(12) UK Patent Application (19) GB (11) 2 346 460 (13) A

(43) Date of A Publication 09.08.2000

(21) Application No 9902311.1

(22) Date of Filing 02.02.1999

(71) Applicant(s)
De La Rue International Limited
(Incorporated in the United Kingdom)
De La Rue House, Jays Close, Viables, BASINGSTOKE, Hampshire, RG22 4BS, United Kingdom

(72) Inventor(s)
John Martin Haslop

(74) Agent and/or Address for Service
Gill Jennings & Every
Broadgate House, 7 Eldon Street, LONDON, EC2M 7LH, United Kingdom

(51) INT CL[7]
G06F 1/00 12/14

(52) UK CL (Edition R)
G4A AAP

(56) Documents Cited
GB 2253080 A **GB 2204970 A** **GB 2198567 A**
WO 97/45783 A1 **WO 91/17524 A1** **US 5182770 A**
US 4458315 A

(58) Field of Search
UK CL (Edition R) **G4A AAP**
INT CL[7] **G06F**

(54) Abstract Title
Authenticating an item

(57) A method for use in authenticating an item carrying a security feature, comprises:
a) inspecting the security feature; and,
b) performing an algorithm on the result of inspecting the security feature to generate a result indicative of, or from which can be determined, the authenticity of the item
wherein one or both of steps a) and b) can only be performed following the supply of data from a separate source.
The item may hold computer software, to be protected from software piracy.

GB 2 346 460 A

Fig.1.

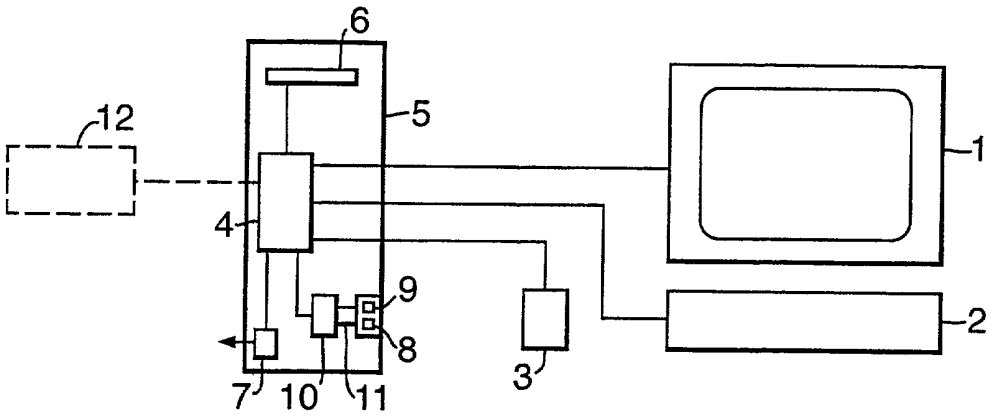


Fig.2.

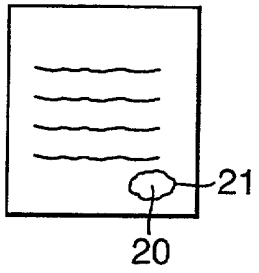
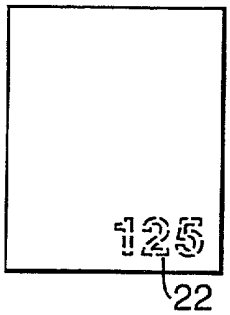


Fig.3.



PROCESSING ASSEMBLY AND METHOD

Considerable expenditure is being incurred by computer software and hardware manufacturers to reduce the problem of software piracy. One successful approach has been to package genuine software carriers such as CD ROMs in secure packaging which includes a security feature such as a hologram enabling the purchaser to confirm that the contents are genuine while allowing computer software manufacturers to police retailers to check that they are only selling genuine versions of the software.

There is a need, however, to decrease still further the ability to supply non-genuine electronic data carriers while there is also a need to be able to achieve authentication remotely when the security feature supplied with a genuine electronic data carrier cannot be viewed by the authenticator.

In accordance with one aspect of the present invention, a method for use in authenticating an item carrying a security feature comprises:

a) inspecting the security feature; and,

b) performing an algorithm on the result of inspecting the security feature to generate a result indicative of, or from which can be determined, the authenticity of the item

wherein one or both of steps a) and b) can only be performed following the supply of data from a separate source.

This invention enables a security feature to be authenticated under known conditions and prevents the possibility of a person overriding the authentication process. Thus, one or both of steps a) and b) can only be carried out following the supply of the data from a separate source.

A large number of different applications of this invention are possible. For example, in a simple application, the data is supplied from a remote source.

This could be supplied via a communications link such as a telephone line, cable or the internet.

In other applications, data may be supplied on a portable carrier which in many cases will be associated with the item carrying the security feature. For example, the item could constitute the portable carrier or alternatively the item could comprise packaging or a manual associated with the portable carrier. The portable carrier itself is preferably an electronic data storage device such as a floppy disk, CD, tape, Zipdrive, smart card, or DVD.

A particularly important application of this invention is for use with electronic data storage devices which carry computer software since the invention provides a way in which the authenticity of that software can be determined.

The data itself can comprise, in a simple case, a key to activate one or both of steps a) and b). The key may be in the form of a password or the like, including one which varies with the day, or it could enable software for carrying out one or both of steps a) and b) to be decrypted if it is in an encrypted form. In some examples, the data may provide both a password and a decryption key.

In other applications, the data may comprise all or part of software defining the algorithm.

In a particularly preferred application, the item is associated with an electronic data storage device, the data being obtained from an auxiliary storage device supplied in association with the electronic data storage device and the item.

The auxiliary storage device may be reprogrammable so that, for example, it could be provided by a device which is carried by a user for other purposes, such as a smart card, but which can be loaded with the appropriate data when the user purchases the electronic data storage device (for example a CD ROM carrying software).

Some examples of applications will now be described.

It is common for a computer software supplier to provide a help desk or the like which can be contacted by

a user if he is unable to operate a computer program which he has purchased. However, the help desk wishes to know whether the user has a genuine copy of the computer software. With the present invention, the remote help desk can instruct the local user to arrange for his computing device to inspect the security feature on the item (for example the security feature might be located on an instruction manual for the software or part of the packaging or the software carrier). If the algorithm for performing step b) is already located on the computing device, the help disk then applies a key which might be related to the time of day etc., that key enabling the algorithm to be performed. For example, the algorithm could be performed by software which is normally encrypted, the key allowing the software to be decrypted.

In the example defined above, the algorithm software is already loaded on the computing device. Further security is achieved if that algorithm is located on the carrier which carries the purchased software. In that case, the algorithm software will be downloaded into the computing device to enable the algorithm to be performed.

In another arrangement, the software defining the algorithm is supplied from a remote source such as the help desk, from another data carrier, such as a smart card, or the like.

In all these cases, the algorithm is then performed and the result of carrying out the algorithm may simply be returned to the help desk for subsequent analysis or the computing device itself could determine whether or not a predetermined condition indicating authenticity is satisfied.

For example, in a simple case, the presence or absence of the security feature may be determined in step a) while the algorithm generates a code which depends at least in part on the result of step a). The code could simply indicate whether or not the security feature is present.

This information could then be displayed locally or transmitted to a remote site for analysis.

In a more sophisticated approach, the algorithm could make a determination of whether or not a predetermined condition is satisfied indicating a successful match between the security feature and an electronic data carrier. For example, a successful match could be established by determining the content of the electronic data carrier, for example a program name, performing an algorithm based on the name or an equivalent value and the result of inspecting the security feature to generate a resultant value which is then compared with a value which is expected if a match is achieved. That final value could be prestored on the electronic data carrier or supplied from a remote source.

It will be appreciated, that the intervention of a remote source is not essential in all cases and the method could be used as a self-check when an electronic data carrier is first activated, the computing device instructing the user appropriately so as to obtain the necessary information about the security feature and then performing the algorithm and only permitting further running of the program stored in the electronic data carrier if a successful match is achieved. In some cases, this check could be required on each occasion the program is to be run.

The simple determination of the presence or absence of the security feature can lead to a relatively sophisticated check by using certain security features which are not obvious to the average user. Thus, security features which are normally concealed such as luminescent, fluorescent, magnetic, stokes and anti-stokes features could be used.

Further sophistication can be achieved if the security feature defines additional information, for example in the form of a code. Thus, in the case of magnetic features or many optical features, the feature could be arranged to

define a code number or the like. Step b) could include locating the code from the inspected security feature.

In some of the examples mentioned above, the data enabling one or both of steps a) and b) to be performed is supplied on a carrier. This could be in the form of a CD ROM or other software carrier as mentioned above but could also be in the form of a smart card.

Other carriers include a floppy disc, CD, tape, Zipdrive, DVD and the like both read only and read/write or a remote data carrier from which data is obtained via a communication medium such as a network, telephone or internet.

The security feature may comprise any conventional security feature, for example of the type used on banknotes and other documents of value and particularly including

a) optical devices such as infra-red, visual, and ultraviolet devices and including anti-stokes, stokes, fluorescent, luminescent and phosphorescent devices;

b) conductive metallic devices;

c) magnetic devices including hard and soft magnetics; and,

d) photochromic and thermochromic inks.

Furthermore, the security feature may be chosen from the group comprising:

a) coded or simple features; and

b) holograms, diffraction gratings and kinegrams.

Step a) could be carried out by a purpose built security feature reading device, for example of the type used with conventional security features, or with a conventional peripheral input device such as a scanner. The type of device will depend upon the security feature which is to be inspected.

In accordance with a second aspect of the present invention, a processing assembly comprises a processor; a user input device and a display coupled to the processor; and an auxiliary, security feature reading device coupled to the processor and located such that an item carrying a

security feature can be presented to the reading device, the processor being programmed or programmable to determine the presence of the security feature from signals supplied by the reading device.

The processing assembly may be made of separate components and in the preferred example, the processor is provided in a Personal Computer (PC). The auxiliary, security feature reading device may be in the form of a peripheral such as a scanner, or in some cases could be included within the same housing as the processor. Thus, where the processor is located in a Personal Computer, the PC could also include the security feature reading device.

In a further alternative, the security feature reading device may be formed as two parts, one part which is common to many computing devices and a second part, separable from the first, and containing information relating to a particular security feature. This second part would be chosen in accordance with the information to be obtained from the security feature and might be sold with an electronic data carrier. For example, the second part could include a suitable filter through which radiation passes to irradiate the security device, the wavelengths passing through the filter being chosen to be appropriate to a genuine security device. The second part would then be fitted to the first part which would have been supplied with the computing device.

The security feature reading device will typically be controlled by the processor which will be suitably programmed to do this. For example, in the case of a luminescent or fluorescent feature, the processor would be programmed to illuminate and then detect radiation emitted by the security feature.

It should be understood that where data is supplied to or from a remote source it may be encrypted, with suitable decryption software being provided at the receiving end and the same may be the case with the data stored on the electronic data carrier.

The program to which the processor responds to determine the presence of a security feature may be stored within the processor or on a separate carrier such as a smart card, a smart card reader being coupled with the processor.

In some cases, the security feature reading device can carry out more than one type of inspection of the security feature. This may be because it includes more than one type of detector (for example magnetic or optical) or because it is capable of detecting a feature at different levels of sensitivity (for example the presence or absence of a magnetic feature at one level and the strength of the magnetic feature at a second, higher level). The selection of the appropriate inspection method could be determined by the data supplied from the separate source.

Some examples of methods and processing assemblies according to the invention will now be described with reference to the accompanying drawings, in which:-

Figure 1 is a schematic, block diagram of a processing assembly;

Figure 2 illustrates schematically a first example of an item carrying a security feature; and,

Figure 3 is a view similar to Figure 2 but illustrating a second security feature.

The processing assembly shown in Figure 1 is based on a conventional PC and includes a monitor 1, keyboard 2 and mouse 3 all connected to a microprocessor 4. The microprocessor 4 is located within a housing 5 which also supports a CD ROM reader 6 and a modem 7. A recess 8 is located in one wall of the housing 5 into which a radiation emitter/detector part 9 of a security feature reading device can be located. A second part of the device is shown at 10 within the housing 5 and is linked to the first part 9 via wires 11. The part 9 is connected to the wires 11 via suitable, separable jack plugs or the like.

In a first example, the authentication of a CD ROM carrying a program such as a game playing program will be

described. The CD ROM will also carry authentication algorithm software and be packaged with a manual having a back page shown in Figure 2 which includes a security feature 20. This security feature 20 is not visible to the naked eye and is in the form of an anti-stokes device.

When the CD ROM is loaded into the reader 6 and the user instructs installation, initially only the authentication algorithm software is downloaded into the processor 4. This algorithm then runs and instructs the user to place the lower right hand corner of the page of the manual adjacent to the part 9 of the reading device. The microprocessor 4 then sends suitable signals to the part 10 which causes appropriate radiation to be emitted by the part 9 causing the characteristic anti-stokes response from the device 20 which is detected by the part 9, suitable signals being passed to the part 10 which provides a "feature present" signal to the microprocessor 4. In order to achieve accurate alignment, the area containing the device 20 is outlined in a visible manner as shown at 21.

In this simple example, the algorithm simply determines that the security device 20 has been detected and then authorises further processing of the software. Typically, this will be a one-off process and this existence of a successful match will be recorded permanently against the software loaded onto the PC.

In another example, instead of or in addition to the authentication algorithm software, the CD ROM includes a code which is downloaded into the microprocessor 4. This code acts as a key allowing the authentication algorithm to be performed.

As an alternative, the key could be supplied via the modem 7 from a remote source as explained earlier.

The authentication algorithm could also operate on a code defining the content of a CD ROM, for example identifying the software. In these more sophisticated examples, the result of the authentication algorithm may

not in itself establish authenticity or a successful match. Instead, the algorithm may generate a further code which must then be authenticated, typically at a remote location, for example via the modem. Following authentication, an access code is then transmitted to the microprocessor 4 allowing further use of the software.

Figure 3 illustrates an alternative form of security device in the form of a code number 22. In this case, the reading device 9,10 obtains sufficient information from the security device to determine the code number. The authentication algorithm may then simply compare the code number obtained from the CD ROM with the code number 22 and if they are the same authorise activation of the software. Alternatively, the code number 22 could be used within the authentication algorithm.

Figure 1 illustrates that an optional card reader 12 could be coupled to the microprocessor 4. This would be used to read a smart card (not shown) supplied with the CD ROM. The smart card will carry a code or software which is required by the microprocessor 4 in order to run the authentication algorithm and/or operate the security feature reading device. This could be required on a one-off basis to achieve initial running of the software or alternatively could be required to be present on each occasion on which the software is to be run.

The smart card may be supplied with the CD ROM so that they must be used together to achieve full authentication. Alternatively, the smart card may already be in the possession of the user for other purposes such as monetary transactions or the like and can be loaded with the appropriate data when the user purchases the software.

CLAIMS

1. A method for use in authenticating an item carrying a security feature, the method comprising:

a) inspecting the security feature; and,

b) performing an algorithm on the result of inspecting the security feature to generate a result indicative of, or from which can be determined, the authenticity of the item

wherein one or both of steps a) and b) can only be performed following the supply of data from a separate source.

2. A method according to claim 1, wherein some or all of the data is supplied from a remote source.

3. A method according to claim 2, wherein some or all of the data is supplied via a communications link such as a telephone line, cable connection or the internet.

4. A method according to any of the preceding claims, wherein some or all of the data is supplied on a portable carrier.

5. A method according to claim 4, wherein the portable carrier is associated with the item.

6. A method according to claim 5, wherein the portable carrier comprises an electronic data storage device.

7. A method according to claim 5 or claim 6, wherein the portable carrier comprises a floppy disk, CD, tape, Zipdrive, smart card, or DVD.

8. A method according to any of claims 5 to 7, wherein the item comprises packaging for the portable carrier.

9. A method according to any of claims 5 to 7, wherein the item comprises a manual for use with software stored on the portable carrier.

10. A method according to any of the preceding claims, wherein the data comprises a key to activate step a) and/or step b).

11. A method according to any of the preceding claims, wherein the data comprises software defining all or part of the algorithm.

12. A method according to any of the preceding claims, wherein the item is associated with an electronic data storage device, the data being obtained from an auxiliary storage device supplied in association with the electronic data storage device and the item.

13. A method according to claim 12, wherein the auxiliary storage device is reprogrammable.

14. A method according to claim 12 or claim 13, wherein the auxiliary storage device comprises a smart card.

15. A method according to any of the preceding claims, further comprising operating the computing device to determine whether or not a predetermined condition indicating authenticity is satisfied.

16. A method according to any of the preceding claims, wherein the security feature is selected from the group comprising:

a) optical devices such as infra-red, visual, and ultraviolet devices and including anti-stokes, stokes, fluorescent, luminescent and phosphorescent devices;

b) conductive metallic devices;

c) magnetic devices including hard and soft magnetics; and,

d) photochromic and thermochromic inks.

17. A method according to any of the preceding claims, wherein the security feature is chosen from the group comprising:

a) coded or simple features; and

b) holograms, diffraction gratings and kinegrams.

18. A method of authenticating an item carrying a security feature substantially as hereinbefore described with reference to any of the examples shown in the accompanying drawings.

19. A processing assembly comprising a computing device having a processor, and a user input device and a display

coupled to the processor; and an auxiliary, security feature reading device coupled to the processor and located such that an item carrying a security feature can be presented to the reading device, the processor being programmed or programmable to determine the presence of the security feature from signals supplied by the reading device.

20. An assembly according to claim 19, wherein the processor is or can be programmed to control operation of the reading device.

21. An assembly according to claim 19 or claim 20, wherein the reading device comprises a detector for detecting radiation emitted by, transmitted through or reflected by the security feature.

22. An assembly according to any of claims 19 to 21, wherein the reading device comprises a radiation emitter for emitting radiation to which the security feature responds.

23. An assembly according to claim 22, wherein the radiation comprises optical, for example i.r., visible or UV radiation, or a magnetic field.

24. An assembly according to any of claims 19 to 23, wherein the reading device can perform more than one type of inspection of the security feature.

25. An assembly according to any of claims 19 to 24, wherein the reading device includes a separate part adapted for use with the security feature.

26. An assembly according to any of claims 19 to 25, wherein the processor is programmed to perform an algorithm using the result of determining the presence of the security device to enable the authenticity of the item to be determined.

27. An assembly according to claim 26, further comprising an auxiliary reader for reading data defining the algorithm and/or data enabling the algorithm to be performed, the reader being coupled to the processor.

28. An assembly according to claim 27, wherein the reader is a smart card reader.

29. An assembly according to any of claims 19 to 28, further comprising means for connecting the processor to a remote data source.

30. An assembly according to any of claims 19 to 29, wherein the computing device includes a housing which supports at least the processor and the reading device.

31. An assembly according to claim 30, wherein the reading device is located within the housing, the housing having an aperture to enable the reading device to view a security feature on an item presented to it.

32. An assembly according to any of claims 19 to 31, wherein the computing device is a Personal Computer.

33. A processing assembly substantially as hereinbefore described with reference to any of the examples shown in the accompanying drawings.

34. An assembly according to any of claims 19 to 33, adapted to carry out a method of authenticating an item carrying a security feature according to any of claims 1 to 18.

14

Application No: GB 9902311.1
Claims searched: 1-18

Examiner: Mike Davis
Date of search: 18 April 2000

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.R): G4A (AAP)

Int Cl (Ed.7): G06F

Other:

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
A	GB 2253080 A	(DISTRIBUTION SYSTEMS & COMPUTERS) eg abstract	-
X	GB 2204970 A	(GENERAL ELECTRIC) whole document	1 at least
X	GB 2198567 A	(HEPTACON) whole document	"
X	WO 97/45783 A1	(TEXIER) whole document	"
X	WO 91/17524 A1	(SCANDIC...) whole document	"
X	US 5182770	(MEDVECZKY ET AL) whole document	"
X	US 4458315	(UCHENICK) whole document	"

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.