METHOD AND SYSTEM FOR AUTHENTICATING OBJECTS

The present invention provides a method of authenticating objects (10), comprising embedding a unique plurality of randomly-located, irregularly shaped, non-interconnected, electrically conductive regions (18, 21) within the surface of said object to thereby provide a unique electrically readable signature correlated to the genuine document; providing a unique identifier on the object; providing means (20, 22) for electrically reading said unique signature and digitally storing the signature in connection with the unique identifier for that object, and when an object is to be authenticated, obtaining a digitized record of the signature and comparing it to the stored signature.
FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AT</td>
<td>Austria</td>
<td>GB</td>
<td>United Kingdom</td>
<td>MR</td>
<td>Mauritania</td>
</tr>
<tr>
<td>AU</td>
<td>Australia</td>
<td>GE</td>
<td>Georgia</td>
<td>MW</td>
<td>Malawi</td>
</tr>
<tr>
<td>BB</td>
<td>Barbados</td>
<td>GN</td>
<td>Guinea</td>
<td>NE</td>
<td>Niger</td>
</tr>
<tr>
<td>BE</td>
<td>Belgium</td>
<td>GR</td>
<td>Greece</td>
<td>NL</td>
<td>Netherlands</td>
</tr>
<tr>
<td>BF</td>
<td>Burkina Faso</td>
<td>HU</td>
<td>Hungary</td>
<td>NO</td>
<td>Norway</td>
</tr>
<tr>
<td>BG</td>
<td>Bulgaria</td>
<td>IE</td>
<td>Ireland</td>
<td>NZ</td>
<td>New Zealand</td>
</tr>
<tr>
<td>BJ</td>
<td>Benin</td>
<td>IT</td>
<td>Italy</td>
<td>PL</td>
<td>Poland</td>
</tr>
<tr>
<td>BR</td>
<td>Brazil</td>
<td>JP</td>
<td>Japan</td>
<td>PT</td>
<td>Portugal</td>
</tr>
<tr>
<td>BY</td>
<td>Belarus</td>
<td>KE</td>
<td>Kenya</td>
<td>RO</td>
<td>Romania</td>
</tr>
<tr>
<td>CA</td>
<td>Canada</td>
<td>KG</td>
<td>Kyrgyzstan</td>
<td>RU</td>
<td>Russian Federation</td>
</tr>
<tr>
<td>CF</td>
<td>Central African Republic</td>
<td>KP</td>
<td>Democratic People's Republic of Korea</td>
<td>SD</td>
<td>Sudan</td>
</tr>
<tr>
<td>CG</td>
<td>Congo</td>
<td>CN</td>
<td>China</td>
<td>SE</td>
<td>Sweden</td>
</tr>
<tr>
<td>CH</td>
<td>Switzerland</td>
<td>CS</td>
<td>Czechoslovakia</td>
<td>SI</td>
<td>Slovenia</td>
</tr>
<tr>
<td>CI</td>
<td>Côte d'Ivoire</td>
<td>CM</td>
<td>Cameroon</td>
<td>SK</td>
<td>Slovakia</td>
</tr>
<tr>
<td>CM</td>
<td>Cameroon</td>
<td>CN</td>
<td>China</td>
<td>SN</td>
<td>Senegal</td>
</tr>
<tr>
<td>CS</td>
<td>Czech Republic</td>
<td>DK</td>
<td>Denmark</td>
<td>TD</td>
<td>Chad</td>
</tr>
<tr>
<td>CZ</td>
<td>Czech Republic</td>
<td>ES</td>
<td>Spain</td>
<td>TG</td>
<td>Togo</td>
</tr>
<tr>
<td>DE</td>
<td>Germany</td>
<td>FI</td>
<td>Finland</td>
<td>TJ</td>
<td>Tajikistan</td>
</tr>
<tr>
<td>FR</td>
<td>France</td>
<td>FR</td>
<td>France</td>
<td>TT</td>
<td>Trinidad and Tobago</td>
</tr>
<tr>
<td>GA</td>
<td>Gabon</td>
<td>GB</td>
<td>United Kingdom</td>
<td>UA</td>
<td>Ukraine</td>
</tr>
<tr>
<td>MN</td>
<td>Mongolia</td>
<td>MR</td>
<td>Mauritania</td>
<td>US</td>
<td>United States of America</td>
</tr>
<tr>
<td>MG</td>
<td>Madagascar</td>
<td>MW</td>
<td>Malawi</td>
<td>UZ</td>
<td>Uzbekistan</td>
</tr>
<tr>
<td>MN</td>
<td>Mongolia</td>
<td>NE</td>
<td>Niger</td>
<td>VN</td>
<td>Viet Nam</td>
</tr>
</tbody>
</table>
METHOD AND SYSTEM FOR AUTHENTICATING OBJECTS

Technical Field

The invention relates to the field of security sensitive documents and cards such as identity cards, credit cards and debit cards. More particularly the invention relates to a method of, and system for, authenticating such cards and detecting counterfeit cards or other documents.

Background Art

Huge financial losses occur regularly as a result of the counterfeiting of security sensitive documents. For example, credit card fraud resulting from the production of counterfeit credit cards and the fraudulent use of such cards to acquire goods is a huge cost to credit card companies. Such companies have taken steps such as the incorporation of holograms into credit cards to make the manufacture of counterfeits more difficult, but sophisticated criminals are able to duplicate such holograms, sometimes by infiltrating the card manufacturing facility. There remains therefore a need for reliable methods for authenticating security sensitive objects or documents such as credit cards.

Disclosure of Invention

The present invention provides a method of authenticating objects, comprising embedding a randomly-located plurality of irregularly shaped, non-interconnected, electrically conductive regions within the surface of the object to thereby provide a unique electrically readable signature correlated to the genuine document; providing a unique identifier on the object; and providing means for electrically reading the unique signature and digitally storing the signature in connection with the unique identifier for that object, whereby when an object is to be authenticated, the signature of the object can be read and compared to the stored signature correlating to the identifier on the object.
According to one aspect of the invention the means for reading the unique electrical signature comprises an object reader, further comprising:

(i) a drive electrode and a sense electrode;
(ii) mounting means for positioning the electrodes adjacent an object reading path;
(iii) a voltage source electrically connected to the drive electrode; and,
(iv) detector means electrically connected to the sense electrode for detecting varying voltage amplitudes capacitively coupled between the drive and sense electrodes by the embedded regions during movement of the object along the path.

The present invention further provides a verifiable object comprising a plurality of randomly-located, irregularly shaped, non-interconnected, electrically conductive regions embedded within the surface of the object, and a unique identifier provided on the object.

The present invention further provides an object authentication device comprising:

(i) a drive electrode and a sense electrode;
(ii) mounting means for positioning the electrodes adjacent an object reading path;
(iii) a voltage source electrically connected to the drive electrode; and,
(iv) detector means electrically connected to the sense electrode for detecting varying voltage amplitudes capacitively coupled between the drive and sense electrodes by the embedded regions during movement of the object along the path.

The present invention further provides an object verification system, comprising:

(a) an object having a plurality of randomly-located irregularly shaped, non-interconnected, electri-
cally conductive regions embedded within the surface of the object, and a unique identifier;
(b) means for generating a digital signature corresponding to said object comprising:
(i) a drive electrode and a sense electrode;
(ii) mounting means for positioning the electrodes adjacent an object reading path;
(iii) a voltage source electrically connected to the drive electrode; and,
(iv) detector means electrically connected to the sense electrode for detecting varying voltage amplitudes capacitively coupled between the drive and sense electrodes by the embedded regions during movement of the object along the path.
c) means for storing the signature correlated to the unique identifier; and
d) means for comparing the stored signature correlated to the unique identifier to a second signature.

The present invention further provides a method of encoding a card with a secure identification verification means and subsequently verifying the identification means, comprising the steps of:
(a) randomly embedding a plurality of irregularly shaped, non-interconnected, electrically conductive regions within the surface of the card;
(b) moving the card along a card reading path;
(c) capacitively coupling in sequence a plurality of said conductive regions to first and second electrodes mounted at a location on the path, as the card progressively moves along the reading path;
(d) detecting the voltage amplitudes capacitively coupled between the electrodes and the sequential embedded regions;
(e) storing, as the identifier, a replica of the voltage amplitudes detected at the selected distances;

(f) subsequently verifying the identification means for a subject card by:

(i) repeating steps (b), (c) and (d); and

(ii) comparing the voltage amplitudes detected at during step (f)(i) with the stored replica.

Brief Description of Drawings

In drawings which illustrate a preferred embodiment of the invention:

Fig. 1 is a top view of a credit card passing through a card guide and card reader according to the invention;

Fig. 2 is a cross-sectional view showing a portion of the card and reader illustrated in Fig. 1;

Fig. 3 is a schematic diagram illustrating the equivalent electrical circuit formed by the card and reader illustrated in Fig. 2;

Fig. 4 is a chart illustrating a signature waveform produced by the card reader and card of the invention;

Fig. 5 is a partial elevation of a second embodiment of the card reader of the invention having an array of four electrodes, with the conductive areas of the credit card super-imposed;

Fig. 6 is a schematic diagram illustrating a third embodiment of the card reader of the invention having an array of nine electrodes;

Fig. 7 is a partial elevation of the second embodiment of the card reader of the invention shown in Fig. 5 having an array of four electrodes, with cross-sectional views taken along either central axis; and

Fig. 8 is a block diagram illustrating a circuit used with the embodiment of the card reader of the invention having an array of four electrodes.
Best Mode(s) For Carrying Out the Invention

As illustrated in Fig. 1, a credit card 10 is in the process of being "swiped" through a plastic card guide 12, which is provided with a standard magnetic stripe sensor 14 and a capacitive sensor array 16 according to the invention.

The plastic credit card 10 of the invention has embedded therein planar conductive regions 18, 21 (Fig. 2) of random shapes, sizes, orientations and depth, but mostly arranged with their planar surfaces generally parallel to the broad surfaces of the card. Such a card may be manufactured in a number of ways. For example, randomly sized flakes of a conductive metal, such as aluminum foil, may be mixed into the molten plastic and the mixture rolled out into flat sheets to form cards. Alternatively, a sheet of plastic may be coated with a conductive metal, and the coating etched into random islands. The coated sheet would then be sandwiched between mylar layers. Similarly the metal coating could be applied to a mylar layer, etched into the random shapes and then sandwiched by bonding the mylar layer to a plastic sheet.

With reference to Figures 2 and 3, card reader 16 is provided with dielectric-covered electrodes 20, 22 which come into sliding contact with the surface of card 10. An AC voltage 15 is applied to electrode 20 through conductor 24. The AC voltage is thus capacitively coupled to a conductive region 18 under electrode 20. If electrode 22 also overlaps the same conductive region 18, the AC voltage is capacitively coupled to electrode 22. The AC voltage measured at V (Fig. 2, 3) depends on the values of the coupling capacitance $C_{xa}$ between the electrode 20 and conductive region 18, and the value of the coupling capacitance $C_{av}$ between the conductive region 18 and the electrode 22, as shown in Fig. 3. To measure the voltage at V, a resistor $R_g$ provides an input impedance off the buffer amplifier connected to the electrode.
As card 10 is slid past the electrodes 20, 22 in the direction of arrow B, the measured AC voltage amplitude \( V \) changes as different conductive regions pass under the electrodes 20, 22, producing a unique amplitude \( Y \) vs. travel distance \( X \) waveform 30 for a given card, illustrated in Fig. 4., where line A indicates the DC or average amplitude, the Y-axis is the AC amplitude and the X-axis is the distance along the card. This signature waveform 30 may be recorded digitally at specified points along the card as determined by another capacitively or magnetically coded track. This digital record may then be stored as a template or signature associated with the card number stored on the standard magnetic strip.

To verify or authenticate a card, the card signature is read in the same way that the template or signature was stored and is compared to the stored signature associated with the card number. To produce a suitable reading, the card 10 must be swiped through the card reader 12 at the proper height by sliding the bottom edge of the card through the appropriate card guide. If the comparison of the reader output to the stored template satisfies preset criteria (such as the Normalized Correlation Coefficient described in more detail below), then the card is considered genuine.

Fig. 5 illustrates an embodiment of the invention which utilizes four dielectric-covered electrodes X, V, H, D on the card-contacting surface of card reader 16. As in the two-electrode embodiment, an AC voltage is applied to electrode X and AC voltage amplitudes are measured at electrodes V, H, D as the card 10, having planar conductive regions 21 of random shapes, sizes, orientations and depth, but mostly arranged with their planar surfaces generally parallel to the broad surfaces of the card, moves past in direction B. The three recorded signatures are then stored as previously described to verify the card at a later date. A further embodiment using nine electrodes is illustrated.
in Fig. 6 whereby eight signatures can be recorded per card to provide a greater degree of security.

Fig. 7 illustrates a preferred construction of the sensing electrodes in the embodiment of the invention which utilizes four dielectric-covered sensing electrodes X, V, H, D on the card-contacting surface of card reader 16. The electrode array is fabricated on a ceramic substrate 40. The surface of the electrodes forms a flat area, with the surrounding area curved convexly such that the electrode array is in close contact with the card, and the card can slide smoothly past the electrode array. The surface dielectric layer is shown at 42. A grounded guard ring 44 is provided with a guard ring ground connection 46.

Fig. 8 illustrates by way of a block diagram the circuit used in the embodiment of the invention which utilizes four dielectric-covered sensing electrodes X, V, H, D on the card-contacting surface of card reader 16. A sine wave 240 Khz oscillator 50, with a 4 volt peak amplitude applies the AC voltage to electrode X. The electrodes H, V, D are all connected to similar signal conditioning circuits 52, consisting of a high-input-impedance buffer 54, followed by a high pass amplifier 56 and detector 58, then a low pass filter 60. The high-input-impedance buffer 54 is necessary since the electrode areas must be small to get sufficient resolution of the card signature. Therefore the coupling capacitance must also be small and thus provide a high impedance signal source. The AC signal from the buffer is then amplified, detected and low pass filtered. The result is a voltage proportional to the amplitude of the AC voltage at the sensing electrode.

The conditioned signals from electrodes H, V, D are each connected to an input of a Sample and Hold circuit 62, operated by a clock signal 64 derived from the magnetic data stripe sensor, which for a specific magnetic data record specifies fixed locations along the card as signal-sampling points. The sampled signals from the H, V, D
channels are fed to three inputs 66, 67, 68 of an Analog to Digital Converter 70. The Analog to Digital Converter 70, under the control of microcomputer 72, converts and stores the signals as card signatures.

The stored card signatures are saved as templates for a referenced card number when the card is put into service. In use, the recorded signatures are sent to the data center where these are compared with the stored templates for similarity of waveforms by calculating the Normalized Correlation Coefficient ("NCC") of the AC component of the Template Vector with the AC component of the signature vector for each of the signal channels. If each of the NCC's are above a specified level, say 0.900 (the maximum being 1.0) then the card is deemed acceptable. Otherwise the card is rejected.

For magnetic data clock sampled card signatures, any change in the magnetic data recording results in a different card signature, which may or may not be desirable. Where the magnetic data is changed periodically, a dedicated magnetic clock channel or a capacitive clock channel would be desirable. In the 3 signature prototype tested, using 64 samples 4 bit accuracy per sample was obtained. This results in 768 bits of security data pattern. In production, 512 bits per signature and 8 signatures per card could be used, resulting in 4096 security bits which is very difficult to duplicate.

The NCC's are calculated as follows. An analog wave-form such as the voltage signal from the capacitive sensor circuits may be sampled at specified points in time, or as is the case here, at specified points along the card. A set of N values $A_0$, $A_1$, ..., $A_N$ is thereby obtained, which can be regarded as a data vector. The data vector can be normalized, i.e. reduced to a magnitude of 1 by defining the normalized vector

$$D_i^* = \frac{D_i}{\sqrt{\sum_{i>1}^N D_i^2}}$$
where $D_i^*$ are the components of the normalized vector and $D_i$ the components of the data vector. If the data vectors are similar, their corresponding normalized vectors have equal or near equal components. A good mathematical measure of the similarity of vector components is the dot product. Therefore the Normalized Correlation Coefficient is defined as follows:

$$NCC = \sum_i \frac{D_i^* \sqrt{\sum_{j=1}^{N} D_{ij}^2 \cdot D_{i} \sqrt{\sum_{j=1}^{N} D_{jj}^2}}}$$

$$= \frac{\vec{D}_1 \cdot \vec{D}_2}{\sqrt{\vec{D}_1 \cdot \vec{D}_1} \cdot \sqrt{\vec{D}_2 \cdot \vec{D}_2}}$$

The maximum value of the NCC is 1 if $D_1 = D_2$ and the minimum value is -1 if $D_1 = -D_2$. Thus the NCC will always be between -1 and 1.

The AC component of a data vector can be used for the calculation of the NCC with the following advantages: a) the DC part of the signal varies with amplifier offset voltages which change with temperature and supply voltages. The AC component is largely unaffected by these changes. The shape of the AC component of the data vector, or alternatively a normalized data vector remains constant. b) the AC data vector gives sharper correlation characteristics.

The comparison of the card signature read from the card to be authenticated to the stored template in the present invention is preferably achieved by calculating the Normalized Correlation Coefficient. The data vector $\vec{T} = T_i$, $i=1,\ldots,n$ is the recorded set of data points for a specific card, and has been referred to as the "template". Where a card number XXXXXXX is presented, the template for that card number is retrieved from memory and correlated with the data vector $\vec{D} = D_i$, $i=1,\ldots,n$ read from that
card. The NCC is calculated and if less than a predetermined value, the card is rejected.

The AC component of $\mathbf{D}$ is

$$\mathbf{D} - \langle \mathbf{D} \rangle = (D_i - \frac{\sum D_k}{N}) \text{ for } i = 1, \ldots, N$$

The AC component of $\mathbf{T}$ is

$$\mathbf{T} - \langle \mathbf{T} \rangle = (T_j - \frac{\sum T_k}{N}) \text{ for } j = 1, \ldots, N$$

Therefore the NCC of the AC components of the data vectors is given by:

$$\begin{align*}
(\mathbf{D} - \langle \mathbf{D} \rangle) \cdot (\mathbf{T} - \langle \mathbf{T} \rangle) & = \mathbf{D} \cdot \mathbf{T} - \langle \mathbf{D} \rangle \cdot \langle \mathbf{T} \rangle + \langle \mathbf{D} \rangle \cdot \langle \mathbf{T} \rangle \\
& = \mathbf{D} \cdot \mathbf{T} - \langle \mathbf{D} \rangle \cdot \langle \mathbf{T} \rangle \\
& = \sum_i D_i T_i - \frac{\sum_i D_i \sum_j T_j}{N}
\end{align*}$$

$$|\mathbf{D} - \langle \mathbf{D} \rangle| = \left[ \sum_i D_i^2 - \left( \frac{\sum_i D_i}{N} \right)^2 \right]^{1/2}$$

$$|\mathbf{T} - \langle \mathbf{T} \rangle| = \left[ \sum_i T_i^2 - \left( \frac{\sum_i T_i}{N} \right)^2 \right]^{1/2}$$

$$\begin{align*}
\text{NCC} & = \frac{(\mathbf{D} - \langle \mathbf{D} \rangle) \cdot (\mathbf{T} - \langle \mathbf{T} \rangle)}{|\mathbf{D} - \langle \mathbf{D} \rangle| \cdot |\mathbf{T} - \langle \mathbf{T} \rangle|} \\
& = \frac{\sum_i D_i T_i - \sum_i D_i \cdot \sum_j T_j / N}{\left[ \sum_i D_i^2 - (\sum_i D_i/N)^2 \right]^{1/2} \left[ \sum_i T_i^2 - (\sum_i T_i/N)^2 \right]^{1/2}}
\end{align*}$$

As will be apparent to those skilled in the art in the light of the foregoing disclosure, many alterations and modifications are possible in the practice of this invention without departing from the spirit or scope thereof. The invention is not restricted to credit card verification but has application wherever the authenticity of a document is to be established, such as high security entry control, security for negotiable instruments or large bank notes, identification cards and passports. Accordingly, the scope of the invention is to be construed in accordance with the substance defined by the following
claims.
WHAT IS CLAIMED IS:

1. An object verification system, comprising:
   (a) an object, comprising a plurality of randomly-located, non-interconnected, electrically conduc-
       tive regions embedded within said object, and provided with a unique identifier;
   (b) means for generating a digital signature corre-
       sponding to said object comprising:
       (i) a drive electrode and a sense electrode;
       (ii) mounting means for positioning said elec-
            trodes adjacent an object reading path;
       (iii) an AC voltage source electrically connected 
            to said drive electrode; and,
       (iv) detector means electrically connected to 
            said sense electrode for detecting varying 
            voltage amplitudes as a consequence of 
            capacitive coupling between said drive and 
            sense electrodes by said embedded regions 
            during movement of said object along said 
            path.
   (c) means for storing said digital signature corre-
       lated to said unique identifier; and
   (d) means for comparing said stored signature corre-
       lated to said unique identifier to a second digital 
       signature.

2. The system of claim 1 wherein said object is a card.

3. The system of claim 1 wherein said means for generat-
   ing a digital signature comprises a plurality of sense 
   electrodes, and said detector means is electrically con-
   nected to said plurality of sense electrodes for detecting 
   varying voltage amplitudes capacitively coupled between 
   said drive and each said sense electrodes by said embedded 
   regions during movement of said object along said path.
4. A system as defined in Claim 1, wherein said embedded regions are irregularly shaped.

5. A system as defined in Claim 1, wherein
   (a) said object has planar surfaces; and,
   (b) said embedded regions comprise planar surfaces oriented substantially parallel to said planar surfaces of said object.

6. A method of encoding a card with a unique identifier and subsequently verifying said identifier, comprising the steps of:
   (a) embedding a plurality of irregularly shaped, non-interconnected, electrically conductive regions within said card;
   (b) moving said card along a card reading path;
   (c) during said moving step:
      (i) applying a voltage to said card at one point on said path, via an electrode in contact with card surface;
      (ii) at another point on said path, via an electrode detecting voltage amplitudes capacitively coupled between said points by said embedded regions;
   (d) storing, as said identifier, a replica of said voltage amplitudes detected at said points;
   (e) subsequently verifying said identifier by:
      (i) repeating steps (b) and (c);
      (ii) comparing said voltage amplitudes detected at said other point on said path during step (e)(i) with said stored replica;
      (iii) declaring said card valid if said compared values match one another within a predefined range; and,
      (iv) declaring said card invalid if said compared values do not match one another within said predefined range.
7. A method as defined in Claim 6, further comprising:
   (a) during step 6(c)(ii), simultaneously detecting, at one or more additional points on said path, voltage amplitudes capacitively coupled between said one point and said additional point(s) by said embedded regions;
   (b) during step 6(d), additionally storing, as said identifier, replicas of said voltage amplitudes detected at said points during said step 11(a); and,
   (c) during said subsequent verification step, simultaneously
      (i) repeating step 6(c)(ii) at each of said additional points;
      (ii) comparing said voltage amplitudes detected at said selected distances during step 11(a) with said replicas stored during step 11(b);
      (iii) declaring said card valid if said compared values match one another within a predefined range; and,
      (iv) declaring said card invalid if said compared values do not match one another within said predefined range.

8. A method as defined in Claim 7, wherein said embedded regions have irregular sizes.

9. A method as defined in Claim 8, wherein said embedded regions are located at irregular depths within said card.

10. A method as defined in Claim 9, wherein said irregular shapes are substantially planar.

11. A method as defined in Claim 10, wherein:
    (a) said card has planar surfaces; and,
(b) said embedded regions are oriented substantially parallel to said card surfaces.

12. A method as defined in Claim 11, wherein said embedded regions have different irregular shapes.

13. A method as defined in Claim 12, wherein said embedded regions have different irregular sizes.

14. A method as defined in Claim 13, wherein said embedded regions are located at different irregular depths within said card.

15. A method of authenticating an object, comprising:
   i) embedding a randomly-located plurality of irregularly shaped, non-interconnected, electrically conductive regions within the surface of said object to thereby provide a unique electrically readable signature correlated to said object;
   ii) providing a unique identifier associated with said object;
   iii) electrically reading said unique signature and digitally storing said signature in connection with said unique identifier for said object;
   iv) electrically reading said unique signature of an unverified object to be authenticated in relation to said unique identifier; and
   v) comparing said unique signature of said unverified object to said stored signature correlating to said unique identifier.

16. A verifiable object comprising a plurality of randomly-located, irregularly shaped, non-interconnected, electrically conductive regions embedded within the surface of said object, and a unique identifier provided in association with said object.
17. The object of claim 16 wherein said unique identifier is an alphanumeric number stored on said object.

18. The object of claim 16 wherein said object is a credit card.
<table>
<thead>
<tr>
<th></th>
<th>40</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>42</td>
<td>44</td>
<td>46</td>
</tr>
</tbody>
</table>

**FIG. 6**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$D_{LT}$</td>
<td>$V_T$</td>
<td>$D_{RT}$</td>
</tr>
<tr>
<td>$H_L$</td>
<td>$X$</td>
<td>$H_R$</td>
</tr>
<tr>
<td>$D_{LB}$</td>
<td>$V_B$</td>
<td>$D_{RB}$</td>
</tr>
</tbody>
</table>

**FIG. 7A**

**FIG. 7B**

**FIG. 7C**
**INTERNATIONAL SEARCH REPORT**

**A. CLASSIFICATION OF SUBJECT MATTER**

| IPC | G06K19/10 | G06K7/08 |

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)

| IPC | G06K |

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US,A,4 218 674 (BROSW JORGEN ET AL) 19 August 1980</td>
<td>15-18</td>
</tr>
<tr>
<td>Y</td>
<td>see column 3, line 50 - column 11, line 68; figures 1-10</td>
<td>1,2,4-6</td>
</tr>
<tr>
<td>Y</td>
<td>DE,A,32 36 374 (BBC BROWN BOVERI &amp; CIE) 5 April 1984 see the whole document</td>
<td>1,2,4-6</td>
</tr>
<tr>
<td>X</td>
<td>US,A,4 527 051 (STENZEL GERHARD) 2 July 1985 see column 3, line 52 - column 8, line 15; figures 1,2</td>
<td>15-18</td>
</tr>
<tr>
<td>A</td>
<td>see column 3, line 52 - column 8, line 15; figures 1,2</td>
<td>1,2,4-6</td>
</tr>
<tr>
<td>X</td>
<td>US,A,3 636 318 (LINDSTROM GUNNAR ET AL) 18 January 1972 see the whole document</td>
<td>15-18</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of box C. Patent family members are listed in annex.

"A" document defining the general state of the art which is not considered to be of particular relevance

"B" earlier document 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 document 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**

13 July 1995

**Date of mailing of the international search report**

03.08.95

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Facs (+31-70) 340-2016

Authorized officer

Gysen, L
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>BE-A- 845935</td>
<td>31-12-76</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CH-A- 607168</td>
<td>30-11-78</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE-A- 2635795</td>
<td>17-03-77</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FR-A- 2324060</td>
<td>08-04-77</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP-A- 52033444</td>
<td>14-03-77</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NL-A- 7610007</td>
<td>11-03-77</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SE-A- 7609944</td>
<td>10-03-77</td>
</tr>
<tr>
<td>DE-A-3236374</td>
<td>05-04-84</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE-C- 2858266</td>
<td>29-08-91</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US-A- 4982073</td>
<td>01-01-91</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FR-A- 2013362</td>
<td>03-04-70</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GB-A- 1274238</td>
<td>17-05-72</td>
</tr>
</tbody>
</table>