記バーコード表現を前記カードから読み出す過程と、
ｂ）前記信号の前記バーコード表現を復号する過程と、
ｃ）前記復号された信号を解読する過程と、
ｄ）前記解読された信号を展開して、前記画像の展開された表現を得る過程と、
ｅ）前記展開された信号を表示装置へ入力して、前記画像の前記展開された表現を表示する過程と、
ｆ）前記第１の部分における前記画像を呈示する過程と、
を備える、識別カードの有効性を確認する方法。
【請求項１８】
請求項１７の方法において、前記暗号化された信号は、公開鍵暗号化システムの暗号化鍵、Ｅｉ、を用いて暗号化される、方法。
【請求項１９】
請求項１８の方法において、前記鍵、Ｅｉ、に対応する解読鍵、Ｄｉ、を、前記公開鍵暗号化システムの第２の暗号化鍵、Ｅ１、で暗号化し、暗号化された解読鍵、Ｅ１［Ｄｉ］を生成し、前記暗号化された解読鍵、Ｅ１［Ｄｉ］を前記暗号化された信号へ付し、前記解読過程は、
ａ）前記暗号化された解読鍵、Ｅ１［Ｄｉ］を対応する解読鍵Ｄ１で解読して前記解読鍵、Ｄｉ、を回復する過程と、
ｂ）前記暗号化された信号を前記鍵、Ｄｉ、で解読する過程と、
を更に備える、方法。
【請求項２０】
識別すべき物その他の実体の画像を第１の部分の上に有し、前記画像の圧縮された表現を有する暗号化された信号の２次元バーコード表現を第２の部分の上に組み込んで有する識別カードの有効性を確認する装置であって、
ａ）前記信号の前記バーコード表現を前記カードから読み出す手段と、
ｂ）前記読み出し手段に応答して、前記信号の前記バーコード表現を復号する復号手段と、
ｃ）前記復号手段に応答して、前記復号された信号を解読する解読手段と、
ｄ）前記解読手段に応答して、前記解読された信号を展開して前記信号の展開された表現を得る展開手段と、
ｅ）前記展開手段に応答して、前記画像の前記展開された表現を表示する表示手段と、
を備える、識別カードの有効性を確認する装置。
【請求項２１】
請求項２０に記載の装置において、前記暗号化された信号は、公開鍵暗号化システムの

暗号化鍵、Ｅｉ、を用いて暗号化される、装置。
【請求項２２】
請求項２１に記載の装置において、前記鍵、Ｅｉ、に対応する解読鍵、Ｄｉ、が、前記公開鍵暗号化システムの暗号化鍵Ｅ１で暗号化されて、暗号化された解読鍵、Ｅ１［Ｄｉ］が生成され、前記暗号化された解読鍵、Ｅ１［Ｄｉ］は前記暗号化された信号へ付され、前記解読手段は、
ａ）前記暗号化された解読鍵、Ｅ１［Ｄｉ］を対応する解読鍵Ｄ１で解読して前記解読鍵、Ｄｉ、を回復する手段と、
ｂ）前記暗号化された信号を前記鍵、Ｄｉ、を用いて解読する手段と、
を更に備える、装置。
【請求項２３】
ａ）物その他の実体を走査して、前記物その他の実体の画像を表す第１の信号を発生する過程と、
ｂ）前記画像を識別カードの第１の部分の上にプリントする過程と、
ｃ）前記画像の表現を有し、少なくとも部分的に前記第１の信号から派生する第２の信号を発生し、暗号化する過程であって、この過程では
ｄ）前記第２の信号は公開鍵暗号化システムの暗号化鍵、Ｅｉ、を用いて暗号化され、暗号化された解読鍵Ｅ１［Ｄｉ］を作成するために、前記公開鍵暗号化システムの第２の暗号化鍵、Ｅ１、を用いて暗号化された、対応する解読鍵、Ｄｉが前記第２の信号に付される、過程と、
ｅ）前記暗号化された第２の信号と前記暗号化された解読鍵Ｅ１［Ｄｉ］とを符号化してこれらの符号化された表現を得て、前記符号化された表現を前記識別カードの第２の部分に組み込む過程と、
ｆ）前記第２の信号と前記暗号化された解読鍵Ｅ１［Ｄｉ］との前記符号化された表現を前記識別カードから読み出す過程と、
ｇ）前記暗号化された解読鍵Ｅ１［Ｄｉ］を、第２の対応する解読鍵、Ｄ１、を用いて復号し、解読鍵Ｄｉを得る過程と、
ｈ）前記解読鍵、Ｄｉ、を用いて前記暗号化された第２の信号を解読する過程と、
ｉ）前記解読された第２の信号を表示装置へ入力して、前記画像の前記表現を表示する過程と、
ｊ）前記第１の部分における前記画像を呈示する過程と、
を備える、物その他の実体を識別する方法。
【請求項２４】
ａ）物その他の実体を走査して、前記物その他の実体の画像を表す第１の信号を生ずる過程と、
ｂ）前記画像を識別カードの第１の部分の上にプリントする過程と、
ｃ）前記画像の表現を有し、少なくとも部分的に前記第１の信号から派生する第２の信号を発生し、暗号化する過程であって、この過程では、
ｄ）前記第２の信号は公開鍵暗号化システムの暗号化鍵、Ｅｉ、を用いて暗号化され、暗号化された解読鍵Ｅ１［Ｄｉ］を作成するために、第２の暗号化鍵、Ｅ１、を用いて暗号化された、対応する解読鍵、Ｄｉが前記第２の信号に付される、過程と、
ｅ）前記暗号化された第２の信号と前記暗号化された解読鍵Ｅ１［Ｄｉ］とを符号化してこれらの符号化された表現を得て、前記符号化された表現を前記識別カードの第２の部分に組み込む過程と、
を、備える、識別カードを製造する方法。
【請求項２５】
ａ）識別カードにより識別すべき物その他の実体の画像を表す第１の信号を発生するための走査手段と、
ｂ）前記走査手段に応答して前記画像を前記識別カードの第１の部分にプリントするプリント手段と、

ｃ）前記画像の表現を有し、少なくとも部分的に前記第１の信号から派生する第２の信号を発生する発生手段と、
ｄ）前記第２の信号を公開鍵暗号化システムの暗号化鍵、Ｅｉ、を用いて暗号化する暗号化手段と、
ｅ）第２の暗号化鍵、Ｅ１、を用いて対応する解読鍵、Ｄｉを暗号化して暗号化された解読鍵Ｅ１［Ｄｉ］を作成し、前記暗号化された解読鍵Ｅ１［Ｄｉ］を前記暗号化された第２の信号に付す追加手段と、
ｆ）前記暗号化された第２の信号と前記暗号化された解読鍵Ｅ１［Ｄｉ］を符号化して、符号化された表現を得る符号化手段と、
ｇ）前記符号化された表現を前記識別カードの第２の部分に組み込む組み込み手段と、
を備える識別カードを製造する装置。
【請求項２６】
識別すべき物その他の実体の画像を第１の部分の上に有し、公開鍵暗号化システムの暗号化鍵Ｅｉを用いて暗号化された信号の符号化された表現を第２の部分上に組み込んで有する識別カードの有効性を確認する装置であって、前記信号は前記画像の表現を有し、さらに前記公開鍵暗号化システムの対応する解読鍵、Ｄｉ、が暗号化鍵、Ｅ１、を用いて暗号化されて生成された、暗号化された解読鍵Ｅ１［Ｄｉ］が前記信号に付され、前記識別カードの有効性を確認する装置は、
ａ）前記符号化された表現を前記カードから読み出す、読み出し手段と、
ｂ）前記読み出し手段に応答して、前記符号化された表現を復号する復号手段と、
ｃ）前記復号手段に応答して、前記暗号化された解読鍵Ｅ１［Ｄｉ］と前記暗号化された信号とを解読し、前記画像の前記表現を得る解読手段と、
ｄ）前記解読手段に応答して、前記画像の前記表現を表示する表示手段と、
ｅ）前記第１の部分における前記画像を呈示する手段と、
を備える装置。
【請求項２７】
識別すべき物その他の実体の画像を第１の部分の上に有し、公開鍵暗号化システムの暗号化鍵Ｅｉを用いて暗号化された信号の符号化された表現を第２の部分上に組み込んで有する識別カードの有効性を確認する方法であって、前記信号は前記画像の表現を有し、さらに前記公開鍵暗号化システムの対応する解読鍵、Ｄｉ、が暗号化鍵、Ｅ１、を用いて暗号化されて生成された、暗号化された解読鍵Ｅ１［Ｄｉ］が前記信号に付され、前記識別カードの有効性を確認する方法は、
ａ）前記符号化された表現を前記カードから読み出す過程と、
ｂ）前記符号化された表現を復号する過程と、
ｃ）前記暗号化された解読鍵Ｅ１［Ｄｉ］を解読し、解読鍵Ｄｉを得る過程と、
ｄ）前記解読鍵Ｄｉを用いて前記暗号化された信号を解読し、前記画像の前記表現を得る過程と、
ｅ）前記画像の前記表現を表示装置に入力し、表示された画像を作成する過程と、
ｆ）前記第１の部分における前記画像を呈示する過程と、
を備える方法。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】
本発明は、物その他の実体の同一性または状態の証拠として機能する識別カードまたはそれに類似の物品に関するものである。更に詳しく言えば、本発明は、偽造または変造に対して高度の安全性を有する識別カードまたは類似の物品と、それらのカードの製造及び認証方法および装置に関するものである。
【０００２】
（この明細書で使用する「識別カード」という用語は、従業員を識別するために事業所により用いられる種類の識別バッジに類似する物を指すものであるが、文書、磁気ディスク

、ＣＤ等、または関連するデータと共に画像を記録でき、かつ識別すべき物その他の実体に関連させることができるその他の任意の適当な物を、ここで使用する「識別カード」という用語が限定なしに含むべきことが、本発明の意図に含まれる。）
物その他の実体の識別は少なくとも歴史のように古い問題である。年取って盲目になったイサクは、エサウの相続権に頼ってエサウをヤコブから見分けることに失敗し、ソロモンは赤子の母親を見つけるためにその赤子を殺すと脅かす事を余儀なくされた。歴史および物語は、所持している人を識別するために用いられる手紙、しるし、玉璽および暗証と、それらが失われ、または偽造された後に続く結末についての話に満ちている。
【０００３】
現代においては、この問題についての最もありふれた解決は、所有者の同一性と、所有者の通常はある特徴、状態、または属性を定める機能を果たす識別カードである。それの例は上記のように従業員バッジであり、最も一般的には運転免許証である。典型的には、そのような識別カードは公称所有者の写真と、文書形式の関連する情報とを含む。
【０００４】
識別カードなどは毎日の管理業務に有用であることが一般に判明しているが、それでも、識別カードは偽造または変造されることがあり、偽の識別文書を供給する目的の適度な規模の非合法事業が存在する。
【０００５】
識別についての高度の安全性が要求される用途に対しては、指紋、声紋、網膜模様、その他の個人的な特徴を認識するための効率的な技術が開発されている。そのようなシステムはシステムが知っている個人を一意に識別するのには極めて成功しているが、選択された個人を指紋のような身体的特徴で識別するデータベースへ接続せねばならない、典型的には可動ではない、極めて高性能の、極めて高価なセンサを必要とすることが欠点である。不法な変更に対する保護と更新を容易にするために、そのようなデータベースは一般に中央に設置せねばならない。したがって、それらの高度なシステムは区域を安全にするために接近を制約することに一般に限定される。
【０００６】
以上の説明から明らかなように、識別カードの最も一般的な用途は個人識別である。しかし、識別の目的は非常に広い種類の物その他の実体に拡張できる。したがって、特定の項目が検査された、または税関を通過した、あるいは特定の会社により製造された、ことを確証できることが望ましい。同様に、美術工芸品の出所、動物の血統または人の家系、あるいは植物が病原菌に犯されていないこと、の確実な証拠を持つことが望ましい。そのような用途、および当業者には明らかであるその他の用途は本発明の範囲内である。
【０００７】
おそらく有体物ではなくて情報に関連するからであろう、文書その他の態様の情報の識別すなわち認証が過去において、通常はある種の暗号化を使用することにより、多分成功裡に取り扱われてきた。したがって、１９８９年８月１日にパストー（Ｐａｓｔｏｒ）へ付与された米国特許第４，８５３，９６１号「信頼できる文書認証装置（Ｒｅｌｉａｂｌｅ　Ｄｏｃｕｍｅｎｔ　Ａｕｔｈｅｎｉｃａｔｉｏｎ　Ｓｙｓｔｅｍ）」には、公開鍵暗号方式を用いる暗号化により文書を認証する装置が開示されている。クラーク（Ｃｌａｒｋ）へ付与された米国特許第４，６３７，０５１号には、暗号化により認証される標識を持つ郵便料金計が開示されている。情報を認証するための暗号化のその他の多くの用途が当業者には知られていることであろう。
【０００８】
【発明が解決しようとする課題】
したがって、本発明の目的は、変造および偽造に対して安全である、物その他の実体を識別するための識別カードを得ることである。
【０００９】
【課題を解決するための手段】
識別カードを製造する方法および装置、およびその識別カードの有効性を確認する方法お

よび装置を提供する本発明により上記目的は達成され、かつ従来技術の諸欠点が克服される。識別カードを製造する装置は、識別すべき物その他の実体の画像を表す第１の信号を発生する走査器と、この走査器に応答して画像を識別カードの第１の部分の上にプリントするプリンタとを含む。この装置は、画像の表現を含み、第１の信号から少なくとも部分的に得られる第２の信号を暗号化する暗号化器と、第２の信号の暗号化の符号化された表現を識別カードの第２の部分に組み込む符号器とを更に含む。

【００１０】

そのようにして製造された識別カードの有効性を確認する装置は、第２の信号の符号化された表現をカードから読出す読出し器と、この読出し器の第２の信号の符号化された表現を復号する復号器と、復号された表現を解読する解読器と、第２の信号に組み込まれている画像の表現を表示する表示器とを含む。

【００１１】

本発明の方法に従って、識別すべき物が走査されて第１の信号を発生し、第１の信号により制御されるプリンタがその物の画像を識別カードの第１の部分の上にプリントする。第１の信号から少なくとも部分的に得られ、画像の表現を含む第２の信号を暗号化および符号化し、識別カードの第２の部分に組み込む。

【００１２】

ひとたび製造されたカードは、第２の信号の符号化された表現を識別カードから読出し、解読された第２の信号に従って表示装置を制御して、第２の信号に含まれている画像の表現を表示する。それから画像の表示された表現およびカードの第１の部分にプリントされた画像を物と比較してそれの同一性を確認する。

【００１３】

本発明の１つの面に従って、第１の信号は処理のためにデジタル信号へ変換される。

【００１４】

本発明の別の面に従って、第２の信号は圧縮された態様の第１の信号を含む。

【００１５】

（信号圧縮は当業者に周知であって、デジタル信号の場合には、伝送または処理せねばならないバイト数を減少し、しかもその信号により表されている情報のほとんど全てを依然として保持するために、信号に対する所定のアルゴリズムの適用を含む。）

本発明の別の面に従って、第２の信号は公開鍵暗号化システムに対する暗号化鍵E_iを用いて暗号化される。

【００１６】

本発明の別の面に従って、暗号化鍵、E_i、に対応する解読鍵、D_i、を、公開鍵暗号化システムに対する第２の暗号化鍵、E_1、で暗号化し、結果としての暗号化された解読鍵、$E_1[D_i]$を、第２の部分に組み込む前に、暗号化された第２の信号へ付す。

【００１７】

本発明の別の面に従って、暗号化された第２の信号を二次元バーコードとして識別カードの第２の部分にプリントする。

【００１８】

本発明の別の面に従って、識別カードの有効性を識別する装置は鍵E_1に対応する解読鍵、D_1を記憶し、暗号化された第２の信号の解読は、暗号化された解読鍵、$E_1[D_i]$を、解読鍵、D_1を用いて解読して解読鍵D_iを得、それから暗号化された第２の信号をその解読鍵を用いて解読する過程を含む。

【００１９】

本発明の別の面に従って、第２の信号はテキスト・メッセージを含み、そのテキスト・メッセージは識別カードにより識別すべき人が知っている暗証を含む。

【００２０】

本発明の更に別の面に従って、第２の信号はテキスト・メッセージを含み、そのテキスト・メッセージは識別カードの第１の部分に平文形式でプリントもされる。

【００２１】

したがって、本発明は、同一性を確認すべき物その他の実体と容易に比較でき、かつ偽造または変造に強い画像を含む識別カードを製造する方法および装置により、上記目的を達成するものであることがわかる。

【００２２】

【実施例】

図１は識別カードＣを製造するための装置１０の概略ブロック図を示す。識別カードが意図されている人（または物その他の実体）が通常のテレビカメラ１２により走査されて、その人の画像を表す第１の信号を発生する。それから、第１の信号をデジタル領域で処理するためにアナログーデジタル変換器１４によりデジタル形式へ変換することが好ましい。しかし、以下に説明する少なくとも信号圧縮技術および暗号化技術を、アナログ信号処理技術における当業者に周知の信号圧縮技術および信号暗号化技術を用いてアナログ領域において実施できる。

【００２３】

それから、第１の信号は圧縮モジュール１６へ入力され、そこで圧縮されて、識別カードに記憶せねばならないデータの量を減少する。

【００２４】

カードＣが現在知られている識別カード、運転免許症などとほぼ同じ形式を持つ場合には、現在の技術状態においてはデータ圧縮を必要とすることに注目すべきである。しかし、データ記憶技術における予測される改良により、または識別カードが高い容量の記憶媒体（たとえば、フロッピーディスク）を含むことができる用途においては、後で述べるように第１の信号を圧縮する必要がないが、完全な信号を処理できることも本発明の範囲内である。

【００２５】

データ圧縮アルゴリズム、とくにビデオ画像信号の圧縮に用いられるデータ圧縮アルゴリズム、は当業者に周知である。市販されているＪＰＥＧアルゴリズムとして知られているアルゴリズムを圧縮器１６に用いることが好ましい。圧縮器１６の動作の動作についてのこれ以上の説明は本発明の理解には不必要であると信ぜられる。

【００２６】

それから圧縮された第１の信号は暗号器２０へ入力されて、暗号化された第２の信号に含まれる。その暗号化された第２の信号は、後で説明するように、識別カードＣに組み込まれる。暗号器２０は周知のＲＳＡ方式のような公開鍵暗号方式のための暗号化鍵、E_i、を用いて第２の信号を暗号化することが好ましい。

【００２７】

それから暗号化された第２の信号は符号器モジュール２２によりある所定のフォーマットに従って符号化される。それは符号発生器２４を制御して符号化されて暗号化された第２の信号を識別カードＣの部分中に組み込ませる。

【００２８】

本発明の好適な実施例に従って、符号化された信号は、ニューヨーク所在のシンボル・テクノロジー・コーポレーション（Ｓｙｍｂｏｌ　Ｔｅｃｈｎｏｌｏｇｙ　Ｃｏｒｐｏｒａｔｉｏｎ）により開発されたＰＤＦ－４１７標準バーコードのような、二次元バーコードとして符号化される。しかし、暗号化された第２の信号は適当な任意のフォーマットへ符号化できる。たとえば、スマートカードまたは記憶カードに対して符号器２２およびコード発生器２４は符号化された第２の信号を適切にフォーマット化された２進データ・ブロックとして記憶できる。

【００２９】

符号化された第２の信号が二次元バーコードとして表される好適な実施例においては、バーコードは識別カードＣの裏ＣＢにプリントすることが好ましい。

【００３０】

本発明の好適な実施例においては、圧縮器モジュール１６と、暗号器モジュール２０と、符号器モジュール２２とはマイクロプロセッサにおけるソフトウエア・モジュールとして

実現される。そのマイクロプロセッサはインテル８０３８６型、またはそれと同等品、あるいはより高い性能のマイクロプロセッサであることが好ましい。

【００３１】

デジタル化された第１の信号はプリンタ２０へも入力される。そのプリンタは、人Ｏの画像を識別カードＣの表面ＣＦにプリントするために識別カードＣを製造する任意の適切な技術を使用できる。それから表面ＣＦと裏面ＣＢを組合わせ、ラミネータ３２により周知の技術を用いてラミネートして識別カードＣを製造する。

【００３２】

本発明の別の好適な実施例に従って、テキスト・メッセージを入力するためにテキスト入力部３０が用いられる。本発明の一実施例においては、テキスト・メッセージの少なくとも一部が圧縮された態様の第１の信号に組合わされて第２の信号を形成する。その第２の信号は暗号器モジュール２０により暗号化され、かつカードＣの表面ＣＦに平文テキストとしてプリントもされる。あるいは、テキスト・メッセージＴを、たとえば、制御キャラクタの削除により圧縮できる。それらのキャラクタは、テキスト・メッセージＴが第２の信号へ組み込まれる前に、テキストＴが回収された時に、所定のフォーマットに従って回復される。したがって、画像Ｉのようにテキスト・メッセージＴは、カードＣの表面ＣＦに人が認識できる形式で、および裏面ＣＢに符号化された形式でカードＣに具体化される。別の実施例においては、テキスト・メッセージは暗証Ｐを含むことができる。その暗証は暗号化され、かつ符号化されるが、表面ＣＦには平文でプリントされない。

【００３３】

本発明の好適な実施例においては、センター４０が暗号化鍵E_iを暗号器モジュール２０へ送る。識別カードＣの安全性を高くするために、鍵E_iを始終変更する。鍵E_iの安全度を最高にするためには、各カードＣを製造するたびに鍵を変更し、または第２の信号の種々の部分を暗号化するために異なる鍵を使用することもできる。

【００３４】

鍵E_iがしばしば変更される環境における第２の信号の暗号化を容易にするために、センター４０は暗号化された解読鍵E_1［D_i］を送って符号器モジュール２２により暗号化された第２の信号へ付させる。このように、下でわかるように、カードＣの有効性を確認する時に、E_1［D_i］を解読することにより必要な解読鍵D_iを得ることができる。

【００３５】

典型的には、暗号化鍵／解読鍵対E_1、D_1は装置１０が動作中はほぼ一定のままである。しかし、各種の組織のための識別カードＣを製造するために装置１０が使用される用途においては、種々の鍵対E_1、D_1を種々の組織のために使用できる。

【００３６】

次に、識別カードＣの有効性を確認するための装置５０が示されている図２を参照する。カードＣの裏面ＣＢが、適切な二次元バーコードを走査できる性能を有するバーコード走査器５２により走査される。本発明の好適な実施例においては、解読鍵D_iを得るために暗号化されている解読鍵E_1［D_i］を解読するために用いられる解読鍵D_1を解読器５８が保存する。それから鍵D_iを用いて、カードの裏面ＣＢから走査される復号された信号を解読する。

【００３７】

鍵D_1はセンター４０から解読器５８により得られる。典型的には、上記のように、装置５０の動作中は鍵D_1は一定に保たれ、装置５０とセンター４０の間の直接通信リンクは不必要であり、鍵D_1は任意の便利なやり方で送ることができる。しかし、識別カードＣが所定の満期期限を有するある用途においては、その満期期限の経過後は鍵D_1を変更することが望ましく、そのような満期期限が十分にしばしば生ずるものとすると、センター４０への直接通信リンクを装置５０に含むことができる。

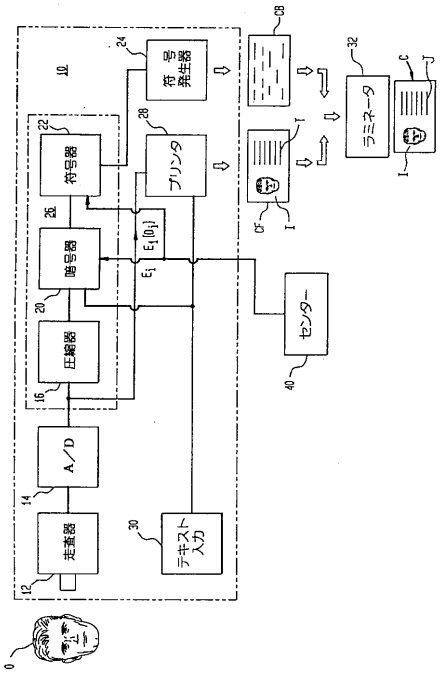
【００３８】

それから、解読された走査信号は装置１０において使用される圧縮アルゴリズムに対して相補的なアルゴリズムにより、通常のやり方で拡張される。本発明の理解のためにはその

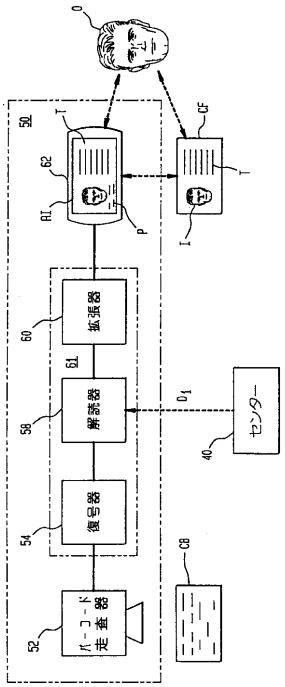
やり方を説明する必要はない。
【００３９】
本発明の好適な実施例においては、復号器モジュール５４と、解読器モジュール５８と、拡張器モジュール６０とをマイクロプロセッサ６１においてソフトウエア・モジュールとして実現できる。
【００４０】
解読され、拡張された信号がそれから通常の表示装置６２により表示される。表示装置は画像Ｔの表現ＲＩと、カードの裏面ＣＢから走査される暗号化された第２の信号に含まれていたテキスト・メッセージＴとを含む。表示装置は暗証Ｐ１含む。その暗証はカードＣを所持することを許されている人Ｏに知られているが、上記のようにカードＣには含まれない。カードの有効性を確認するために、画像Ｉがそれの表現ＲＩと比較され、カードＣにプリントされていて、表示装置６２に示されているテキスト・メッセージＴが比較される。圧縮により表現ＲＩが画像Ｉに対して多少劣化させられることに注目すべきである。しかし、上記ＪＰＥＧアルゴリズムを使用すると、人の顔の画像の十分に正確な表現をデータの約１０００バイトとして符号化でき、ほぼ従来の札入れ寸法のカードの裏面に約６．３５×４．４５ｃｍ（約２．５０×１．７５インチ）の区域に上記ＰＤＦ－４１７二次元バーコードを用いてプリントできる。もちろん、上記のように、記憶装置技術の改良と、より大きいデータ記憶容量を有する媒体の使用との少なくとも一方により、識別カードＣの表現ＲＩの実施例を画像Ｉへ任意に近づけることができる。
【００４１】
暗証Ｐを含む実施例においては、暗証Ｐは表示装置６２の上に示されるが、カードの表面ＣＦにはもちろんプリントされない。暗証ＰはカードＣを所持する事を許されている人Ｏは知っている。画像Ｉと、カードの表面ＣＦにプリントされているテキスト・メッセージＴを、表示装置６２に示されている表現ＲＩとテキスト・メッセージＴと比較することにより有効であることが確認されると、カードＣを所持している人Ｏと画像Ｉを比較し、かつ暗証Ｐを知っているかどうかその人Ｏを試すことにより、その人を確認できる。それからテキスト・メッセージＴはその人Ｏの同一性を確認し、かつその人Ｏの状態または特徴も確認できる。
【図面の簡単な説明】
【図１】本発明に従って識別カードを製造する装置の概略ブロック図である。
【図２】本発明に従って製造された識別カードの有効性を確認する装置の概略ブロック図である。
【符号の説明】
１０　識別カードを製造する装置
１２　走査器
１４　アナログーデジタル変換器
１６　圧縮器
２０　暗号器
２２　符号器
２４　符号発生器
２８　プリンタ
３０　テキスト入力部
３２　ラミネータ
４６　センター
５０　識別カードの有効性を確認する装置
５２　バーコード走査器
５４　復号器
５８　解読器
６０　拡張器
６１　マイクロプロセッサ

６２　表示装置

【図１】


10
12
走査器
14
A/D
16
圧縮器
18
暗号器
20
符号器
22
符号発生器
24
プリンタ
28
テキスト入力
30
ラミネータ
32
センター
40
CB
CF
C
I
T
O

【図２】


50
52
バーコード走査器
54
復号器
56
解読器
58
拡張器
60
62
センター
40
CB
CF
C
I
T
O

フロントページの続き

(72)発明者　ジェームズ、アール、マーカス
アメリカ合衆国コネチカット州、ノーウォーク、ブロード、コート、１

合議体
審判長　吉岡　浩
審判官　橋本　正弘
審判官　彦田　克文

(56)参考文献　特開昭５８－１９２１９０（ＪＰ，Ａ）
特開昭６２－２４５７４７（ＪＰ，Ａ）
実開昭６１－５３１７７（ＪＰ，Ｕ）
一松　信　監修：“データ保護と暗号化の研究”，日本経済新聞社，１９８３．７．２９，1版１刷，ｐ．５９－６４“３　ＭＩＸ方式による暗号系”