Abstract: A method for authenticity verification. The method can comprise conducting a transaction between first and second parties, the parties being respectively located at first and second locations remote one-another, the outcome of the transaction being the transfer of title to goods and/or services from the first party to the second party. Data describing a value entitlement token of the second party can be captured to create a signature for the value entitlement token, the signature being based upon an intrinsic property of the value entitlement token. The signature can be transmitted from the second party to a third party which can compare the signature to a database of stored signatures. A validation result indicating whether the value entitlement token corresponds to a value entitlement token signature in the database can be transmitted from the third party to the first party.
AUTHENTICITY VERIFICATION FIELD

The present invention relates to authenticity verification, and in particular to enhanced authenticity verification for situations where entitlement to value, goods or services passes at a location remote in time or space from a delivery point for the value, goods or services, for example with reference to remote card-based transactions.

In many e-commerce and similar situations, transfer of entitlement to value, goods or services is often performed at a location remote from an entity which administers the value or provides the goods or services. In such transactions, payment for the entitlement to the value, goods or services is often made from the remote location. It is therefore desirable that such transactions are subjected to a high level of security, to minimise the risks of fraud on the part of both the end user and the service provider or goods supplier.

To address such issues of remote access to entitlement to value, goods or services, systems can be implemented such as security mechanisms for paying for items in a remote access system such as an on-line access or ordering facility. In these circumstances, a numerical indicator of authority to transfer value from the purchaser to the supplier may be given. Typically this may include a credit or debit card number, and may be supplemented by a numeric PIN (Personal Identification Number) or alphanumeric password. This system does not however offer a guarantee that the purchaser actually has possession of the credit or debit card, although restrictions on a delivery address based on an invoicing address for the credit or debit card may be used as a further safeguard.
SUMMARY

The present invention has been made, at least in part, in consideration of problems and drawbacks of conventional systems.

The present invention has at least in part resulted from the inventor's work on applying authentication techniques using tokens made of magnetic materials, where the uniqueness is provided by un reproducible defects in the magnetic material that affect the token's magnetic response (as detailed in PCT/GB03/03917, Cowburn). As part of this work, magnetic materials were fabricated in barcode format, i.e. as a number of parallel strips. As well as reading the unique magnetic response of the strips by sweeping a magnetic field with a magnetic reader, an optical scanner was built to read the barcodes by scanning a laser beam over the barcode and using contrast from the varying reflectivity of the barcode strips and the article on which they were formed. This information was complementary to the magnetic characteristic, since the barcode was being used to encode a digital signature of the unique magnetic response in a type of well known self authentication scheme, for example as also described above for banknotes (see for example, Kravolec "Plastic tag makes foolproof ID", Technology research news, 2 October 2002).

To the surprise of the inventor, it was discovered when using this optical scanner that the paper background material on which the magnetic chips were supported gave a unique optical response to the scanner. On further investigation, it was established that many other unprepared surfaces, such as surfaces of various types of cardboard and plastic, show the same effect. Moreover, it has been established by the inventor that the unique characteristic arises at least in part from speckle, but also includes non-speckle contributions.

It has thus been discovered that it is possible to gain all the advantages of speckle based techniques without having to use a specially prepared token or specially prepare an article in any other way. In particular, many types of paper, cardboard and plastics have been found to give unique characteristic scattering signals from a
coherent light beam, so that unique digital signatures can be obtained from almost any paper document or cardboard packaging item.

The above-described known speckle readers used for security devices appear to be based on illuminating the whole of a token with a laser beam and imaging a significant solid angle portion of the resultant speckle pattern with a CCD (see for example GB 2 221 870 and US 6,584,214), thereby obtaining a speckle pattern image of the token made up of a large array of data points.

The reader used by the inventor does not operate in this manner. It uses four single channel detectors (four simple phototransistors) which are angularly spaced apart to collect only four signal components from the scattered laser beam. The laser beam is focused to a spot covering only a very small part of the surface. Signal is collected from different localised areas on the surface by the four single channel detectors as the spot is scanned over the surface. The characteristic response from the article is thus made up of independent measurements from a large number (typically hundreds or thousands) of different localised areas on the article surface. Although four phototransistors are used, analysis using only data from a single one of the phototransistors shows that a unique characteristic response can be derived from this single channel alone! However, higher security levels are obtained if further ones of the four channels are included in the response.

Viewed from a first aspect, the present invention provides A method for authenticity verification. The method can comprise conducting a transaction between first and second parties, the parties being respectively located at first and second locations remote one-another, the outcome of the transaction being the transfer of title to goods and/or services from the first party to the second party. Data describing a value entitlement token of the second party can be captured to create a signature for the value entitlement token, the signature being based upon an intrinsic property of the value entitlement token. The signature can be transmitted from the second party to a third party which can compare the signature to a database of stored signatures. A validation result indicating whether the value entitlement token corresponds to a value.
entitlement token signature in the database can be transmitted from the third party to
the first party. Thus the authenticity of a value entitlement token can be confidently
checked to avoid fraudulent copying or use of the token without the need for the token
to be physically present at a vendor or provider location for obtaining goods and/or
services. The value entitlement token can be a credit and/or debit card.

In one embodiment, the first and third parties are co-located, such that the
validation authority and the vendor are a single entity. Thus a vendor can provide its
own validation services. In other embodiments, these parties are separate entities,
such that a single authentication entity can provide authentication services for a
number of vendors. Such a third party can be a payment clearing authority.

In some embodiments, the method can further comprise transmitting data
describing the value entitlement token and/or a user thereof from the second party to
the first party and/or the third party. This information can include a card number, a
card validity period, a card holder name or a card holder address. In one embodiment,
This data can be compared to a database storing details of valid and/or invalid value
entitlement tokens and/or users. Thus it can be established whether the card has been
reported lost or stolen or if the user has been barred from use of the card. Also a
check can be performed to determine whether sufficient funds are available to pay for
the ordered goods or services. This database can be co-located with the signature
database, or can be separate. Both databases can be administered by a single payment
authentication entity, or can be administered separately.

In some embodiments, the step of creating the first and/or second signature
comprises: exposing the written entitlement token to coherent radiation; collecting a
set of data points that measure scatter of the coherent radiation from intrinsic structure
of the written entitlement token; and determining a signature of the written
entitlement token from the set of data points. Thereby a secure and reliable signature
generation system with a high confidence margin can be used to provide the
authentication.
In one embodiment, the signature can be divided into blocks of contiguous data and a comparison operation be performed between each block and respective blocks of stored ones of the signatures from the database of stored signatures. An attribute of a comparison result therefrom can be compared to an expected attribute of the comparison to determine a compensation value for use in determining the validation result. The compensation value can be used to compensate for damage to the value entitlement token and/or non-linearities in the capturing step. Thus a damaged value entitlement token and/or a data capture process where data is not gathered linearly can be taken account of to ensure that the value entitlement token is correctly validated despite such factors, but a false match is still avoided.

Viewed from a second aspect, the present invention provides a system for authenticity verification. The system can comprise first and second computer systems remote one-another and operable to communicate therebetween via a data communications channel. The first computer system can be operable to enable a user at the second computer system to conduct a transaction with the first computer system, the outcome of the transaction being the provision by the first computer system to the user of entitlement to goods and/or services. The system can also comprise a signature generator co-located with the second computer system and operable to create a signature for a value entitlement token of the user, based upon an intrinsic property of the value entitlement token. The second computer system can be operable to transmit the signature to a third computer system. The third computer system can be operable to compare the signature to a database of stored signatures, to produce a validation result indicating whether the value entitlement token corresponds to a value entitlement token signature in the database. The third computer system can be further operable to transmitting the validation result to the first computer system. Thus the authenticity of a value entitlement token can be confidently checked to avoid fraudulent copying or use of the token without the need for the token to be physically present at a vendor or provider location for obtaining goods and/or services. The value entitlement token can be a credit and/or debit card.
In one embodiment, the first and third computer systems are a single computer system such that a vendor can provide its own validation services. Alternatively, they may be separate computer systems, such that the third computer system may belong to a payment clearing authority offering services to a number of vendors.

In some embodiments, the second computer system can be operable to transmit data describing the value entitlement token and/or a user thereof to the first and/or the third computer system. This information can include a card number, a card validity period, a card holder name or a card holder address. In one embodiment, this data can be compared to a database storing details of valid and/or invalid value entitlement tokens and/or users. Thus it can be established whether the card has been reported lost or stolen or if the user has been barred from use of the card. Also a check can be performed to determine whether sufficient funds are available to pay for the ordered goods or services. This database can be co-located with the signature database, or can be separate. Both databases can be administered by a single payment authentication entity, or can be administered separately.

In some embodiments, the signature generator can comprise: a reading volume arranged to receive an article; a source for generating a coherent light beam; a detector arrangement for collecting a set of data points from signals obtained when the coherent light beam scatters from the reading volume, wherein different ones of the data points relate to scatter from different parts of the reading volume; and a data acquisition and processing module operable to determine a signature of the article from the set of data points. Thus the signatures can be generated with a high confidence in the ability of the system to establish the uniqueness of an item.

In some embodiments the third computer system can be operable to split the signature into blocks of contiguous data and to perform a comparison operation between each block and respective blocks of stored ones of the signatures from the database of stored signatures; and to compare an attribute of a comparison result therefrom to an expected attribute of the comparison to determine a compensation value for use in determining the validation result to compensate for damage to the
value entitlement token and/or non-linearities in the signature creation. Thus a non-linear path of the token through the signature generator can be corrected, as can damage to the token, such as stretching or compression of the token.

In one embodiment, the signature can be divided into blocks of contiguous data and a comparison operation be performed between each block and respective blocks of stored ones of the signatures from the database of stored signatures. Thereby a higher granularity of data processing can be achieved. In some embodiments, an attribute of a comparison result therefrom can be compared to an expected attribute of the comparison to determine a compensation value for use in determining the validation result. The compensation value can be used to compensate for damage to the value entitlement token and/or non-linearities in the capturing step. Thus a damaged value entitlement token and/or a data capture process where data is not gathered linearly can be taken account of to ensure that the value entitlement token is correctly validated despite such factors, but a false match is still avoided. In some examples selected blocks can be selected as critical blocks such that a block-level match for the critical blocks as well as an overall signature match is required for a positive authenticity result. This can allow for article regions such as signatures, names, photographs and numbers to be marked as more important that other regions of the article.

Viewed from a third aspect, the present invention provides a method for authenticating a credit or bank card. The method can comprise scanning a credit or bank card to create a signature based upon an intrinsic property thereof and transmitting the signature to a comparison entity operable to compare the signature to a database of stored signatures. The method can also comprise creating an authentication result based upon an outcome of the comparison. Thus a credit or debit card can be validated against a database of genuine cards to ensure that a genuine card is present. As this is based upon an intrinsic property of the card, a copy of the card showing identical text, numbers and icons/logos will fail the validation check.
In one embodiment the method further comprises transmitting data describing the card and/or a card holder to a validation entity, comparing the data to a database of invalid cards and/or card holders; and creating a validation result based upon an outcome of the comparison. Thus the account to which the card relates can be checked to ensure that, for example, the card has not been stopped or reported lost or stolen. The databases can be held separately or together and can be held on behalf of the same or separate entities.

In some embodiments, it is ensured that different ones of the data gathered in relation to the intrinsic property of the article relate to scatter from different parts of the article by providing for movement of the coherent beam relative to the article. The movement may be provided by a motor that moves the beam over an article that is held fixed. The motor could be a servo motor, free running motor, stepper motor or any suitable motor type. Alternatively, the drive could be manual in a low cost reader. For example, the operator could scan the beam over the article by moving a carriage on which the article is mounted across a static beam. The coherent beam cross-section will usually be at least one order of magnitude (preferably at least two) smaller than the projection of the article so that a significant number of independent data points can be collected. A focusing arrangement may be provided for bringing the coherent beam into focus in the article. The focusing arrangement may be configured to bring the coherent beam to an elongate focus, in which case the drive is preferably configured to move the coherent beam over the article in a direction transverse to the major axis of the elongate focus. An elongate focus can conveniently be provided with a cylindrical lens, or equivalent mirror arrangement.

In other embodiments, it can be ensured that different ones of the data points relate to scatter from different parts of the article, in that the detector arrangement includes a plurality of detector channels arranged and configured to sense scatter from respective different parts of the article. This can be achieved with directional detectors, local collection of signal with optical fibres or other measures. With directional detectors or other localised collection of signal, the coherent beam does not need to be focused. Indeed, the coherent beam could be static and illuminate the
whole sampling volume. Directional detectors could be implemented by focusing lenses fused to, or otherwise fixed in relation to, the detector elements. Optical fibres may be used in conjunction with microlenses.

It is possible to make a workable reader when the detector arrangement consists of only a single detector channel. Other embodiments use a detector arrangement that comprises a group of detector elements angularly distributed and operable to collect a group of data points for each different part of the reading volume, preferably a small group of a few detector elements. Security enhancement is provided when the signature incorporates a contribution from a comparison between data points of the same group. This comparison may conveniently involve a cross-correlation.

Although a working reader can be made with only one detector channel, there are preferably at least 2 channels. This allows cross-correlations between the detector signals to be made, which is useful for the signal processing associated with determining the signature. It is envisaged that between 2 and 10 detector channels will be suitable for most applications with 2 to 4 currently being considered as the optimum balance between apparatus simplicity and security.

The detector elements are advantageously arranged to lie in a plane intersecting the reading volume with each member of the pair being angularly distributed in the plane in relation to the coherent beam axis, preferably with one or more detector elements either side of the beam axis. However, non-planar detector arrangements are also acceptable.

The use of cross-correlations of the signals obtained from the different detectors has been found to give valuable data for increasing the security levels and also for allowing the signatures to be more reliably reproducible over time. The utility of the cross-correlations is somewhat surprising from a scientific point of view, since speckle patterns are inherently uncorrelated (with the exception of signals from opposed points in the pattern). In other words, for a speckle pattern there will by
definition be zero cross-correlation between the signals from the different detectors so long as they are not arranged at equal magnitude angles offset from the excitation location in a common plane intersecting the excitation location. The value of using cross-correlation contributions therefore indicates that an important part of the scatter signal is not speckle. The non-speckle contribution could be viewed as being the result of direct scatter, or a diffuse scattering contribution, from a complex surface, such as paper fibre twists. At present the relative importance of the speckle and non-speckle scatter signal contribution is not clear. However, it is clear from the experiments performed to date that the detectors are not measuring a pure speckle pattern, but a composite signal with speckle and non-speckle components.

Incorporating a cross-correlation component in the signature can also be of benefit for improving security. This is because, even if it is possible using high resolution printing to make an article that reproduces the contrast variations over the surface of the genuine article, this would not be able to match the cross-correlation coefficients obtained by scanning the genuine article.

In the one embodiment, the detector channels are made up of discrete detector components in the form of simple phototransistors. Other simple discrete components could be used such as PIN diodes or photodiodes. Integrated detector components, such as a detector array could also be used, although this would add to the cost and complexity of the device.

From initial experiments which modify the illumination angle of the laser beam on the article to be scanned, it also seems to be preferable in practice that the laser beam is incident approximately normal to the surface being scanned in order to obtain a characteristic that can be repeatedly measured from the same surface with little change, even when the article is degraded between measurements. At least some known readers use oblique incidence (see GB 2 221 870). Once appreciated, this effect seems obvious, but it is clearly not immediately apparent as evidenced by the design of some prior art speckle readers including that of GB 2 221 870 and indeed the first prototype reader built by the inventor. The inventor's first prototype reader
with oblique incidence functioned reasonably well in laboratory conditions, but was quite sensitive to degradation of the paper used as the article. For example, rubbing the paper with fingers was sufficient to cause significant differences to appear upon re-measurement. The second prototype reader used normal incidence and has been found to be robust against degradation of paper by routine handling, and also more severe events such as: passing through various types of printer including a laser printer, passing through a photocopier machine, writing on, printing on, deliberate scorching in an oven, and crushing and reflattening.

It can therefore be advantageous to mount the source so as to direct the coherent beam onto the reading volume so that it will strike an article with near normal incidence. By near normal incidence means \( \pm 5, 10 \) or \( 20 \) degrees. Alternatively, the beam can be directed to have oblique incidence on the articles. This will usually have a negative influence in the case that the beam is scanned over the article.

It is also noted that in the readers described in the detailed description, the detector arrangement is arranged in reflection to detect radiation back scattered from the reading volume. However, if the article is transparent, the detectors could be arranged in transmission.

A signature generator can be operable to access the database of previously recorded signatures and perform a comparison to establish whether the database contains a match to the signature of an article that has been placed in the reading volume. The database may be part of a mass storage device that forms part of the reader apparatus, or may be at a remote location and accessed by the reader through a telecommunications link. The telecommunications link may take any conventional form, including wireless and fixed links, and may be available over the internet. The data acquisition and processing module may be operable, at least in some operational modes, to allow the signature to be added to the database if no match is found.
When using a database, in addition to storing the signature it may also be useful to associate that signature in the database with other information about the article such as a scanned copy of the document, a photograph of a passport holder, details on the place and time of manufacture of the product, or details on the intended sales destination of vendable goods (e.g. to track grey importation).

The invention allows identification of articles made of a variety of different kinds of materials, such as paper, cardboard and plastic.

By intrinsic structure we mean structure that the article inherently will have by virtue of its manufacture, thereby distinguishing over structure specifically provided for security purposes, such as structure given by tokens or artificial fibres incorporated in the article.

By paper or cardboard we mean any article made from wood pulp or equivalent fibre process. The paper or cardboard may be treated with coatings or impregnations or covered with transparent material, such as cellophane. If long-term stability of the surface is a particular concern, the paper may be treated with an acrylic spray-on transparent coating, for example.

Data points can thus be collected as a function of position of illumination by the coherent beam. This can be achieved either by scanning a localised coherent beam over the article, or by using directional detectors to collect scattered light from different parts of the article, or by a combination of both.

The signature is envisaged to be a digital signature in most applications. Typical sizes of the digital signature with current technology would be in the range 200 bits to 8k bits, where currently it is preferable to have a digital signature size of about 2k bits for high security.

A further implementation of the invention can be performed without storing the digital signatures in a database, but rather by labelling the entitlement token with a
label derived from the signature, wherein the label conforms to a machine-readable encoding protocol.
BRIEF DESCRIPTION OF THE FIGURES

Specific embodiments of the present invention will now be described by way of example only with reference to the accompanying figures in which:

- Figure 1 is a schematic side view of an example of a reader apparatus;
- Figure 2 is a schematic perspective view showing how the reading volume of the reader apparatus of Figure 1 is sampled;
- Figure 3 is a block schematic diagram of the functional components of the reader apparatus of Figure 1;
- Figure 4 is a perspective view of the reader apparatus of Figure 1 showing its external form;
- Figure 5 is a perspective view showing another example of an external form for the reader of Figure 1;
- Figure 6A is schematic cross-sectional view through an alternative reader configuration;
- Figure 6B is a perspective view of another alternative reader configuration;
- Figure 6C is a perspective view of another alternative reader configuration;
- Figure 7A shows schematically in side view an alternative imaging arrangement for a reader based on directional light collection and blanket illumination;
Figure 7B shows schematically in plan view the optical footprint of a further alternative imaging arrangement for a reader in which directional detectors are used in combination with localised illumination with an elongate beam;

Figure 8A is a microscope image of a paper surface with the image covering an area of approximately 0.5 x 0.2 mm;

Figure 8B is a microscope image of a plastic surface with the image covering an area of approximately 0.02 x 0.02 mm;

Figure 9A shows raw data from a single photodetector using the reader of Figure 1 which consists of a photodetector signal and an encoder signal;

Figure 9B shows the photodetector data of Figure 9A after linearisation with the encoder signal and averaging the amplitude;

Figure 9C shows the data of Figure 9B after digitisation according to the average level;

Figure 10 is a flow diagram showing how a signature of an article is generated from a scan;

Figure 11 is a flow diagram showing how a signature of an article obtained from a scan can be verified against a signature database;

Figure 12 is a flow diagram showing how the verification process of Figure 11 can be altered to account for non-idealities in a scan;

Figure 13A shows an example of cross-correlation data data gathered from a scan;
Figure 13b shows an example of cross-correlation data gathered from a scan where the scanned article is distorted;

Figure 13C shows an example of cross-correlation data gathered from a scan where the scanned article is scanned at non-linear speed;

Figure 14 is a schematic representation of an article for authenticity verification.

Figure 15 is a schematic cut-away perspective view of a multi-scan head scanner;

Figure 16 is a schematic cut-away perspective view of a multi-scan head position scanner;

Figure 17 is a schematic overview of a distributed transaction environment such as an e-commerce environment; and

Figures 18A, 18B and 18C are a schematic plan views of different types of credit or bank card.

While the invention is susceptible to various modifications and alternative forms, specific embodiments are shown by way of example in the drawings and are herein described in detail. It should be understood, however, that drawings and detailed description thereto are not intended to limit the invention to the particular form disclosed, but on the contrary, the invention is to cover all modifications, equivalents and alternatives falling within the spirit and scope of the present invention as defined by the appended claims.
DESCRIPTION OF PARTICULAR EMBODIMENTS

For providing security and authorisation services in environments such as an e-commerce environment, a system for uniquely identifying a physical item can be used to reduce possibilities for fraud, and to enhance both actual and perceived reliability of the e-commerce system, for both provider and end-users.

Examples of systems suitable for performing such item identification will now be described with reference to Figures 1 to 11.

Figure 1 shows a schematic side view of a first example of a reader apparatus. The optical reader apparatus is for measuring a signature from an article (not shown) arranged in a reading volume of the apparatus. The reading volume is formed by a reading aperture which is a slit in a housing. The housing contains the main optical components of the apparatus. The slit has its major extent in the x direction (see inset axes in the drawing). The principal optical components are a laser source for generating a coherent laser beam and a detector arrangement made up of a plurality of photodetector elements, where k = 4 in this example, labelled 16a, 16b, 16c and 16d. The laser beam is focused by a cylindrical lens into an elongate focus extending in the y direction (perpendicular to the plane of the drawing) and lying in the plane of the reading aperture. In one example reader, the elongate focus has a major axis dimension of about 2 mm and a minor axis dimension of about 40 micrometres. These optical components are contained in a subassembly. In the present example, the four detector elements are distributed either side of the beam axis offset at different angles in an interdigitated arrangement from the beam axis to collect light scattered in reflection from an article present in the reading volume. In the present example, the offset angles are -70, -20, +30 and +50 degrees. The angles either side of the beam axis are chosen so as not to be equal so that the data points they collect are as independent as possible. All four detector elements are arranged in a common plane. The photodetector elements detect light scattered from an article placed on the housing when the coherent beam scatters from the reading volume. As illustrated, the source is mounted to direct the laser
beam 15 with its beam axis in the z direction, so that it will strike an article in the reading aperture at normal incidence.

Generally it is desirable that the depth of focus is large, so that any differences in the article positioning in the z direction do not result in significant changes in the size of the beam in the plane of the reading aperture. In the present example, the depth of focus is approximately 0.5 mm which is sufficiently large to produce good results where the position of the article relative to the scanner can be controlled to some extent. The parameters, of depth of focus, numerical aperture and working distance are interdependent, resulting in a well known trade off between spot size and depth of focus.

A drive motor 22 is arranged in the housing 12 for providing linear motion of the optics subassembly 20 via suitable bearings 24 or other means, as indicated by the arrows 26. The drive motor 22 thus serves to move the coherent beam linearly in the x direction over the reading aperture 10 so that the beam 15 is scanned in a direction transverse to the major axis of the elongate focus. Since the coherent beam 15 is dimensioned at its focus to have a cross-section in the xz plane (plane of the drawing) that is much smaller than a projection of the reading volume in a plane normal to the coherent beam, i.e. in the plane of the housing wall in which the reading aperture is set, a scan of the drive motor 22 will cause the coherent beam 15 to sample many different parts of the reading volume under action of the drive motor 22.

Figure 2 is included to illustrate this sampling and is a schematic perspective view showing how the reading area is sampled n times by scanning an elongate beam across it. The sampling positions of the focused laser beam as it is scanned along the reading aperture under action of the drive is represented by the adjacent rectangles numbered 1 to n which sample an area of length T and width V. Data collection is made so as to collect signal at each of the n positions as the drive is scanned along the slit. Consequently, a sequence of k x n data points are collected that relate to scatter from the n different illustrated parts of the reading volume.
Also illustrated schematically are optional distance marks 28 formed on the underside of the housing 12 adjacent the slit 10 along the x direction, i.e. the scan direction. An example spacing between the marks in the x-direction is 300 micrometres. These marks are sampled by a tail of the elongate focus and provide for linearisation of the data in the x direction in situations where such linearisation is required, as is described in more detail further below. The measurement is performed by an additional phototransistor 19 which is a directional detector arranged to collect light from the area of the marks 28 adjacent the slit.

In alternative examples, the marks 28 can be read by a dedicated encoder emitter/detector module 19 that is part of the optics subassembly 20. Encoder emitter/detector modules are used in bar code readers. In one example, an Agilent HEDS-1500 module that is based on a focused light emitting diode (LED) and photodetector can be used. The module signal is fed into the PIC ADC as an extra detector channel (see discussion of Figure 3 below).

With an example minor dimension of the focus of 40 micrometers, and a scan length in the x direction of 2 cm, n=500, giving 2000 data points with k = 4. A typical range of values for k x n depending on desired security level, article type, number of detector channels 'k' and other factors is expected to be 100 < k x n < 10,000. It has also been found that increasing the number of detectors k also improves the insensitivity of the measurements to surface degradation of the article through handling, printing etc. In practice, with the prototypes used to date, a rule of thumb is that the total number of independent data points, i.e. k x n, should be 500 or more to give an acceptably high security level with a wide variety of surfaces. Other minima (either higher or lower) may apply where a scanner is intended for use with only one specific surface type or group of surface types.

Figure 3 is a block schematic diagram of functional components of the reader apparatus. The motor 22 is connected to a programmable interrupt controller (PIC) 30 through an electrical link 23. The detectors 16a...d of the detector module 16 are connected through respective electrical connection lines 17a...d to an analogue-to-
digital converter (ADC) that is part of the PIC 30. A similar electrical connection line 21 connects the marker reading detector 19 to the PIC 30. It will be understood that optical or wireless links may be used instead of, or in combination with, electrical links. The PIC 30 is interfaced with a personal computer (PC) 34 through a data connection 32. The PC 34 may be a desktop or a laptop. As an alternative to a PC, other intelligent devices may be used, for example a personal digital assistant (PDA) or a dedicated electronics unit. The PIC 30 and PC 34 collectively form a data acquisition and processing module 36 for determining a signature of the article from the set of data points collected by the detectors 16a...d.

In some examples, the PC 34 can have access through an interface connection 38 to a database (dB) 40. The database 40 may be resident on the PC 34 in memory, or stored on a drive thereof. Alternatively, the database 40 may be remote from the PC 34 and accessed by wireless communication, for example using mobile telephony services or a wireless local area network (LAN) in combination with the internet. Moreover, the database 40 may be stored locally on the PC 34, but periodically downloaded from a remote source. The database may be administered by a remote entity, which entity may provide access to only a part of the total database to the particular PC 34, and/or may limit access the database on the basis of a security policy.

The database 40 can contain a library of previously recorded signatures. The PC 34 can be programmed so that in use it can access the database 40 and performs a comparison to establish whether the database 40 contains a match to the signature of the article that has been placed in the reading volume. The PC 34 can also be programmed to allow a signature to be added to the database if no match is found.

The way in which data flow between the PC and database is handled can be dependent upon the location of the PC and the relationship between the operator of the PC and the operator of the database. For example, if the PC and reader are being used to confirm the authenticity of an article, then the PC will not need to be able to add new articles to the database, and may in fact not directly access the database, but...
instead provide the signature to the database for comparison. In this arrangement the
database may provide an authenticity result to the PC to indicate whether the article is
authentic. On the other hand, if the PC and reader are being used to record or validate
an item within the database, then the signature can be provided to the database for
storage therein, and no comparison may be needed. In this situation a comparison
could be performed however, to avoid a single item being entered into the database
twice.

Figure 4 is a perspective view of the reader apparatus 1 showing its external
form. The housing 12 and slit-shaped reading aperture 10 are evident. A physical
location aid 42 is also apparent and is provided for positioning an article of a given
form in a fixed position in relation to the reading aperture 10. In the present example,
the physical location aid 42 is in the form of a right-angle bracket in which the corner
of a document or packaging box can be located. This ensures that the same part of the
article can be positioned in the reading aperture 10 whenever the article needs to be
scanned. A simple angle bracket or equivalent, is sufficient for articles with a well-
defined corner, such as sheets of paper, passports, ID cards and packaging boxes.
Other shaped position guides could be provided to accept items of different shapes,
such as circular items including CDs and DVDs, or items with curved surfaces such
as cylindrical packaging containers. Where only one size and shape of item is to be
scanned a slot may be provided for receiving the item.

Thus there has now been described an example of a scanning and signature
generation apparatus suitable for use in a security mechanism for remote verification
of article authenticity. Such a system can be deployed to allow an article to be
scanned in more than one location, and for a check to be performed to ensure that the
article is the same article in both instances, and optionally for a check to performed to
ensure that the article has not been tampered with between initial and subsequent
scannings.

Figure 5 shows an example of an alternative physical configuration for a
reader where a document feeder is provided to ensure that article placement is
consistent. In this example, a housing 60 is provided, having an article feed tray 61 attached thereto. The tray 61 can hold one or more articles 62 for scanning by the reader. A motor can drive feed rollers 64 to carry an article 62 through the device and across a scanning aperture of an optics subassembly 20 as described above. Thus the article 62 can be scanned by the optics subassembly 20 in the manner discussed above in a manner whereby the relative motion between optics subassembly and article is created by movement of the article. Using such a system, the motion of the scanned item can be controlled using the motor with sufficient linearity that the use of distance marks and linearisation processing may be unnecessary. The apparatus could follow any conventional format for document scanners, photocopiers or document management systems. Such a scanner may be configured to handle line-feed sheets (where multiple sheets are connected together by, for example, a perforated join) as well as or instead of handing single sheets.

Thus there has now been described an apparatus suitable for scanning articles in an automated feeder type device. Depending upon the physical arrangement of the feed arrangement, the scanner may be able to scan one or more single sheets of material, joined sheets or material or three-dimensional items such as packaging cartons.

Figures 6 show examples of further alternative physical configurations for a reader. In this example, the article is moved through the reader by a user. As shown in Figure 6A, a reader housing 70 can be provided with a slot 71 therein for insertion of an article for scanning. An optics subassembly 20 can be provided with a scanning aperture directed into the slot 71 so as to be able to scan an article 62 passed through the slot. Additionally, guide elements 72 may be provided in the slot 71 to assist in guiding the article to the correct focal distance from the optics sub-assembly 20 and/or to provide for a constant speed passage of the article through the slot.

As shown in Figure 6B, the reader may be configured to scan the article when moved along a longitudinal slot through the housing 70, as indicated by the arrow. Alternatively, as shown in Figure 6C, the reader may be configured to scan the article
when inserted into or removed from a slot extending into the reader housing 70, as indicated by the arrow. Scanners of this type may be particularly suited to scanning articles which are at least partially rigid, such as card, plastic or metal sheets. Such sheets may, for example, be plastic items such as credit cards or other bank cards.

Thus there have now been described an arrangement for manually initiated scanning of an article. This could be used for scanning bank cards and/or credit cards. Thereby a card could be scanned at a terminal where that card is presented for use, and a signature taken from the card could be compared to a stored signature for the card to check the authenticity and un-tampered nature of the card. Such a device could also be used, for example in the context of reading a military-style metal ID-tag (which tags are often also carried by allergy sufferers to alert others to their allergy). This could enable medical personnel treating a patient to ensure that the patient being treated was in fact the correct bearer of the tag. Likewise, in a casualty situation, a recovered tag could be scanned for authenticity to ensure that a casualty has been correctly identified before informing family and/or colleagues.

The above-described examples are based on localised excitation with a coherent light beam of small cross-section in combination with detectors that accept light signal scattered over a much larger area that includes the local area of excitation. It is possible to design a functionally equivalent optical system which is instead based on directional detectors that collect light only from localised areas in combination with excitation of a much larger area.

Figure 7A shows schematically in side view such an imaging arrangement for a reader which is based on directional light collection and blanket illumination with a coherent beam. An array detector 48 is arranged in combination with a cylindrical microlens array 46 so that adjacent strips of the detector array 48 only collect light from corresponding adjacent strips in the reading volume. With reference to Figure 2, each cylindrical microlens is arranged to collect light signal from one of the n sampling strips. The coherent illumination can then take place with blanket illumination of the whole reading volume (not shown in the illustration).
A hybrid system with a combination of localised excitation and localised detection may also be useful in some cases.

Figure 7B shows schematically in plan view the optical footprint of such a hybrid imaging arrangement for a reader in which directional detectors are used in combination with localised illumination with an elongate beam. This example may be considered to be a development of the example of Figure 1 in which directional detectors are provided. In this example three banks of directional detectors are provided, each bank being targeted to collect light from different portions along the \( x \times w \) excitation strip. The collection area from the plane of the reading volume are shown with the dotted circles, so that a first bank of, for example 2, detectors collects light signal from the upper portion of the excitation strip, a second bank of detectors collects light signal from a middle portion of the excitation strip and a third bank of detectors collects light from a lower portion of the excitation strip. Each bank of detectors is shown having a circular collection area of diameter approximately \( 1/m \), where \( m \) is the number of subdivisions of the excitation strip, where \( m = 3 \) in the present example. In this way the number of independent data points can be increased by a factor of \( m \) for a given scan length \( l \). As described further below, one or more of different banks of directional detectors can be used for a purpose other than collecting light signal that samples a speckle pattern. For example, one of the banks may be used to collect light signal in a way optimised for barcode scanning. If this is the case, it will generally be sufficient for that bank to contain only one detector, since there will be no advantage obtaining cross-correlations when only scanning for contrast.

Having now described the principal structural components and functional components of various reader apparatuses, the numerical processing used to determine a signature will now be described. It will be understood that this numerical processing can be implemented for the most part in a computer program that runs on the PC 34 with some elements subordinated to the PIC 30. In alternative examples,
the numerical processing could be performed by a dedicated numerical processing
device or devices in hardware or firmware.

Figure 8A is a microscope image of a paper surface with the image covering
an area of approximately 0.5 x 0.2 mm. This figure is included to illustrate that
macroscopically flat surfaces, such as from paper, are in many cases highly structured
at a microscopic scale. For paper, the surface is microscopically highly structured as
a result of the intermeshed network of wood or other fibres that make up the paper.
The figure is also illustrative of the characteristic length scale for the wood fibres
which is around 10 microns. This dimension has the correct relationship to the optical
wavelength of the coherent beam of the present example to cause diffraction and
hence speckle, and also diffuse scattering which has a profile that depends upon the
fibre orientation. It will thus be appreciated that if a reader is to be designed for a
specific class of goods, the wavelength of the laser can be tailored to the structure
feature size of the class of goods to be scanned. It is also evident from the figure that
the local surface structure of each piece of paper will be unique in that it depends on
how the individual wood fibres are arranged. A piece of paper is thus no different
from a specially created token, such as the special resin tokens or magnetic material
deposits of the prior art, in that it has structure which is unique as a result of it being
made by a process governed by laws of nature. The same applies to many other types
of article.

Figure 8B shows an equivalent image for a plastic surface. This atomic force
microscopy image clearly shows the uneven surface of the macroscopically smooth
plastic surface. As can be surmised from the figure, this surface is smoother than the
paper surface illustrated in Figure 8A, but even this level of surface undulation can be
uniquely identified using the signature generation scheme of the present example.

In other words, it can be essentially pointless to go to the effort and expense of
making specially prepared tokens, when unique characteristics are measurable in a
straightforward manner from a wide variety of every day articles. The data collection
and numerical processing of a scatter signal that takes advantage of the natural
structure of an article's surface (or interior in the case of transmission) is now described.

Figure 9A shows raw data from a single one of the photodetectors 16a...d of the reader of Figure 1. The graph plots signal intensity I in arbitrary units (a.u.) against point number n (see Figure 2). The higher trace fluctuating between $I = 0$-250 is the raw signal data from photodetector 16a. The lower trace is the encoder signal picked up from the markers 28 (see Figure 2) which is at around $I = 50$.

Figure 9B shows the photodetector data of Figure 10A after linearisation with the encoder signal (n.b. although the x axis is on a different scale from Figure 10A, this is of no significance). As noted above, where a movement of the article relative to the scanner is sufficiently linear, there may be no need to make use of a linearisation relative to alignment marks. In addition, the average of the intensity has been computed and subtracted from the intensity values. The processed data values thus fluctuate above and below zero.

Figure 9C shows the data of Figure 9B after digitisation. The digitisation scheme adopted is a simple binary one in which any positive intensity values are set at value 1 and any negative intensity values are set at zero. It will be appreciated that multi-state digitisation could be used instead, or any one of many other possible digitisation approaches. The main important feature of the digitisation is merely that the same digitisation scheme is applied consistently.

Figure 10 is a flow diagram showing how a signature of an article is generated from a scan.

Step S1 is a data acquisition step during which the optical intensity at each of the photodetectors is acquired approximately every lms during the entire length of scan. Simultaneously, the encoder signal is acquired as a function of time. It is noted that if the scan motor has a high degree of linearisation accuracy (e.g. as would a stepper motor) then linearisation of the data may not be required. The data is acquired
by the PIC 30 taking data from the ADC 31. The data points are transferred in real
time from the PIC 30 to the PC 34. Alternatively, the data points could be stored in
memory in the PIC 30 and then passed to the PC 34 at the end of a scan. The number
n of data points per detector channel collected in each scan is defined as \( N \) in the
following. Further, the value \( k(i) \) is defined as the i-th stored intensity value from
photodetector \( k \), where \( i \) runs from 1 to \( N \). Examples of two raw data sets obtained
from such a scan are illustrated in Figure 9A.

Step S2 uses numerical interpolation to locally expand and contract \( \alpha(i) \) so
that the encoder transitions are evenly spaced in time. This corrects for local
variations in the motor speed. This step can be performed in the PC 34 by a computer
program.

Step S3 is an optional step. If performed, this step numerically differentiates
the data with respect to time. It may also be desirable to apply a weak smoothing
function to the data. Differentiation may be useful for highly structured surfaces, as it
serves to attenuate uncorrelated contributions from the signal relative to correlated
(speckle) contributions.

Step S4 is a step in which, for each photodetector, the mean of the recorded
signal is taken over the \( N \) data points. For each photodetector, this mean value is
subtracted from all of the data points so that the data are distributed about zero
intensity. Reference is made to Figure 9B which shows an example of a scan data set
after linearisation and subtraction of a computed average.

Step S5 digitises the analogue photodetector data to compute a digital
signature representative of the scan. The digital signature is obtained by applying the
rule: \( a_k(i) > 0 \) maps onto binary '1' and \( a_k(i) \leq 0 \) maps onto binary '0'. The digitised
data set is defined as \( dk(i) \) where \( i \) runs from 1 to \( N \). The signature of the article may
incorporate further components in addition to the digitised signature of the intensity
data just described. These further optional signature components are now described.
Step S6 is an optional step in which a smaller 'thumbnail' digital signature is created. This is done either by averaging together adjacent groups of \( m \) readings, or more preferably by picking every \( c \)th data point, where \( c \) is the compression factor of the thumbnail. The latter is preferred since averaging may disproportionately amplify noise. The same digitisation rule used in Step S5 is then applied to the reduced data set. The thumbnail digitisation is defined as \( t_k(i) \) where \( i \) runs 1 to \( N/c \) and \( c \) is the compression factor.

Step S7 is an optional step applicable when multiple detector channels exist. The additional component is a cross-correlation component calculated between the intensity data obtained from different ones of the photodetectors. With 2 channels there is one possible cross-correlation coefficient, with 3 channels up to 3, and with 4 channels up to 6 etc. The cross-correlation coefficients are useful, since it has been found that they are good indicators of material type. For example, for a particular type of document, such as a passport of a given type, or laser printer paper, the cross-correlation coefficients always appear to lie in predictable ranges. A normalised cross-correlation can be calculated between \( a_k(i) \) and \( a_l(i) \), where \( k \neq l \) and \( k, l \) vary across all of the photodetector channel numbers. The normalised cross-correlation function \( F \) is defined as

\[
\Gamma(k,l) = \frac{\sum_{i=1}^{N} a_k(i) a_l(i)}{\sqrt{\left(\sum_{i=1}^{N} a_k(i)^2\right) \left(\sum_{i=1}^{N} a_l(i)^2\right)}}
\]

Another aspect of the cross-correlation function that can be stored for use in later verification is the width of the peak in the cross-correlation function, for example the full width half maximum (FWHM). The use of the cross-correlation coefficients in verification processing is described further below.

Step S8 is another optional step which is to compute a simple intensity average value indicative of the signal intensity distribution. This may be an overall average of each of the mean values for the different detectors or an average for each
detector, such as a root mean square (rms) value of $a_k(i)$. If the detectors are arranged in pairs either side of normal incidence as in the reader described above, an average for each pair of detectors may be used. The intensity value has been found to be a good crude filter for material type, since it is a simple indication of overall reflectivity and roughness of the sample. For example, one can use as the intensity value the unnormalised rms value after removal of the average value, i.e. the DC background.

The signature data obtained from scanning an article can be compared against records held in a signature database for verification purposes and/or written to the database to add a new record of the signature to extend the existing database.

A new database record will include the digital signature obtained in Step S5. This can optionally be supplemented by one or more of its smaller thumbnail version obtained in Step S6 for each photodetector channel, the cross-correlation coefficients obtained in Step S7 and the average value(s) obtained in Step S8. Alternatively, the thumbnails may be stored on a separate database of their own optimised for rapid searching, and the rest of the data (including the thumbnails) on a main database.

Figure 11 is a flow diagram showing how a signature of an article obtained from a scan can be verified against a signature database.

In a simple implementation, the database could simply be searched to find a match based on the full set of signature data. However, to speed up the verification process, the process can use the smaller thumbnails and pre-screening based on the computed average values and cross-correlation coefficients as now described.

Verification Step V1 is the first step of the verification process, which is to scan an article according to the process described above, i.e. to perform Scan Steps S1 to S8.

Verification Step V2 takes each of the thumbnail entries and evaluates the number of matching bits between it and $t_k(i+y)$, where $j$ is a bit offset which is varied...
to compensate for errors in placement of the scanned area. The value of \( j \) is determined and then the thumbnail entry which gives the maximum number of matching bits. This is the 'hit' used for further processing.

Verification Step V3 is an optional pre-screening test that is performed before analysing the full digital signature stored for the record against the scanned digital signature. In this pre-screen, the rms values obtained in Scan Step S8 are compared against the corresponding stored values in the database record of the hit. The 'hit' is rejected from further processing if the respective average values do not agree within a predefined range. The article is then rejected as non-verified (i.e. jump to Verification Step V6 and issue fail result).

Verification Step V4 is a further optional pre-screening test that is performed before analysing the full digital signature. In this pre-screen, the cross-correlation coefficients obtained in Scan Step S7 are compared against the corresponding stored values in the database record of the hit. The 'hit' is rejected from further processing if the respective cross-correlation coefficients do not agree within a predefined range. The article is then rejected as non-verified (i.e. jump to Verification Step V6 and issue fail result).

Another check using the cross-correlation coefficients that could be performed in Verification Step V4 is to check the width of the peak in the cross-correlation function, where the cross-correlation function is evaluated by comparing the value stored from the original scan in Scan Step S7 above and the re-scanned value:

\[
\Gamma_{s',j}(j) = \frac{\sum_{i=1}^{N} a_i(i) a_i(i+j)}{\sqrt{\left(\sum_{i=1}^{N} a_i(i)^2\right)\left(\sum_{i=1}^{N} a_i(i)^2\right)} }
\]

If the width of the re-scanned peak is significantly higher than the width of the original scan, this may be taken as an indicator that the re-scanned article has been
tampered with or is otherwise suspicious. For example, this check should beat a fraudster who attempts to fool the system by printing a bar code or other pattern with the same intensity variations that are expected by the photodetectors from the surface being scanned.

Verification Step V5 is the main comparison between the scanned digital signature obtained in Scan Step S5 and the corresponding stored values in the database record of the hit. The full stored digitised signature, \( d_k^{\text{db}}(i) \) is split into \( n \) blocks of \( q \) adjacent bits on \( k \) detector channels, i.e. there are \( qk \) bits per block. A typical value for \( q \) is 4 and a typical value for \( k \) is 4, making typically 16 bits per block. The \( qk \) bits are then matched against the \( qk \) corresponding bits in the stored digital signature \( d_k^{\text{db}}(i+j) \). If the number of matching bits within the block is greater or equal to some pre-defined threshold \( z_{\text{thresh}} \), then the number of matching blocks is incremented. A typical value for \( Z_{\text{thresh}} \) is 13. This is repeated for all \( n \) blocks. This whole process is repeated for different offset values \( o_f \) to compensate for errors in placement of the scanned area, until a maximum number of matching blocks is found. Defining \( M \) as the maximum number of matching blocks, the probability of an accidental match is calculated by evaluating:

\[
p(M) = \sum_{W=H-M}^{n} s^w (1-s)^{n-w} \frac{n!}{w!(n-w)!}
\]

where \( s \) is the probability of an accidental match between any two blocks (which in turn depends upon the chosen value of \( Z_{\text{thresh}} \)). \( M \) is the number of matching blocks and \( p(M) \) is the probability of \( M \) or more blocks matching accidentally. The value of \( s \) is determined by comparing blocks within the data base from scans of different objects of similar materials, e.g. a number of scans of paper documents etc. For the case of \( q=4 \), \( k=4 \) and \( z_{\text{thresh}}=13 \), we typical value of \( s \) is 0.1. If the \( qk \) bits were entirely independent, then probability theory would give \( s=0.01 \) for \( Z_{\text{thresh}}=13 \). The fact that a higher value is found empirically is because of correlations between the \( k \) detector channels and also correlations between adjacent bits in the block due to a finite laser spot width. A typical scan of a piece of paper
yields around 314 matching blocks out of a total number of 510 blocks, when compared against the data base entry for that piece of paper. Setting $M=3 \ 14$, $\leq 510$, $p=0.1$ for the above equation gives a probability of an accidental match of $10^{-177}$.

Verification Step V6 issues a result of the verification process. The probability result obtained in Verification Step V5 may be used in a pass/fail test in which the benchmark is a pre-defined probability threshold. In this case the probability threshold may be set at a level by the system, or may be a variable parameter set at a level chosen by the user. Alternatively, the probability result may be output to the user as a confidence level, either in raw form as the probability itself, or in a modified form using relative terms (e.g. no match / poor match / good match / excellent match) or other classification.

It will be appreciated that many variations are possible. For example, instead of treating the cross-correlation coefficients as a pre-screen component, they could be treated together with the digitised intensity data as part of the main signature. For example the cross-correlation coefficients could be digitised and added to the digitised intensity data. The cross-correlation coefficients could also be digitised on their own and used to generate bit strings or the like which could then be searched in the same way as described above for the thumbnails of the digitised intensity data in order to find the hits.

Thus there have now been described a number of examples arrangements for scanning an article to obtain a signature based upon intrinsic properties of that article. There have also been described examples of how that signature can be generated from the data collected during the scan, and how the signature can be compared to a later scan from the same or a different article to provide a measure of how likely it is that the same article has been scanned in the later scan.

Such a system has many applications, amongst which are security and confidence screening of items for fraud prevention and item traceability.
In some examples, the method for extracting a signature from a scanned article can be optimised to provide reliable recognition of an article despite deformations to that article caused by, for example, stretching or shrinkage. Such stretching or shrinkage of an article may be caused by, for example, water damage to a paper or cardboard based article.

Also, an article may appear to a scanner to be stretched or shrunk if the relative speed of the article to the sensors in the scanner is non-linear. This may occur if, for example the article is being moved along a conveyor system, or if the article is being moved through a scanner by a human holding the article. An example of a likely scenario for this to occur is where a human scans, for example, a bank card using a scanner such as that described with reference to Figures 6A, 6B and 6C above.

As described above, where a scanner is based upon a scan head which moves within the scanner unit relative to an article held stationary against or in the scanner, then linearisation guidance can be provided by the optional distance marks 28 to address any non-linearities in the motion of the scan head. Where the article is moved by a human, these non-linearities can be greatly exaggerated.

To address recognition problems which could be caused by these non-linear effects, it is possible to adjust the analysis phase of a scan of an article. Thus a modified validation procedure will now be described with reference to Figure 12. The process implemented in this example uses a block-wise analysis of the data to address the non-linearities.

The process carried out in accordance with Figure 12, can include some or all of the steps of smoothing and differentiating the data, computing and subtracting the mean, and digitisation for obtaining the signature and thumbnail described with reference to Figure 10, but are not shown in Figure 12 so as not to obscure the content of that figure.
As shown in Figure 1, the scanning process for a validation scan using a block-wise analysis starts at step S21 by performing a scan of the article to acquire the date describing the intrinsic properties of the article. This scanned data is then divided into contiguous blocks (which can be performed before or after digitisation and any smoothing/differentiation or the like) at step S22. In one example, a scan length of 54mm is divided into eight equal length blocks. Each block therefore represents a subsection of scanned area of the scanned article.

For each of the blocks, a cross-correlation is performed against the equivalent block for each stored signature with which it is intended that article be compared at step S23. This can be performed using a thumbnail approach with one thumbnail for each block. The results of these cross-correlation calculations are then analysed to identify the location of the cross-correlation peak. The location of the cross-correlation peak is then compared at step S24 to the expected location of the peak for the case were a perfectly linear relationship to exist between the original and later scans of the article.

This relationship can be represented graphically as shown in Figures 13A, 13B and 13C. In the example of Figure 13A, the cross-correlation peaks are exactly where expected, such that the motion of the scan head relative to the article has been perfectly linear and the article has not experienced stretch or shrinkage. Thus a plot of actual peak positions against expected peak results in a straight line which passes through the origin and has a gradient of 1.

In the example of Figure 13B, the cross-correlation peaks are closer together than expected, such that the gradient of a line of best fit is less than one. Thus the article has shrunk relative to its physical characteristics upon initial scanning. Also, the best fit line does not pass through the origin of the plot. Thus the article is shifted relative to the scan head compared to its position upon initial scanning.

In the example of Figure 13C, the cross correlation peaks do not form a straight line. In this example, they approximately fit to a curve representing a $y^2$
function. Thus the movement of the article relative to the scan head has slowed during the scan. Also, as the best fit curve does not cross the origin, it is clear that the article is shifted relative to its position upon initial scanning.

A variety of functions can be test-fitted to the plot of points of the cross-correlation peaks to find a best-fitting function. Thus curves to account for stretch, shrinkage, misalignment, acceleration, deceleration, and combinations thereof can be used.

Once a best-fitting function has been identified at step S25, a set of change parameters can be determined which represent how much each cross-correlation peak is shifted from its expected position at step S26. These compensation parameters can then, at step S27, be applied to the data from the scan taken at step S21 in order substantially to reverse the effects of the shrinkage, stretch, misalignment, acceleration or deceleration on the data from the scan. As will be appreciated, the better the best-fit function obtained at step S25 fits the scan data, the better the compensation effect will be.

The compensated scan data is then broken into contiguous blocks at step S28 as in step S22. The blocks are then individually cross-correlated with the respective blocks of data from the stored signature at step S29 to obtain the cross-correlation coefficients. This time the magnitude of the cross-correlation peaks are analysed to determine the uniqueness factor at step S29. Thus it can be determined whether the scanned article is the same as the article which was scanned when the stored signature was created.

Accordingly, there has now been described an example of a method for compensating for physical deformations in a scanned article, and for non-linearities in the motion of the article relative to the scanner. Using this method, a scanned article can be checked against a stored signature for that article obtained from an earlier scan of the article to determine with a high level of certainty whether or not the same article is present at the later scan. Thereby an article constructed from easily distorted
material can be reliably recognised. Also, a scanner where the motion of the scanner
relative to the article may be non-linear can be used, thereby allowing the use of a
low-cost scanner without motion control elements.

In some scanner apparatuses, it is also possible that it may be difficult to
determine where a scanned region starts and finishes. Of the examples discussed
above, this is most problematic for the example of Figure 6B, where an article to be
scanned passes through a slot, such that the scan head may "see" more of an article
than the intended scan area. One approach to addressing this difficulty would be to
define the scan area as starting at the edge of the article. As the data received at the
scan head will undergo a clear step change when an article is passed though what was
previously free space, the data retrieved at the scan head can be used to determine
where the scan starts.

In this example, the scan head is operational prior to the application of the
article to the scanner. Thus initially the scan head receives data corresponding to the
unoccupied space in front of the scan head. As the article is passed in front of the
scan head, the data received by the scan head immediately changes to be data
describing the article. Thus the data can be monitored to determine where the article
starts and all data prior to that can be discarded. The position and length of the scan
area relative to the article leading edge can be determined in a number of ways. The
simplest is to make the scan area the entire length of the article, such that the end can
be detected by the scan head again picking up data corresponding to free space.
Another method is to start and/or stop the recorded data a predetermined number of
scan readings from the leading edge. Assuming that the article always moves past the
scan head at approximately the same speed, this would result in a consistent scan area.
Another alternative is to use actual marks on the article to start and stop the scan
region, although this may require more work, in terms of data processing, to
determine which captured data corresponds to the scan area and which data can be
discarded.
Thus there has now been described a number of techniques for scanning an item to gather data based on an intrinsic property of the article, compensating if necessary for damage to the article or non-linearities in the scanning process, and comparing the article to a stored signature based upon a previous scan of an article to determine whether the same article is present for both scans.

Another characteristic of an article which can be detected using a block-wise analysis of a signature generated based upon an intrinsic property of that article is that of localised damage to the article. For example, such a technique can be used to detect modifications to an article made after an initial record scan.

For example, many documents, such as passports, ID cards and driving licenses, include photographs of the bearer. If an authenticity scan of such an article includes a portion of the photograph, then any alteration made to that photograph will be detected. Taking an arbitrary example of splitting a signature into 10 blocks, three of those blocks may cover a photograph on a document and the other seven cover another part of the document, such as a background material. If the photograph is replaced, then a subsequent rescan of the document can be expected to provide a good match for the seven blocks where no modification has occurred, but the replaced photograph will provide a very poor match. By knowing that those three blocks correspond to the photograph, the fact that all three provide a very poor match can be used to automatically fail the validation of the document, regardless of the average score over the whole signature.

Also, many documents include written indications of one or more persons, for example the name of a person identified by a passport, driving licence or identity card, or the name of a bank account holder. Many documents also include a place where written signature of a bearer or certifier is applied. Using a block-wise analysis of a signature obtained therefrom for validation can detect a modification to alter a name or other important word or number printed or written onto a document. A block which corresponds to the position of an altered printing or writing can be expected to produce a much lower quality match than blocks where no modification has taken
place. Thus a modified name or written signature can be detected and the document failed in a validation test even if the overall match of the document is sufficiently high to obtain a pass result.

An example of an identity card 300 is shown in Figure 300. The identity card 300 includes a printed bearer name 302, a photograph of the bearer 304, a signature of the bearer 306 (which may be written onto the card, or printed from a scan of a written signature or a signature captured electronically), and a printed card number 308. In order to protect against fraudulent alteration to the identity card, a scan area for generating a signature based upon an intrinsic property of the card can include one or more of those elements. Various example scan areas are marked in Figure 15 to illustrate the possibilities. Example scan area 321 includes part of the printed name 302 and part of the photograph 304. Example scan area 322 includes part of the printed name. Example scan area 323 includes part of the signature 306. Example scan area 324 includes part of the card number 308.

The area and elements selected for the scan area can depend upon a number of factors, including the element of the document which it is most likely that a fraudster would attempt to alter. For example, for any document including a photograph the most likely alteration target will usually be the photograph as this visually identifies the bearer. Thus a scan area for such a document might beneficially be selected to include a portion of the photograph. Another element which may be subjected to fraudulent modification is the bearer's signature, as it is easy for a person to pretend to have a name other than their own, but harder to copy another person's signature. Therefore for signed documents, particularly those not including a photograph, a scan area may beneficially include a portion of a signature on the document.

In the general case therefore, it can be seen that a test for authenticity of an article can comprise a test for a sufficiently high quality match between a verification signature and a record signature for the whole of the signature, and a sufficiently high match over at least selected blocks of the signatures. Thus regions important to the
assessing the authenticity of an article can be selected as being critical to achieving a positive authenticity result.

In some examples, blocks other than those selected as critical blocks may be allowed to present a poor match result. Thus a document may be accepted as authentic despite being torn or otherwise damaged in parts, so long as the critical blocks provide a good match and the signature as a whole provides a good match.

Thus there have now been described a number of examples of a system, method and apparatus for identifying localised damage to an article, and for rejecting an inauthentic an article with localised damage or alteration in predetermined regions thereof. Damage or alteration in other regions may be ignored, thereby allowing the document to be recognised as authentic.

In some scanner apparatuses, it is also possible that it may be difficult to determine where a scanned region starts and finishes. Of the examples discussed above, this is most problematic for the example of Figure 6B, where an article to be scanned passes through a slot, such that the scan head may "see" more of an article than the intended scan area. One approach to addressing this difficulty would be to define the scan area as starting at the edge of the article. As the data received at the scan head will undergo a clear step change when an article is passed though what was previously free space, the data retrieved at the scan head can be used to determine where the scan starts.

In this example, the scan head is operational prior to the application of the article to the scanner. Thus initially the scan head receives data corresponding to the unoccupied space in front of the scan head. As the article is passed in front of the scan head, the data received by the scan head immediately changes to be data describing the article. Thus the data can be monitored to determine where the article starts and all data prior to that can be discarded. The position and length of the scan area relative to the article leading edge can be determined in a number of ways. The simplest is to make the scan area the entire length of the article, such that the end can
be detected by the scan head again picking up data corresponding to free space. Another method is to start and/or stop the recorded data a predetermined number of scan readings from the leading edge. Assuming that the article always moves past the scan head at approximately the same speed, this would result in a consistent scan area. Another alternative is to use actual marks on the article to start and stop the scan region, although this may require more work, in terms of data processing, to determine which captured data corresponds to the scan area and which data can be discarded.

Thus there has now been described an number of techniques for scanning an item to gather data based on an intrinsic property of the article, compensating if necessary for damage to the article or non-linearities in the scanning process, and comparing the article to a stored signature based upon a previous scan of an article to determine whether the same article is present for both scans.

When using a biometric technique such as the identity technique described with reference to Figures 1 to 14 above for the verification of the authenticity or identity of an article, difficulties can arise with the reproducibility of signatures based upon biometric characteristics. In particular, as well as the inherent tendency for a biometric signature generation system to return slightly different results in each signature generated from an article, where an article is subjected to a signature generation process at different signature generation apparatuses and at different times there is the possibility that a slightly different portion of the article is presented on each occasion, making reliable verification more difficult.

Examples of systems, methods and apparatuses for addressing these difficulties will now be described. First, with reference to Figure 15, a multi-scan head signature generation apparatus for database creation will be described.

As shown in Figure 15, a reader unit 100 can include two optic subassemblies 20, each operable to create a signature for an article presented in a reading volume 102 of the reader unit. Thus an item presented for scanning to create a signature for
recording of the item in an item database against which the item can later be verified, can be scanned twice, to create two signatures, spatially offset from one another by a likely alignment error amount. Thus a later scan of the item for identification or authenticity verification can be matched against both stored signatures. In some examples, a match against one of the two stored signatures can be considered as a successful match.

In some examples, further read heads can be used, such that three, four or more signatures are created for each item. Each scan head can be offset from the others in order to provide signatures from positions adjacent the intended scan location. Thus greater robustness to article misalignment on verification scanning can be provided.

The offset between scan heads can be selected dependent upon factors such as a width of scanned portion of the article, size of scanned are relative to the total article size, likely misalignment amount during verification scanning, and article material.

Thus there has now been described a system for scanning an article to create a signature database against which an article can be checked to verify the identity and/or authenticity of the article.

An example of another system for providing multiple signatures in an article database will now be describe with reference to Figure 16.

As shown in Figure 16, a reader unit 100' can have a single optic subassembly 20 and an alignment adjustment unit 104. In use, the alignment adjustment unit 104 can alter the alignment of the optics subassembly 20 relative to the reading volume 102 of the reader unit. Thus an article placed in the reading volume can be scanned multiple times by the optics subassembly 20 in different positions so as to create multiple signatures for the article. In the present example, the alignment adjustment unit 104 can adjust the optics subassembly to read from two different locations. Thus a later scan of the item for identification or authenticity verification can be matched
against both stored signatures. In some examples, a match against one of the two stored signatures can be considered as a successful match.

In some examples, further read head positions can be used, such that three, four or more signatures are created for each item. Each scan head position can be offset from the others in order to provide signatures from positions adjacent the intended scan location. Thus greater robustness to article misalignment on verification scanning can be provided.

The offset between scan head positions can be selected dependent upon factors such as a width of scanned portion of the article, size of scanned are relative to the total article size, likely misalignment amount during verification scanning, and article material.

Thus there has now been described another example of a system for scanning an article to create a signature database against which an article can be checked to verify the identity and/or authenticity of the article.

Although it has been described above that a scanner used for record scanning (i.e. scanning of articles to create reference signatures against which the article can later be validated) can use multiple scan heads and/or scan head positions to create multiple signatures for an article, it is also possible to use a similar system for later validation scanning.

For example, a scanner for use in a validation scan may have multiple read heads to enable multiple validation scan signatures to be generated. Each of these multiple signatures can be compared to a database of recorded signatures, which may itself contain multiple signatures for each recorded item. Due to the fact that, although the different signatures for each item may vary these signatures will all still be extremely different to any signatures for any other items, a match between any one record scan signature and any one validation scan signature should provide sufficient confidence in the identity and/or authenticity of an item.
A multiple read head validation scanner can be arranged much as described with reference to Figure 15 above. Likewise, a multiple read head position validation scanner can be arranged much as described with reference to Figure 16 above. Also, for both the record and validation scanners, a system of combined multiple scan heads and multiple scan head positions per scan head can be combined into a single device.

In e-commerce systems and similar systems, entitlement to value, goods or services can be transferred at a time and/or location which is remote from a physical possession transfer of the value, goods or services. Thus a vendor or merchant may wish to ensure that payment is being made genuinely by the true holder of a bank or credit card account before shipping goods or issuing a token indicating entitlement to services. In this regard, it is worth noting that under certain regulatory regimes as regards credit cards, liability for fraudulently made transactions can be the responsibility of the vendor rather than the credit card issuer. For example, under UK law, any transaction performed where the card is not physically presented to the vendor for authorisation is categorised as a "Cardholder Not Present" or "Card Not Present" transaction. In such circumstances, an "authorisation" performed on the card account by an issuing bank does not guarantee to the person accepting payment from the card that the bank will release the funds to that person. Such an "authorisation" means only that the card has not been reported lost or stolen, and that the card holder has sufficient funds available in their account to pay for the transaction. Should a transaction be fraudulently made in a Card Not Present situation, and the cardholder subsequently challenge the validity of the transaction, the value of the transaction can and often is charged to the vendor who accepted the fraudulent payment by the issuing bank. Thus a vendor may desire a higher level of security that a person making a Card Not Present transaction is in fact the account holder and that the card that is being used for payment is in the possession of that account holder.

Thus, in the present example, a system, apparatus and method for increasing fraud resistance in the successful operation of such systems is presented. According to this system, method and apparatus, a physical credit card can be independently
validated to ensure that a purchaser using the card to make a purchase is in possession of the card at the time of making the purchase.

Suitable systems for effecting this security provision will be described in the following examples, making reference to various real-world applications in which the security provision can be applied.

One example is where a person uses an on-line shopping facility to purchase a ticket for access to an event or for travel using a conventional credit card. In this example, the user places an order for the ticket using an online portal provided for the purpose by a ticket vendor or supply agency. During the purchase process, the purchaser is requested to provide a scan of their credit card being used for payment for the ticket. This is in addition to a request for any other security information that the vendor may request, such as name and address details of the cardholder, the card number, expiry date etc and/or a password or personal identification number associated with the card or the purchaser's account with the vendor. Data gathered from the scan of the credit card can be used to create a signature based upon an intrinsic property of the credit card which cannot be duplicated by creating a new card having the same appearance as the original card. The signature can then be sent to a card authorisation entity to be compared with a signature generated from a previous scan of the user's credit card stored by the card authorisation entity. The previous scan used to create the database signature can be taken by the card issuer upon creating the card for sending out to the account holder, or after receipt of the card by the card holder upon attendance by the card holder with their card at an authorised premises where the identity of the card holder can be checked before the database signature is created. Thus it can be verified by the vendor, prior to accepting the transaction, that the physical card is in the possession of the person making the transaction. Thereby the vendor can be more confident that the transaction can be accepted, particularly if the "traditional" checks have been performed and it has been established that the card has not been reported lost or stolen. The clear implication of positive results from these two checks is that, as the account holder is in possession of the card (not lost or stolen) and the card is present for the making of the transaction
(matching signature), the account holder must be the individual placing the order and thus the chances of the transaction being fraudulent are significantly reduced compared to merely knowing that the card is not reported lost or stolen.

This process is illustrated in Figure 17. As shown in Figure 17, an e-commerce environment 201 includes a user terminal 208 by means of which a user can access a purchase mechanism for goods or services from a vendor 205 via a network 206 such as the Internet. This purchase mechanism can be any conventional system for allowing a remote user to purchase goods or services through a shopping or ordering portal. Such online remote ordering systems are used by many businesses, charities and governments. The process of purchasing the goods or services can, for example, be performed using an online shopping basket system where a user views one or more items which he can select for purchase.

Once one or more items have been selected by the user, a purchase operation can be performed in which the user enters details to authorise a transaction for purchase of the selected goods or services. This may include entering details of a credit card or debit card using which the user wishes to perform the transaction, as well as details such as a requested delivery time and location for the items. The transaction processing of the present example, also includes the user scanning their credit or debit card at the user terminal 208 using a scanner 210 in data communication with the terminal. The scanner 210 may be a separate unit operable to communicate with the user terminal 208 via a cable or wireless connection or may be integral to the user terminal 208.

The scan of the user's credit or debit card is used to generate a signature for based on an intrinsic property of the card. The scanner 210 can be a scanner as described above with reference to any of Figures 1 to 15. Thus in the present example, the signature is based upon the physical surface of the card, measured at a microscopic level. This signature is thus unique to that card, and a copy of the card would have a different signature if scanned in the same way, as discussed above with reference to figures 1 to 16. This signature is then transmitted from the user terminal
208 to a provider 203, in some examples via the vendor 205. This transmitted
signature can be encrypted to prevent third parties copying the signature during
transmission. This encryption can be effected using conventional data encryption
techniques such as a public key encryption and, in the case of an internet transaction,
may use a secure socket layer encryption scheme. The provider 203, which can be a
bank or an entity authorised to provide funds clearing services on behalf of one or
more banks, can have a database 204 of signatures taken from issued credit and debit
cards. A signature received by the provider as part of an online transaction can be
checked against the database 204. If a match is found in the database, then it can be
determined that an issued credit or debit card is being used for the transaction.
Further, the database can contain information describing the cardholder such that a
cross-check can be performed to ensure that the supplied card details from the user
match the cardholder details in the database. The provider can, in the case of a
positive match result, indicate to the vendor 205 that the card is genuine such that the
vendor can base a decision on whether to allow the transaction to go ahead on that
information.

Thus, it can be established that a credit or debit card offered for payment in a
remote transaction is not lost or stolen, and that sufficient funds are available for the
payment, and that the user initiating the transaction is in possession of the physical
card against which the other checks have been performed. Thereby a large degree of
certainty that fraudulent behaviour is not occurring during a card not present
transaction can be achieved.

As the card is authenticated against a signature generated from that same card
at an earlier time, copies of the card will fail the validation test as they will have been
made using a material sheet having a different intrinsic property to that of the sheet of
the validated card. Thereby, fraud on the part of persons acquiring details of the card
to obtain goods or services using someone else's account can be prevented.

Thus there has now been described an example of a system for a card to be
used at a location convenient for a purchaser of goods or services, and for a merchant
relying on the genuine nature of the card for payment for goods or services to be able to validate the card for authentication when the card is used in a card not present type transaction. Thereby fraudulent reproduction of a credit or debit card can be prevented without subjecting the purchaser to a need to travel to an inconvenient location to make a purchase.

In the above, it has been described that a database 204 of signatures for issued cards be pre-existent at the provider 203. These signatures can be obtained by a card issuer upon issue of the card to a user. Thus where cards are distributed by postal means, the signature can be taken by the issuing authority prior to shipment of the card to the cardholder. To provide an additional layer of security, the cardholder can be requested to scan the card at a user terminal and to transmit a signature generated from that scan to the provider 203 in order to validate the card for use. In such an example, only if the signature transmitted from the user terminal for validation matches the signature in the database would the card be activated for use by the cardholder. Such a provision would prevent fraud by staff of the issuing authority sending out a card different to the card which had been scanned, thus enabling the staff member to keep the scanned card for their own use or for sale to a third party to use in making transactions against the account of the cardholder without the cardholder's permission.

In another example, the scan of the card to create the signature for the database 204 could be made in the presence of both a representative of the issuing authority and the cardholder. In such a circumstance the scanned area of the card could include a signature space on the card where the cardholder has already written their signature. Thus the scan of the card for a later remote transaction includes a check that the card has not been tampered with to alter or replace the signature.

In either of the above examples for taking the initial "validation" scan of the card, the scanned area may include different portions of the card. Examples of this are shown in Figures 18A, 18B and 18C where various examples of cards 220 are depicted. In these figures, a scan area 221 is depicted using a dashed line as there is
no requirement for this area to be marked or indicated on the card in any way. As shown in Figure 18A, the scanned area 221 may include a portion of surface of the card with no coverings or printings 222, and a portion of a magnetic strip 223 provided on the card for reading using a conventional magnetic strip reader. As shown in Figure 18B, the scanned area 221 may include a portion of a signature region 224, as discussed above, and a portion of one or more numerals, letters, images or logos 225, 226 imprinted onto or into the card. As shown in Figure 18C, the scanned area 221 may include a portion of the card onto or into which a memory chip 227 has been embedded (such as in a so-called "smart-cards").

In addition to the examples of credit and debit cards given above, a variety of other payment authorisation tokens or value tokens may be used for remote transactions. Examples of other token types include loyalty cards (where a card holder receives "points" or other value indicators which can be used to claim shopping discounts, special offers or selected products), vouchers certificates, coupons etc, all of which can in certain circumstances be used to purchase goods and/or services, or to obtain discounts from the purchase of goods and/or services.

Thus there have now been described a number of examples of systems which can use a signature for a payment authorisation article which is based upon an intrinsic property of that article to provide further security and/or confidence to a transaction system where remote access is provided to authorise payment using the article.

Although the above examples have been described in the context of the coherent light based signature generation scheme described in detail above, the systems can also be implemented using, for example a signature generation scheme based upon, for example, analysis of magnetic field of an article.

Although the above examples have been described in the context of a payment authorisation article which is a plastic credit or debit card. However, any article which performs the function of a payment authorisation article may be used in
systems such as those described above. For example, the payment authorisation
article may be made from an alternative substrate, such as cardboard or metal. Also,
it is common for plastic cards to be overlaid with a paper layer, at least in parts to
make printing onto the card easier for the card issuer. Thus a signature from a
"plastic" card may include signature portions from plastic and/or paper materials. As
a paper or cardboard surface is in most circumstances rougher than the surface of a
plastic item (giving a correspondingly greater uniqueness measure), it may be
desirable where a greater resistance to fraud is desired to employ tokens having at
least a paper or card portion from which a signature can be generated. In other
examples, it may be desirable to use a plastic token with a matt surface over and
above a plastic item with a glossy surface. Such a matt surface could be created only
for a portion of the token, or for the entire token. A matt surface could be created on
a glossy plastic token using, for example, chemical or mechanical roughening.

In some examples, the payment authorisation article may be "printed" with the
signature determined from scanning the article. This could be done in the form of
writing token data to a magnetic strip or embedded chip of a plastic card, such as the
plastic cards commonly used for bank cards and credit cards. This could be
performed using a scanner such as those discussed with reference to Figures 6B and
6C above, which scanner could optionally be additionally equipped with a writing
head such that the writing and scanning could take place simultaneously in the same
device. The plastic card could be scanned, optionally including at least a surface
portion including the magnetic strip or embedded chip as discussed above, to create
the signature for validation of that card.

Although the embodiments above have been described in considerable detail,
numerous variations and modifications will become apparent to those skilled in the art
once the above disclosure is fully appreciated. It is intended that the following claims
be interpreted to embrace all such variations and modifications as well as their
equivalents.
CLAIMS

1. A method for authenticity verification, the method comprising:
   conducting a transaction between first and second parties, the parties being respectively located at first and second locations remote one-another, the outcome of the transaction being the transfer of title to goods and/or services from the first party to the second party;
   capturing data describing a value entitlement token of the second party to create a signature for the value entitlement token, the signature being created by directing a coherent beam onto the value entitlement token, collecting a set comprising groups of data points from signals obtained when the coherent beam scatters from the value entitlement token, wherein different ones of the groups of data points relate to scatter from respective different parts of the value entitlement token, and processing the set of groups of data points;
   transmitting the signature from the second party to a third party;
   comparing the signature to a database of stored signatures at the third party; and
   transmitting from the third party to the first party a validation result indicating whether the value entitlement token corresponds to a value entitlement token signature in the database.

2. The method of claim 1, wherein the first and third parties are co-located.

3. The method of claim 1 or 2, wherein the outcome of the transaction is dependent upon the validation result.

4. The method of any preceding claim, wherein the value entitlement token is at least one of a credit card, a debit card, a loyalty card, a voucher, a certificate and a token.

5. The method of any preceding claim, wherein the third party is a payment clearing authority.
6. The method of any preceding claim, further comprising transmitting from the second party to the first party data describing the value entitlement token and/or a user thereof.

7. The method of claim 6, further comprising comparing the data describing the value entitlement token and/or the user to a database describing invalid value entitlement tokens and/or users to create an authorisation result.

8. The method of claim 7, wherein the outcome of the transaction is dependent upon a combination of the validation result and the authorisation result.

9. The method of any preceding claim, wherein the comparing comprises: splitting the signature into blocks of contiguous data and performing a comparison operation between each block and respective blocks of stored ones of the signatures from the database of stored signatures.

10. The method of any preceding claim, wherein, in the event that the comparison step indicates substantial identity between attributes of the signature and a signature from the database of stored signatures, a positive validation result is returned.

11. The method of any preceding claim, wherein, in the event that the comparison step does not indicate substantial identity between attributes of the signature and a signature from the database of stored signatures, a negative validation result is returned.

12. The method any preceding claim, wherein the signatures in the database of stored signatures include a signature of the value entitlement token made from a scan of the value entitlement token previous to the commencement of the transaction.

13. The method of any preceding claim, wherein the first location comprises an e-commerce server or a computer terminal.
14. The method of any preceding claim, wherein the second location comprises a computer terminal.

15. A system for authenticity verification, the system comprising:
first and second computer systems remote one-another and operable to communicate therebetween via a data communications channel, wherein the first computer system is operable to enable a user at the second computer system to conduct a transaction with the first computer system, the outcome of the transaction being the provision by the first computer system to the user of entitlement to goods and/or services;

a signature generator co-located with the second computer system and operable to create a signature for a value entitlement token of the user, the signature generator operable to create the signature by directing a coherent beam onto the value entitlement token, collecting a set comprising groups of data points from signals obtained when the coherent beam scatters from the value entitlement token, wherein different ones of the groups of data points relate to scatter from respective different parts of the value entitlement token, and processing the set of groups of data points, the second computer system being operable to transmit the signature to a third computer system;

the third computer system being operable to compare the signature to a database of stored signatures, to produce a validation result indicating whether the value entitlement token corresponds to a value entitlement token signature in the database and the third computer system being further operable to transmitting the validation result to the first computer system.

16. The system of claim 15, wherein a single computer system comprises the first and third computer systems.

17. The system of claim 15 or 16, wherein the outcome of the transaction is dependent upon the validation result.
18. The system of any of claims 15 to 17, wherein the value entitlement token is at least one of a credit card, a debit card, a loyalty card, a voucher, a certificate and a token.

19. The system of any of claims 15 to 18, wherein the third computer system is representative of a payment clearing authority.

20. The system of any of claims 15 to 19, wherein the second computer system is further operable to transmit data describing the value entitlement token and/or data describing a user thereof to the first computer system.

21. The system of claim 20, wherein the first computer system is further operable to cause the data describing the value entitlement token and/or the user to a database describing invalid value entitlement tokens and/or users to create an authorisation result.

22. The system of claim 21, wherein the outcome of the transaction is dependent upon the validation result and the authorisation result.

23. The system of any of claims 15 to 22, wherein the third computer system is operable to split the signature into blocks of contiguous data and to perform a comparison operation between each block and respective blocks of stored ones of the signatures from the database of stored signatures.

24. The system of any of claims 15 to 23, wherein the validation result is positive if there is determined to be substantial identity between the signature and a signature from the database of stored signatures.

25. The system of any of claims 15 to 24, wherein the validation result is negative if there is determined not to be substantial identity between the signature and a signature from the database of stored signatures.
26. A method for authenticating a value transfer token, the method comprising:
scanning a value transfer token, selected from a group comprising a credit
 card, a bank card, a loyalty card, a voucher, a certificate and a token, to create a
signature by directing a coherent beam onto the value transfer token, collecting a set
comprising groups of data points from signals obtained when the coherent beam
scatters from the value entitlement token, wherein different ones of the groups of data
points relate to scatter from respective different parts of the value entitlement token,
and processing the set of groups of data points;
transmitting the signature to a comparison entity operable to compare the
signature to a database of stored signatures; and
creating an authentication result based upon an outcome of the comparison.

27. The method of claim 26, further comprising:
transmitting data describing the token and/or a token holder to a validation
entity;
comparing the data to a database of invalid tokens and/or token holders; and
creating a validation result based upon an outcome of the comparison.

28. The method of claim 27, wherein the database of stored signatures and the
database of invalid tokens and/or token holders are a single database.

29. The method of claim 27 or 28, further comprising using the authentication
result and the validation result to determine whether the token is to be accepted as
payment.

30. A system substantially as hereinbefore described, with reference to Figures 14
or 15.

31. Apparatus substantially as hereinbefore described.

32. A method substantially as hereinbefore described.
Fig. 2
Fig. 4
Fig. 8A

Fig. 8B
START SCAN

S1 SCAN TO ACQUIRE DATA

S2 LINEARISE DATA

S3 DIFFERENTIATE & SMOOTH

S4 COMPUTE AND SUBTRACT MEAN

S5 DIGITISE TO OBTAIN DIGITAL SIGNATURE

S6 DIGITISE TO OBTAIN THUMBNAIL DIGITAL SIGNATURE

S7 COMPUTE CROSS-CORRELATION COEFFICIENTS

S8 COMPUTE AVERAGE VALUES

END SCAN

Fig. 10
START VERIFY

V1
SCAN ARTICLE (STEPS S1-S8)

V2
SEARCH THUMBNAILS TO FIND HIT

V3
PRE-SCREEN HIT USING AVERAGE VALUE

V4
PRE-SCREEN HIT USING CROSS-CORRELATION COEFFICIENTS

V5
ANALYSE DIGITAL SIGNATURE OF HIT

V6
ISSUE RESULT

END VERIFY

Fig. 11
11/16

START

S21 SCAN TO Acquire DATA

S22 BREAK SCAN DATA INTO CONTIGUOUS BLOCKS

S23 COMPUTE CROSS-CORRELATION COEFFICIENTS

S24 COMPARE LOCATION OF CROSS-CORRELATION PEAKS TO EXPECTED LOCATION

S25 FIT SELECTED FUNCTION TO COMPARED POSITIONS

S26 CHECK DEVIATIONS FROM FUNCTION TO DETERMINE CHANGE PARAMETERS

S27 STRETCH AND SHIFT SCANNED DATA TO COMPENSATE FOR CHANGE PARAMETERS

S28 BREAK COMPENSATED SCAN DATA INTO CONTIGUOUS BLOCKS

S29 COMPUTE CROSS-CORRELATION COEFFICIENTS

S30 CALCULATE UNIQUENESS

END

Fig. 12
12/16

Fig. 13A

Gradient = 1

Fig. 13B

Gradient ≠ 1

offset

Fig. 13C
INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2006/002688

A CLASSIFICATION OF SUBJECT MATTER
INV. G07F7/08 G07D7/12

According to International Patent Classification (IPC) and both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G07D

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)
EPO-Internal

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>UO 2004/057625 A (THALES [FR]; COLINEAU JOSEPH [FR]; LEHUREAU JEAN-CLAUDE [FR]; BINET RE) 8 July 2004 (2004-07-08) abstract</td>
<td>1-29</td>
</tr>
<tr>
<td>X</td>
<td>GB 2 221 870 A (DE LA RUE CO PLC [GB]) 21 February 1990 (1990-02-21) cited in the application abstract</td>
<td>1-29</td>
</tr>
<tr>
<td>X</td>
<td>DE 196 12 819 A1 (BRINCKMANN WILLI [DE]) 2 October 1997 (1997-10-02) column 1, line 42 - column 2, line 42</td>
<td>1-29</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C

See patent family annex

Date of the actual completion of the international search
13 December 2006

Date of mailing of the international search report
27/12/2006

Name and mailing address of the ISA/
European Patent Office P B 581 B Patentsstraat 2 NL-2280 HV Rijswijk Tel (+31-70) 340-2040, Tx 31 BE 1 spo nl Fax (+31-70) 340-3016

Authorized officer

Mez δ i, Stephan
Continuation of Box II.2

Claims Nos.: 30-32

Either the subject-matter of claims 30-32 is identical to the previous claims, in this case a search is not necessary, or it is different, in this case it is not possible to perform a search, because the difference is not described in the claims.

The applicant's attention is drawn to the fact that claims relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure. If the application proceeds into the regional phase before the EPO, the applicant is reminded that a search may be carried out during examination before the EPO (see EPO Guideline C-VI, 8.5), should the problems which led to the Article 17(2) declaration be overcome.
This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. [ ] Claims Nos.: because they relate to subject matter not required to be searched by this Authority, namely:

2. [X] Claims Nos.: 30-32 because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
   
   see FURTHER INFORMATION sheet PCT/ISA/210

3. [ ] Claims Nos.: because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

This International Searching Authority found multiple inventions in this international application, as follows:

1. [X] As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. [ ] As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest: [ ] The additional search fees were accompanied by the applicants protest.

[ ] No protest accompanied the payment of additional search fees.
<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>US 2003156294 A1</td>
<td>21-08-2003</td>
<td>AT 260495 T</td>
<td>15-03-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 5483001 A</td>
<td>20-11-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2407433 A1</td>
<td>15-11-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 60102150 D1</td>
<td>01-04-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 60102150 T2</td>
<td>26-08-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DK 1281161 T3</td>
<td>05-07-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1281161 A1</td>
<td>05-02-2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ES 2215896 T3</td>
<td>16-10-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 200353536 T</td>
<td>18-11-2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LU 90580 A1</td>
<td>09-11-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NO 20025345 A</td>
<td>08-01-2003</td>
</tr>
<tr>
<td>WO 2004057525 A</td>
<td>08-07-2004</td>
<td>AU 2003298351 A1</td>
<td>14-07-2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1745387 A</td>
<td>08-03-2006</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1573661 A1</td>
<td>14-09-2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FR 2849245 A1</td>
<td>25-06-2004</td>
</tr>
<tr>
<td>GB 2221870 A</td>
<td>21-02-1990</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>DE 19612819 A1</td>
<td>02-10-1997</td>
<td>NONE</td>
<td></td>
</tr>
</tbody>
</table>