**PCT** WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00, 17/30

A1

(11) International Publication Number: **WO 98/03904**

(43) International Publication Date: 29 January 1998 (29.01.98)

(21) International Application Number: PCT/NO97/00185

(22) International Filing Date: 17 July 1997 (17.07.97)

(30) Priority Data:
962997 18 July 1996 (18.07.96) NO

(71)(72) Applicant and Inventor: SIGBJÖRNSEN, Sigurd [NO/NO]; Tykkåsen 52, N-4870 Fevik (NO).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: HAGLUND, Magne, Arild [NO/NO]; Gunder Danielsens vei 53, N-4890 Grimstad (NO). OLESHCHUK, Vladimir A. [UA/NO]; Landgraffs vei 20, N-4890 Grimstad (NO).

(74) Agent: J.K. THORSENS PATENTBUREAU A/S; P.O. Box 9276 Grönland, N-0134 Oslo (NO).

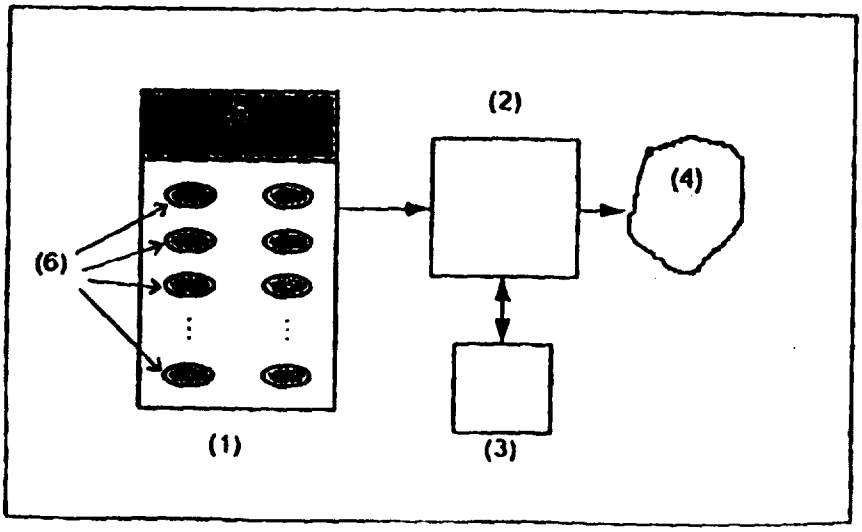
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

**Published**
*With international search report.*
*In English translation (filed in Norwegian).*

(54) Title: PROTECTION OF DATABASE CONTENTS AGAINST USE WITHOUT PERMIT

(57) Abstract

An arrangement is described for protecting items of information of a database against use without permit from the proprietor of the rights. By rendering meaningless an item of information in the database which is not to be exploited without permission, by encrypting or otherwise corrupting, or moving from the database to a storage location hidden to the user a function associated with the item of information for the control of the interpretation and presentation thereof to a user by a computer, this function becomes unavailable for the utilization in the computer of the user and hence, the corresponding item of information cannot be correctly interpreted. Thus, it will be possible to exploit such selected items of information stored in a database only with a corresponding authorization.



*FOR THE PURPOSES OF INFORMATION ONLY*

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

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **AL** | Albania | **ES** | Spain | **LS** | Lesotho | **SI** | Slovenia |
| **AM** | Armenia | **FI** | Finland | **LT** | Lithuania | **SK** | Slovakia |
| **AT** | Austria | **FR** | France | **LU** | Luxembourg | **SN** | Senegal |
| **AU** | Australia | **GA** | Gabon | **LV** | Latvia | **SZ** | Swaziland |
| **AZ** | Azerbaijan | **GB** | United Kingdom | **MC** | Monaco | **TD** | Chad |
| **BA** | Bosnia and Herzegovina | **GE** | Georgia | **MD** | Republic of Moldova | **TG** | Togo |
| **BB** | Barbados | **GH** | Ghana | **MG** | Madagascar | **TJ** | Tajikistan |
| **BE** | Belgium | **GN** | Guinea | **MK** | The former Yugoslav Republic of Macedonia | **TM** | Turkmenistan |
| **BF** | Burkina Faso | **GR** | Greece | | | **TR** | Turkey |
| **BG** | Bulgaria | **HU** | Hungary | **ML** | Mali | **TT** | Trinidad and Tobago |
| **BJ** | Benin | **IE** | Ireland | **MN** | Mongolia | **UA** | Ukraine |
| **BR** | Brazil | **IL** | Israel | **MR** | Mauritania | **UG** | Uganda |
| **BY** | Belarus | **IS** | Iceland | **MW** | Malawi | **US** | United States of America |
| **CA** | Canada | **IT** | Italy | **MX** | Mexico | **UZ** | Uzbekistan |
| **CF** | Central African Republic | **JP** | Japan | **NE** | Niger | **VN** | Viet Nam |
| **CG** | Congo | **KE** | Kenya | **NL** | Netherlands | **YU** | Yugoslavia |
| **CH** | Switzerland | **KG** | Kyrgyzstan | **NO** | Norway | **ZW** | Zimbabwe |
| **CI** | Côte d'Ivoire | **KP** | Democratic People's Republic of Korea | **NZ** | New Zealand | | |
| **CM** | Cameroon | | | **PL** | Poland | | |
| **CN** | China | **KR** | Republic of Korea | **PT** | Portugal | | |
| **CU** | Cuba | **KZ** | Kazakstan | **RO** | Romania | | |
| **CZ** | Czech Republic | **LC** | Saint Lucia | **RU** | Russian Federation | | |
| **DE** | Germany | **LI** | Liechtenstein | **SD** | Sudan | | |
| **DK** | Denmark | **LK** | Sri Lanka | **SE** | Sweden | | |
| **EE** | Estonia | **LR** | Liberia | **SG** | Singapore | | |

# PROTECTION OF DATABASE CONTENTS AGAINST USE WITHOUT PERMIT

## Technical Field

Present invention relates to protection of databases against use without permit from the rights owner, and in particular a method of preventing non-authorized exploitation of information contained in a database, a method and device for the preparation of information in a database to be exploited in a computer only with a corresponding authorization, and a method and device to enable authorized exploitation in a computer, of information from a database which is prepared according to one aspect of the invention.

The invention is just as usable in connection with databases which are available to the public at large and which typically are reached through a communication network, such as INTERNET, in particular, as with databases delivered to individual customers on a computer readable carrier medium, such as in particular a CD-ROM (read only compact laser disc), preferably for local exploitation in a computer or workstation, particularly a personal computer (PC).

To be able to retrieve from a database information contained therein, the information is generally stored in a structured manner according to predetermined rules and criteria. For example, a database can be arranged such that by naming a selected word for a topic all occurrences or entries in the database in which the topic word is present are fetched one after the other, or it is produced a list of the locations in the database in which the topic word is present, or the like. The information stored in a database has the form of data which by the retrieval must be "translated" from the computer representation to a language or manner of expression comprehensible to human beings. Hence, the data may represent plain text, audio, images, hypertext, animations, etc. Currently, a plurality of standard formats are used to handle such data for various purposes which specify how storage and transfer of data are to take place, for example, and which are decisive for the "translation" of the data into human comprehensible form. The formats are available to everybody. For example, data representing text and graphics can be stored and transferred in Postscript or PDF formats, video stills in GIF or JPG format, live video images in MPEG or QCIF format, etc.

By using an individual format a specifically coded and often additionally compressed or packed representation of the information is achieved in the form of objects, for example,

as in the case of an object oriented database. Usually, therefore, a corresponding special software is required to interpret the data formatted in this way to present them in a manner directed at human beings, such as in the form of a text or a picture accompanied by audio, or not, on a medium suitable therefor, such as a display screen, paper, etc. As a rule, such software is easily available to a user, and in addition often free of charge, by being included on the same physical carrier medium as the database, for example, such as on the same CD-ROM as that carrying the delivered database, this in particular being the case with respect of so-called multimedia products, or by fetching the software through the same network as that by which the database is reached, such as typically is the case where INTERNET, for example, is used.

Databases containing information (data) represented by means of more than one of the formats mentioned above, i.e. especially multimedia databases, will, by and by, be easily available to the people at large and increasingly more commonly used. Such databases would be available locally, such as on a laser disc of some kind, or through a network, such as INTERNET, and later also public telecommunication networks (particularly ISDN – Integrated Services Digital Network).

**Background Art**

Today there are databases which are open giving everybody unrestricted admission but there are also databases which are closed to the public in general and where a password og other authentication is required to get admission at all. Databases contain pieces of information, however, which for different reasons are more or less valuable to the owner, and which then can be said to belong to an "open" and a "closed" class, respectively. In such a case, a commonly used protection by password of the admission to the database as such, will shut the public in general out from the database as a whole, this being undesirable to many database owners, whereas, on the other hand, free admission would give access also to the "closed" class of information, which, of course, is not desirable.

So, where it is desirable to distribute through a network or on CD-ROMs particularly costly data, such as maps, animations, etc. stored in a database accessible to everybody, to restricted groups of users or customers, it must be possible to protect the information intended for such distribution against use without authorization, if the distribution should be justifiable in a business-like way. There are, however, no known

methods or techniques that provide sufficient protection as against abuse of such costly data which are retrievable from an otherwise "open" database.

Therefore, there is a need for a mechanism or arrangement which makes it possible to protect selected portions of the contents of a database against abuse, and which enables the owner of a database to give users having various demands permission to get information from those portions of the database which correspond to their needs but not from other portions thereof. Then, the owner can make a charge depending on the authorization given to the individual customers, and especially entrusted users only can be given admission to any secret information (data) in the database at the same time as everybody are presented with at least the "home page" of the database when calling the base.

Thus, a purpose of the present invention is to provide a protection arrangement enabling database owners and/or the proprietors of the pieces of information stored in a database to protect their product against use without permit, in such a manner that the entire database or portions thereof may be copied and freely distributed while the database, in principle, is open to everybody but still in such a manner that selected portions of the contents therein cannot be utilized unless the necessary permission or authorization exists.

Furthermore, a purpose of the invention is to provide a protection arrangement of a universal nature being capable of handling not only individual entries or objects in a database, but complete databases, whereby different authorizations can be assigned at a plurality of levels with respect of different selected portions of the database contents, for example.

These and other purposes should more clearly appear from the description below of exemplary preferred embodiments of the present invention taken in combination with the appended drawings.

**Description of Invention**

In a first general aspect of the present invention it is provided a method of preventing the contents of a database from being used without permit, whereby at least a selected portion of the contents of the database is caused to be incomprehensible to a user, said portion then being converted into comprehensible form by means of a key if permission

exists, the method of the invention being characterized in rendering meaningless said at least one selected portion of the contents of the database by encrypting, or otherwise corrupting, or moving from the database to a storage location hidden to the user at least one parameter associated with the selected portion for the control of the interpretation and presentation to a user by a computer, of data in that portion of the database in such a manner that the parameter is not available for utilization in the user's computer and said data cannot be correctly interpreted for the presentation to the user.

Hence, the invention also relates to a method of allowing exploitation of the contents of a database only with a corresponding permit, whereby those selected portions of the contents of the database which are caused to be incomprehensible can be correctly interpreted only if said parameter controlling the interpretation and presentation thereof by a computer is rendered meaningful and made available for utilization in the user's computer.

Accoding to the invention preferably said parameter is encrypted using a first key, and the decryption of said encrypted parameter is performed using a second key stored in a tamperproof unit connected to the user's computer. Also, it is possible to encrypt the first key prior to being stored in the tamperproof unit such that the key itself must be decrypted before it can be used for said decryption.

Accoding to the invention the encryption of said parameter may takes place prior to the completion of the database contents for use, or take place when a user fetches information from a database, in which preferably no parameter is pre-encrypted.

The decryption will take place when the computer in the processing of information fetched from the database hits an indication of encryption being performed. This indication is of such a kind that enables a computer program running on the user's computer to localize the encrypted parameters to decrypt them and use them for the control of the interpretation and presentation of the data they are associated with.

According to a preferred embodiment of the invention, when the computer hits such an indication of encryption being performed, a communication channel is established between the computer and the tamperproof unit through which the encrypted parameters are transferred to the tamperproof unit in a first transfer step for the decryption therein by a processor included in the unit. The decrypted parameters are then transferred in the

opposite direction through the communication channel in a second transfer step for the further utlitization in the computer in respect of correct interpretation and presentation of the data they are related to.

In a special embodiment of the invention the first and second algorithms as well as the corresponding first and second keys are determined in accordance with an asymmetric, two-key cryptographic arrangement (public-key / private-key cryptosystem), such as the RSA cryptosystem. In this case, preferably the first key is the known (public) key, and the second key is the secret (or private) key in the cryptographic arrangement.

In another version of the invention, where at least one parameter associated with a portion of the database contents is moved from the database to a hidden storage location, this is accomplished by storing the moved parameters in a tamperproof unit to be connected to the computer of a user. So, when the computer in the processing of information fetched from the database misses a parameter for the interpretation and presentation of data being processed, the computer establishes a communication channel to the tamperproof unit to communicate said absence. The tamperproof unit then provides the missing parameter which is stored in the unit, and transfers this parameter the opposite direction through the communication channel such that the missing parameter can be used in the computer for the correct interpretation and presentation of the data concerned.

In another aspect, the invention relates to a device for preventing the contents of a database to be used without permit. According to the invention this device is characterized in that it comprises crypto-equipment adapted to render meaningless a selected portion of the contents of the database by performing encryption or otherwise corruption of at least one parameter associated with the selected portion for the control of the interpretation and presentation to a user by a computer, of data in that part of the database in such a manner that the parameter is unavailable for utilization in the user's computer, and said data cannot be correctly interpreted for the presentation to the user.

The crypto-equipment according to the invention is preferably adapted to encrypt said parameter using a first key prior to the completion of the database contents for use, or at the same time as when a user fetches information from a database, the database preferably not being pre-encrypted.

In a preferred embodiment of this device which comprises a tamperproof unit to be connected to a user's computer, and having a computer-readable storage medium and a processor of its own, the tamperproof unit is adapted to decrypt in accordance with a decryption algorithm the encrypted parameter using a second key stored in the tamperproof unit which is different from said first key.

Preferably, the tamperproof unit is adapted to perform by a command from the computer to which the unit is connected said decryption of the encrypted parameter when the computer in the processing of information fetched from the database hits an indication of at least one encrypted parameter being present in the fetched information. This is achieved by adapting the computer to establish a communication channel between itself and the tamperproof unit when it hits said indication of the presence of at least one encrypted parameter. Through this communication channel the computer then transfers in a first transfer step the encrypted parameters to the tamperproof unit for the decryption by means of the unit's own processor. Then, the tamperproof unit returns in a second transfer step the result of the decryption of the encrypted parameters through the communication channel to the computer for further utilization therein.

In still another aspect, the invention relates to a device for preparing a database in such a manner that the contents thereof cannot be used without permit. According to the invention this device is characterized in that it comprises crypto and preprocessing equipment adapted to render meaningless at least one selected portion of the contents of the database by performing encryption using a first key, of at least one parameter associated with the selected portion for the control of the interpretation and presentation to a user by a computer, of data in that portion of the database. At the same time the preprocessing equipment includes in a start-up file or the like for the whole of the database, or in a start or introductory field for that portion of the database having an encrypted parameter associated therewith an indication of at least one encrypted parameter being present in the database and where such encrypted parameters are located. This indication is intended to be used for the establishment of communication with a tamperproof unit connected to a user's computer.

In still a further aspect, the invention relates to a device for allowing exploitation of the contents of a database only with a corresponding permit. According to the invention this device is characterized in that it comprises preprocessing equipment adapted to render meaningless at least one selected portion of the contents of the database by moving to a

storage location hidden to the user at least one parameter associated with the selected portion for the control of the interpretation and presentation to a user by a computer, of data in that part of the database in such a manner that the parameter is unavailable for the utilization in the user's computer, and said data can then be correctly interpreted only if said parameter is made available for the utilization in the user's computer.

In a version of this latter device, the preprocessing equipment is adapted to move said parameters from the database to a storage in a tamperproof unit to be connected to a user's computer.

With the methods and devices according to the invention a mechanism or arrangement is achieved which makes it utmost difficult to exploit the contents stored in a database, such as in the form of objects, entities, data occurrences, entries in tables, etc. if permission from the copyright proprietor does not exist. Also, this hinderance against unauthorized use can be made even more secure, such as by distorting the communication of a user's computer with the tamperproof unit connected thereto.

**Brief Description of Drawings**

In the following description, it is referred to the accompanying drawings, on which:

Figure 1 is a simplified diagram showing the principle of a typical current situation whereby items of information are transferred from a database,

Figure 2 is a simplified diagram showing the principle corresponding to that of Figure 1, and including a peripheral unit according to the invention,

Figure 3 is a simplified diagram showing the principle of retrieval of objects,

Figure 4 is an example of the communication of a user terminal with a database manager encrypted at several levels,

Figure 5 is an example of a sequence for encrypting data in a database, and

Figure 6 is an example of a sequence for decrypting data in a database.

**Description of Preferred Embodiments**

It is referred to Figures 1, 2 and 3, all of which serving to illustrate the principle of using a database 1 in which the stored information has the form of data which must be "translated" from a computer language to a language or manner of expression comprehensible to human beings.

In Figure 1, a typical flow of data between a user and a database is demonstrated. When a users has established connection with and been given admission to the database 1, data from the database 1 is transferred to the user's computer through the connection 4, the data being available either locally at a workstation (in the case of the CD-ROM) or centrally through a network (INTERNET). Possibly the user must enter a password to gain access to the database, and then usually all information stored in the database is available for the exploitation by the user. When the user has gained access to the database the data is processed in the user's computer by means of special software so as to present the contents of the database to the user in a comprehensible form. In principle, once the data is fetched and transferred from the database, the data can currently be unrestricted copied and distributed. This also applies to data stored locally, such as on a CD-ROM.

Given the technology of today, it is relatively simple and inexpensive to read out and store on a CD-ROM, for example, the whole or major parts of a database. Then, such a CD-ROM copy can freely be used by non-authorized users. The result is that already it has become very difficult to safeguard copyrights by means of known methods of protecting databases, and in the future, this problem will be even larger given the possibility of *inter alia* recording data on (or "burn") SD-CDs (Super Density Compact Disks) having a storage capacity of about 4.8 gigabytes per layer.

The stored data of a database which is to be protected against abuse is represented in a format which requires a special (viewer) program to present the data in a form directed at human beings, i.e. as audio, images, text, etc. Such special software should be independent of the information content, and can usually be employed with respect of all items of information having the same format. Therefore, it is not practical to protect this special software. The protection of the information, i.e. the objects or data in the database, seems to be a better solution.

In any "packed", or coded representation of data there are vital components, namely parameters, which are necessary to interpret and present the data correctly to the user. Therefore, a basis for the present invention is that if such parameters are stored in an encrypted form in the database, it will not be possible for a non-authorized user to interpret the contents of the database.

The part of the information in the database that according to the invention is encrypted according to an encryption algorithm using a first key, is therefore selected on the basis that it is completely decisive for enabling the corresponding portion of information in the database to be correctly interpreted. The selected part of the information in the database which is encrypted comprises one or more parameters associated with the corresponding portion of the database information for the purpose of controlling the interpretation and presentation of the latter to a user such that, upon the decryption of the encrypted parameters, the corresponding part of the information can be correctly interpreted and presented in a correct manner to the user. Such parameters are generally associated with, or included in each individual object of the database, or groups of corresponding object.

To be able to interpret the contents of the database, a user having permit therefor must use certain items of information for the decryption of the parameters of the database which are decrypted. The items of information enabling the decryption may be stored in a separate tamperproof unit of equipment, for example, such as a dongle or a smart card being machine readable by the user's workstation. Software for the communication with the tamperproof unit for the purpose of having the parameters decrypted when data from the database is to be used, must in this case be integrated in the special software installed on the user's workstation or terminal. Hence, the special software must provide for establishing a link to the database (or database server), and that access to the database is granted, as well as unpack the desired data fetched from the database to interpret the data with respect of their presentation in a comprehensible manner to the user.

To make it possible for the data to be used by authorized users only, (e.g. paying users or customers only), and not to be distributed in a usable form without restrictions, the contents of the database 1 may be encrypted with reference to Figure 2, in the following manner:

- A selection of parameters belonging to the database objects 6 (which are packed) is encrypted. The various items of information may in principle be encrypted using different keys.
- In the initial phase (when the user establishes communication with the database) a data file, hereinafter called the start-up file 5, is transferred to the user. The start-up file contains "guiding information" hereinafter called key data, in encrypted form. The encrypted key data is transferred to a peripheral device 3, such as a card reader

station for smart cards, which then finds the keys previously stored in the tamperproof unit (on the smart card) and which is to be employed (by that unit) for the decryption of the parameters contained in the objects received from the database.

In a version of the present invention, the key data in the start-up file may be encrypted either using a known (public) key to be decrypted in the tamperproof unit using a corresponding secret or private key stored on the smart card, for example, which may be denoted a master key, or be encrypted using the secret key, such as with symmetric cryptographic systems, e.g. DES. Only when the parameters are decrypted the objects or data can be unpacked to be presented to the user 4.

By having such an extended data format the interpretation of the data will take place as explained in the following.

The tamperproof unit contains a master key which is known to the "owner" of the database only and not available to the user. When the user wishes to establish communication with the database to retrieve data therefrom, the database start-up file is transferred to the user.

The special software reads the start-up file and then conveys the key data from the start-up file which is encrypted by a known key, to the peripheral unit. If the peripheral unit (or the smart card placed therein) is authorized for the use of that database, it contains a master key for the decryption of the encrypted key data of the start-up file. The key data comprises references and/or addresses to such keys that are prestored in the peripheral unit and which must be employed to decrypt the parameters of the objects for thus being able to interpret the objects correctly.

The special software may recognize the encrypted parameters to convey them to the peripheral unit. Possibly each object contains an initial sequence defining which key is to be employed in the decryption of the parameters of that object and an indication as to the position of the encrypted parameters. In this way, in principle all objects in the database may be encrypted using different keys, furthermore enabling authorization of the tamperproof unit at several levels. As mentioned above, such an initial sequence is itself preferably encrypted such that the decryption must be carried out by means of the master key.

The tamperproof unit decrypts the encrypted parameters by means of the deducted keys and returns the result to the special software which now can utilize the decrypted parameters to interpret and display correctly the corresponding items of information, and the processing continues further.

In Figure 3, a further development of the arrangement just described is shown. The database 1 of Figure 3 may physically be located either in a local workstation (e.g. in the form of a CD-ROM), or be available through a network (e.g. through INTERNET). When the user establishes communication with the database the initial file is transferred in encrypted state to the user's computer 2 through the link 5 to the database 1. The peripheral unit (the smart card) 3 receives the encrypted key data which is decrypted by means of the master key being present in the tamperproof unit (on the smart card). The keys to be used for the decryption of the encrypted parameters are thereby determined in the tamperproof unit such that parameters can be obtained which enables the objects to be interpreted correctly, as is shown and described with reference to Figure 2.

In the case of the database being a CD-ROM, the key data must already be encrypted in agreement with the tamperproof unit (smart card). The encryption algorithms being used are dependent on the application (CD-ROM, distributed databases, etc.), and in principle they may be either symmetric, e.g. of the DES type (Data Encryption Standard, Bureau of Standards, U.S.A., 1977), or asymmetric, e.g. of the RSA type (Rivest, Shamir, Adleman).

To present the data a special software is used which communicates with the tamper-proof unit (smart card) 3 to enable the decryption of the parameters and the presentation of the data to the user. As a result, the objects (the data) being transferred from the database to a user will always be unusable in their present form. Therefore, the database (a CD-ROM, for example) can be distributed without restrictions and be copied in an unlimited number as it can be used only with a tamperproof unit (smart card) carrying the authorization and the correct master key. In other words, the permission to use the database is resident in the tamperproof unit (the smart card).

Also, it is possible to place the access authorization to the data in a database at several levels by using different encryption keys on each of the objects in the database, or on groups of items of information in the database. Such a principle seems to be most interesting if access to the database in question is made through a network (e.g.

INTERNET), the method may, however, be used on local databases also, such as a database carried on a CD-ROM.

Figure 4 demonstrates how the communication between a user terminal and a database manager can take place when having such encryption at multiple levels. The database manager and the user (in fact, the user's computer) start in respective initial states 1 and 4, respectively. When communication between user and database is established through the intermediate network (e.g. INTERNET) 13, in the example shown, a first authentication session 10 of the user is carried out while he and the manager still are in the initial state 1, 4. During this session, or this communication step, the master key being stored in the tamperproof unit (on the smart card) 9, is used. If the this unit (the smart card) 9 holds an authorization to exploit the database the user is granted access to a limited part of the database contents as indicated in Figure 4 by transition 14 having the meaning of "authorized OK". If the user is admitted to more than one "information layer" in the database (by authorization at multiple levels) the keys are transferred in encrypted form to the tamperproof unit which then decrypts the key data by means of the master key (on the smart card) to find which keys are to be utilized in the decryption of the parameters.

In Figure 4, when the user is in the state denoted 5 and the database manager is in the state denoted 2, in a new communication step 11, the user can perform restricted operations (such as searching) in the database without transferring any data to his computer or terminal. Data which is found in the database in this manner, may then, at this level (level 0) be transferred to the user without being distorted.

When the user searches for information in the database at a higher level (levels 1, ... n) thereof, the database manager will distort or corrupt the objects (data) 3 in such a manner that they can be utilized only by assistance by the tamperproof unit (the smart card). In one embodiment of the process, the keys to be used for the decryption of the parameters at the various levels (level 1, ... n) can be transferred to the user during the authentication phase for temporary storage in the user terminal (in encrypted form), or in the tamperproof unit connected to the terminal, or they may already have been transferred to the smart card.

Each corrupted object contains an initial sequence indicating which key identified by key number, for example, to be used for the decryption of the encrypted parameters in the

object, as well as where, i.e. in what position, the encrypted parameters are found in that object. In a further session 12 the corrupted items of information are transferred through the network 13 to the user. Then, the user can continue the communication with the database by means of the special software and render the objects usable by means of the tamperproof unit (the smart card) to have the database contents presented (at 8) in a comprehensible manner.

Example of message sequence for a local database

As shown in Figure 6, such a prosess is initiated when the user calls (at 1) the database. The user then (at 2) receives a message including a start-up file containing the following information:

- a database identifier which is recognized in the tamperproof unit (by comparison with an identifier stored on the smart card, for example), and
- a set of references to decryption keys (stored in the tamperproof unit, particularly on the smart card) to be used during the decryption of the encrypted parameters of the database.

The references to the decryption keys, or the keys themselves, can be encrypted by a known (public) key corresponding to the master or private key stored in the tamper-proof unit (on the smart card) which is not available to the user.

The start-up file contents will be forwarded (in session 2a) to the peripheral unit (the smart card) which then checks the identity of the database. Only if the identity of the database is recognized and accepted by the tamperproof unit (the smart card) the references to the decryption keys to be used are decrypted by means of a chosen decryption algorithm and master key. Then, in the tamperproof unit (the smart card), the decryption keys are determined for later use. If the identity of the database is not recognized nor accepted by the tamperproof unit, the user receives a message (at 5) saying that admission to the database is denied.

If the user (in fact, the tamperproof unit) is authorized to exploit the database a home page or a table of contents for the database is presented to that person. Whether or not this object is to be encrypted is, of course, a decision of the database "owner".

Starting from the home page or the table of contents the user can search for more information by "designating" (in session 3) one or more objects in the database. These

objects are packed and/or coded in a specific format (e.g. postscript, PDF, GIF, MPEG, and more) and thus contain parameters which are decisive for unpacking and/or decoding the contents in the objects for the presentation thereof in a way that is comprehensible to the user. At least some of the these parameters are encrypted, and the encrypted parameters must be recognized by the special software and/or decoding software to be forwarded to the tamperproof unit (the smart card) to be decrypted therein by means of the correct key.

To obtain a "tidy" structure of the database it is sensible to use the same key for the encryption of parameters within one and the same object. The keys to be used and the position of the encrypted parameters in the objects are indicated in the initial sequence (header) of each object. This is necessary to enable corruption at multiple levels and at all times enabling the decryption of the correct parameter while the information in the object is in binary form. This heading or additional information accompanying the object should be encrypted at the same level as the start-up file, the master key of the peripheral unit and/or smart card being usable for the decryption of the heading. The cryptographic algorithm used may be the same for all objects.

When the user (at 3) accesses and object the special software will receive (at 4) the initial sequence of the object and its contents in corrupted form. The initial sequence 8.1 is transferred (at 6a) to the tamperproof unit to be decrypted using the master key. An indication as to which key to be used in the decryption of the parameters is stored in the tamperproof unit (on the smart card), and an indication as to where the encrypted parameters are located in the object is returned (at 6b) to the user's computer for the utilization by the special software such that the encrypted parameters can be located and transferred (at 7) to the tamperproof unit to be decrypted using the correct key (one specific key among ten keys, for example) stored in the tamperproof unit and defined in the initial sequence of the object. When the encrypted parameters 7.1, 7.2, 7.3, ... of the object are received by the special software they are forwarded (at 7) to the tamperproof unit to be decrypted in the tamperproof unit using the correct key, then being returned (at 8) to the user's computer. So, instead of the encrypted parameters, the special software will employ the decrypted parameters 4.1, 4.2, ... received from the tamperproof unit (the smart card) such that the format of the object can be correctly decoded or "unpacked" (in block 11) and the object be presented to the user in a comprehensible manner. If even better security is desirable, it is, of course, possible also additionally to

scramble the communication between the user's computer and the tamperproof unit (the smart card).

Example of message sequence for a remote database connected to a network

In principle, this message sequence may be similar to that of a local database as described herein before. The major difference lies in that such databases, at the start, may be uncorrupted and that a distortion or corruption involving encryption of parameters in packed objects is carried out when a user accesses the database. Then the flow of authorization messages takes place between the user and the database manager located at the database. In general, the sequence is such as that shown in Figure 4.

**Claims**

1. A method of preventing the contents of a database from being used without permit, whereby at least a selected portion of the contents of the database is caused to be incomprehensible to a user, said portion then being converted into comprehensible form by means of a key if permission exists,
c h a r a c t e r i z e d i n rendering meaningless said at least one selected portion (6; Figure 2) of the contents of the database (1; Figure 2) by encrypting, or otherwise corrupting, or moving from the database to a storage location hidden to the user at least one parameter (4.1, ... 4.m; Figure 5) associated with the selected portion for the control of the interpretation and presentation to a user by a computer, of data in that portion of the database in such a manner that the parameter is not available for utilization in the user's computer and said data cannot be correctly interpreted for the presentation to the user.

2. A method of allowing exploitation of the contents of a database only with a corresponding permit, whereby at least a selected portion of the contents of the database is caused to be incomprehensible to a user, said portion then being converted into comprehensible form by means of a key if permission exists,
c h a r a c t e r i z e d i n rendering meaningless said at least one selected portion (6; Figure 2) of the contents of the database (1; Figure 2) by encrypting, or otherwise corrupting, or moving from the database to a storage location hidden to the user at least one parameter (4.1, ... 4.m; Figure 5) associated with the selected portion for controlling the interpretation and presentation to a user by a computer, of that portion of the database in such a manner that the parameter is not available for utilization in the user's computer, and said data can be correctly interpreted only if said parameter is rendered meaningful and made available for utilization in the user's computer.

3. A method according to claim 1 or 2,
c h a r a c t e r i z e d i n encrypting said parameter (4.1, ... 4.m) using a first key, and performing decryption of said encrypted parameter using a second key stored in a tamperproof unit connected to the user's computer.

4. A method according to any of the preceeding claims,
c h a r a c t e r i z e d i n that the encryption of said parameter takes place prior to the completion of the database contents for use, or takes place when a user fetches

information from a database, preferably no parameter associated with the database contents being pre-encrypted.

5. A method according to claim 3,
characterized in encrypting the first key in accordance with an encryption algorithm and a third key prior to the storage thereof in said tamperproof unit, and decrypting the encrypted key in accordance with a decryption algorithm and a fourth key for the use thereof as said second key.

6. A method according to any of the preceeding claims,
characterized in that the decryption of the encrypted parameter which is performed using the second key takes place when the computer in the processing of information fetched from the database hits an indication of encryption being performed which indicates that at least one encrypted parameter is present in the information fetched and where such encrypted parameters are located such that when being localized and decrypted the decrypted parameters can be used to control the interpretation and presentation of the related data.

7. A method according to claim 6,
characterized in that when the computer hits said indication of encryption being performed, a communication channel is established between the computer and the tamperproof unit through which the encrypted parameters are transferred to the tamperproof unit in a first transfer step for the decryption therein by a processor included in the unit, the respective decrypted parameters then being transferred in the opposite direction through the communication channel in a second transfer step for the further utlitization in the computer in respect of correct interpretation and presentation of the related data.

8. A method according to claim 6 or 7,
characterized in providing said indication of encryption being performed as an instruction or the like resulting in the establishment of said communication channel between the computer and the tamperproof unit.

9. A method according to claim 6 or 7,
characterized in embedding said indication of encryption being performed in a start-up file or the like for the whole of the database, and/or in a start or introductory

file for the individual portions of the database having an encrypted parameter associated therewith, this indication preferably having the form of a reference.

10. A method according to any of the preceeding claims,
characterized in that the encryption and decryption algorithms using said first and second keys are determined in accordance with an asymmetric, two-key cryptographic arrangement (public key cryptosystem), such as the RSA cryptosystem, the first key preferably being the known (public) key and the second key being the secret (or private) key in such a cryptographic arrangement, or in accordance with a symmetric cryptographic arrangement.

11. A method according to claim 1,
characterized in that, in the case at least one parameter associated with a portion of the database contents is moved from the database to a hidden storage location, this is accomplished by storing the moved parameters in a tamperproof unit to be connected to the computer of a user such that when the computer in the processing of information fetched from the database misses a parameter for the interpretation and presentation of data being processed thereby, a communication channel is established between the computer and the tamperproof unit through which said absence is communicated to the tamperproof unit in a first transfer step, the unit's own processor then providing the missing parameter which is stored in the unit and then is transferred the opposite direction through the communication channel in a second transfer step for the further utilization in the computer with respect of correct interpretation and presentation of the data concerned.

12. A device for preventing the contents of a database to be used without permit, the device being adapted to cause at least one selected portion of the database contents to be incomprehensible to a user, and then to be converted by processing in a user's computer into comprehensible form by means of a key if permission exists,
characterized in that the device comprises crypto-equipment adapted to render meaningless at least one selected portion (6; Figure 2) of the contents of the database (1; Figure 2) by performing encryption or otherwise corruption of at least one parameter (4.1, ... 4.m; Figure 5) associated with the selected portion for the control of the interpretation and presentation to a user by a computer, of data in that part of the database in such a manner that the parameter is unavailable for utilization in the user's computer, and said data cannot be correctly interpreted for the presentation to the user.

13. A device according to claim 12,
characterized in that said crypto-equipment is adapted to encrypt said parameter (4.1, ... 4.m) using a first key prior to the completion of the database contents for use, or when a user fetches information from a database, the database preferably not being pre-encrypted.

14. A device according to claim 13 comprising a tamperproof unit to be connected to a user's computer, the tamperproof unit at least comprising a computer-readable storage medium and a processor of its own,
characterized in that said tamperproof unit is adapted to decrypt in accordance with a decryption algorithm the encrypted parameter using a second key stored in the tamperproof unit which is different from said first key.

15. A device according to claim 14,
characterized in that said tamperproof unit is adapted to perform by a command from the computer to which the unit is connected said decryption of the encrypted parameter when the computer in the processing of information fetched from the database hits an indication of at least one encrypted parameter being present in the fetched information and where such encrypted parameters are present in the information fetched from the database.

16. A device according to claim 15,
characterized in that said computer is adapted to establish a communication channel between itself and the tamperproof unit when it hits said indication of the presence of at least one encrypted parameter to transfer through this communication channel the encrypted parameters to the tamperproof unit in a first transfer step for the decryption by means of the unit's own processor which after the decryption of the encrypted parameters returns the result through the communication channel in a second transfer step to the computer for further utilization therein.

17. A device for preparing a database such that the contents thereof cannot be used without permit, the device being adapted to cause at least one selected portion of the database content to be incomprehensible to a user and by the processing in a user's computer being converted into comprehensible form by means of a key if permission exists,

characterized in that the device comprises crypto and preprocessing equipment adapted to render meaningless said at least one selected portion (6; Figure 2) of the contents of the database (1; Figure 2) by performing encryption using a first key, of at least one parameter (4.1, ... 4.m; Figure 5) associated with the selected portion for the control of the interpretation and presentation to a user by a computer, of data in that portion of the database and at the same time include in a start-up file or the like for the whole of the database, or in a start or introductory field for that portion of the database having an encrypted parameter associated therewith an indication of at least one encrypted parameter being present in the database and where such encrypted parameters are located, said indication being intended to be used for the establishment of communication with a tamperproof unit connected to a user's computer.

18. A device for allowing exploitation of the contents of a database only with a corresponding permit, the device being adapted to cause at least one selected portion of the database content to be incomprehensible to a user and by the processing in a user's computer being converted into comprehensible form by means of a key if permission exists,

characterized in that the device comprises preprocessing equipment adapted to render meaningless said at least one selected portion (6; Figure 2) of the contents of the database (1; Figure 2) by moving to a storage location hidden to the user at least one parameter (4.1, ... 4.m; Figure 5) associated with the selected portion for the control of the interpretation and presentation to a user by a computer, of data in that part of the database in such a manner that the parameter is unavailable for the utilization in the user's computer, and said data can be correctly interpreted only if said parameter is made available for the utilization in the user's computer.

19. A device according to claim 18,

characterized in that said preprocessing equipment is adapted to move said parameters from the database to a storage in a tamperproof unit to be connected to a user's computer.

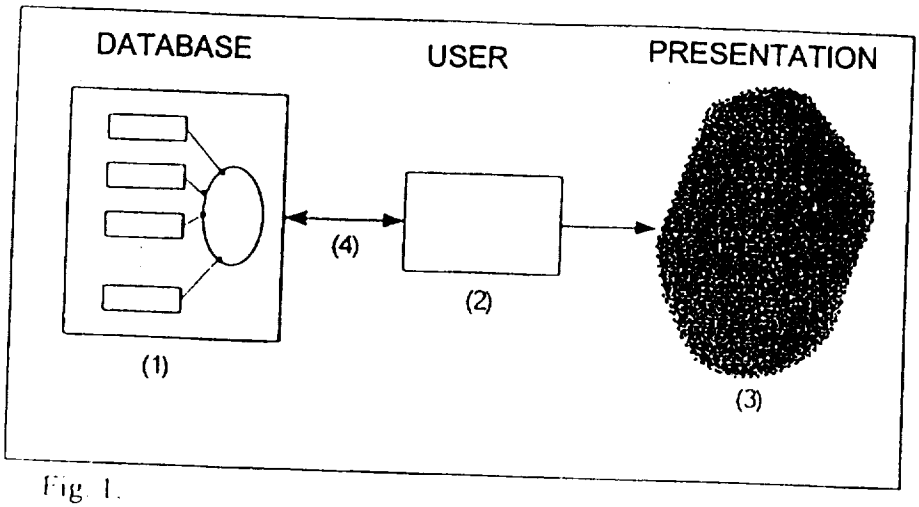



Fig. 1.

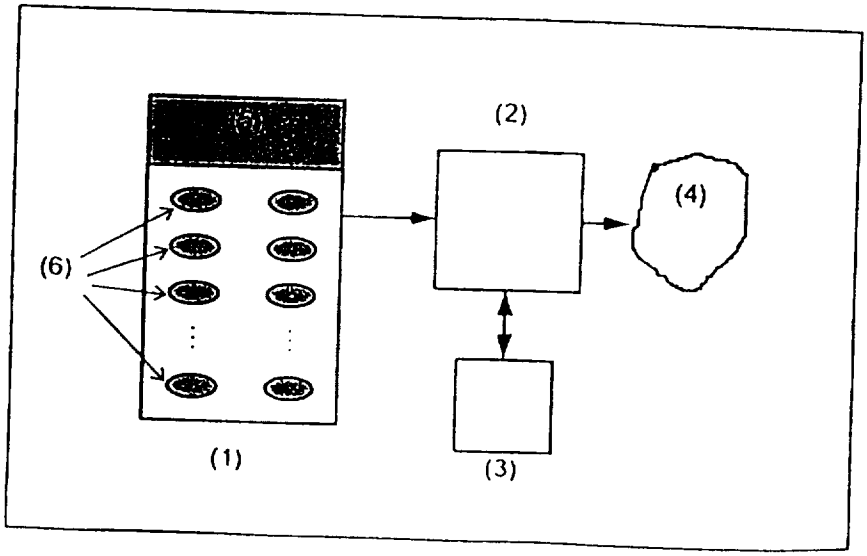



Fig. 2.

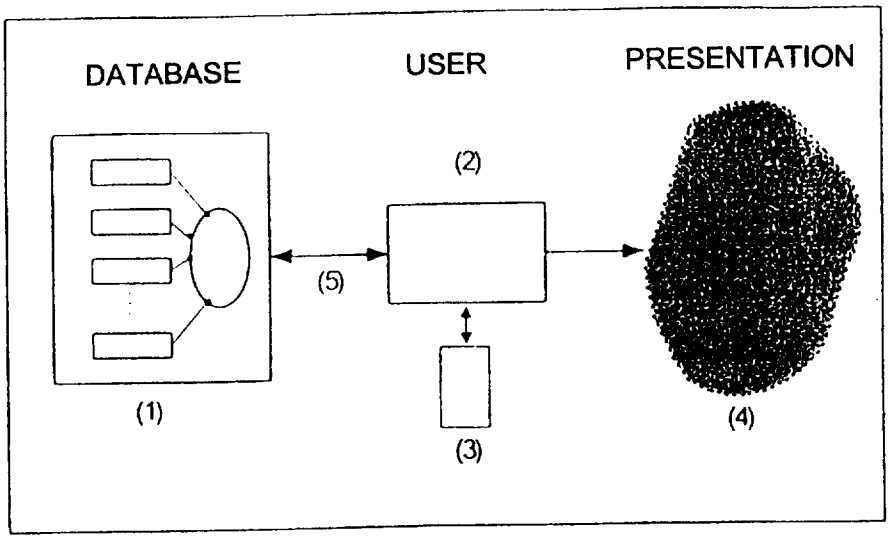

DATABASE
USER
PRESENTATION
(1)
(2)
(3)
(4)
(5)

Fig. 3

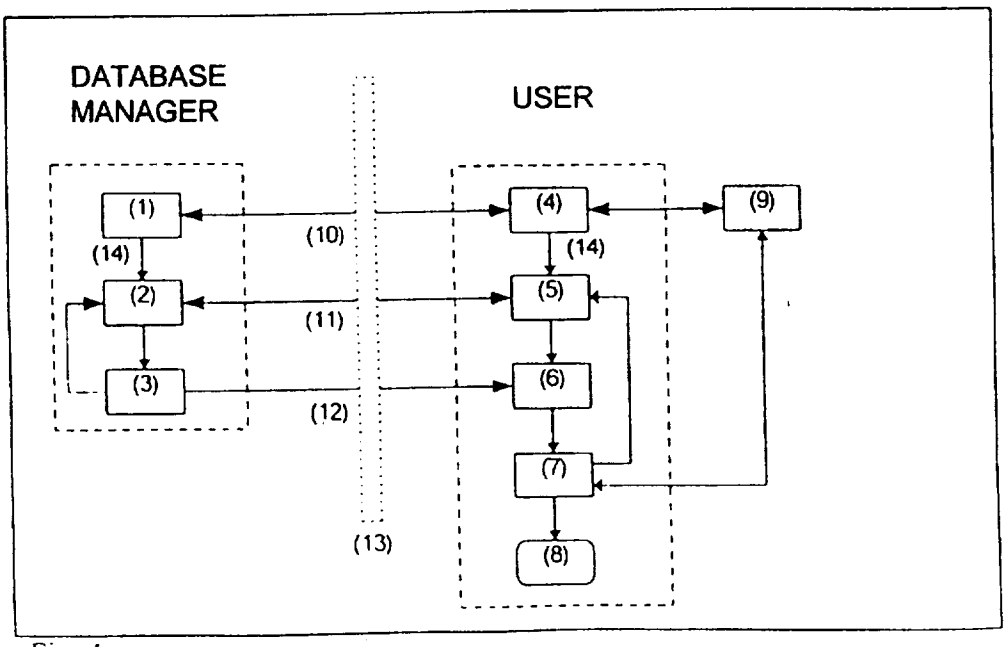

DATABASE MANAGER
USER
(1)
(2)
(3)
(4)
(5)
(6)
(7)
(8)
(9)
(10)
(11)
(12)
(13)
(14)
(14)

Fig. 4

Fig. 5

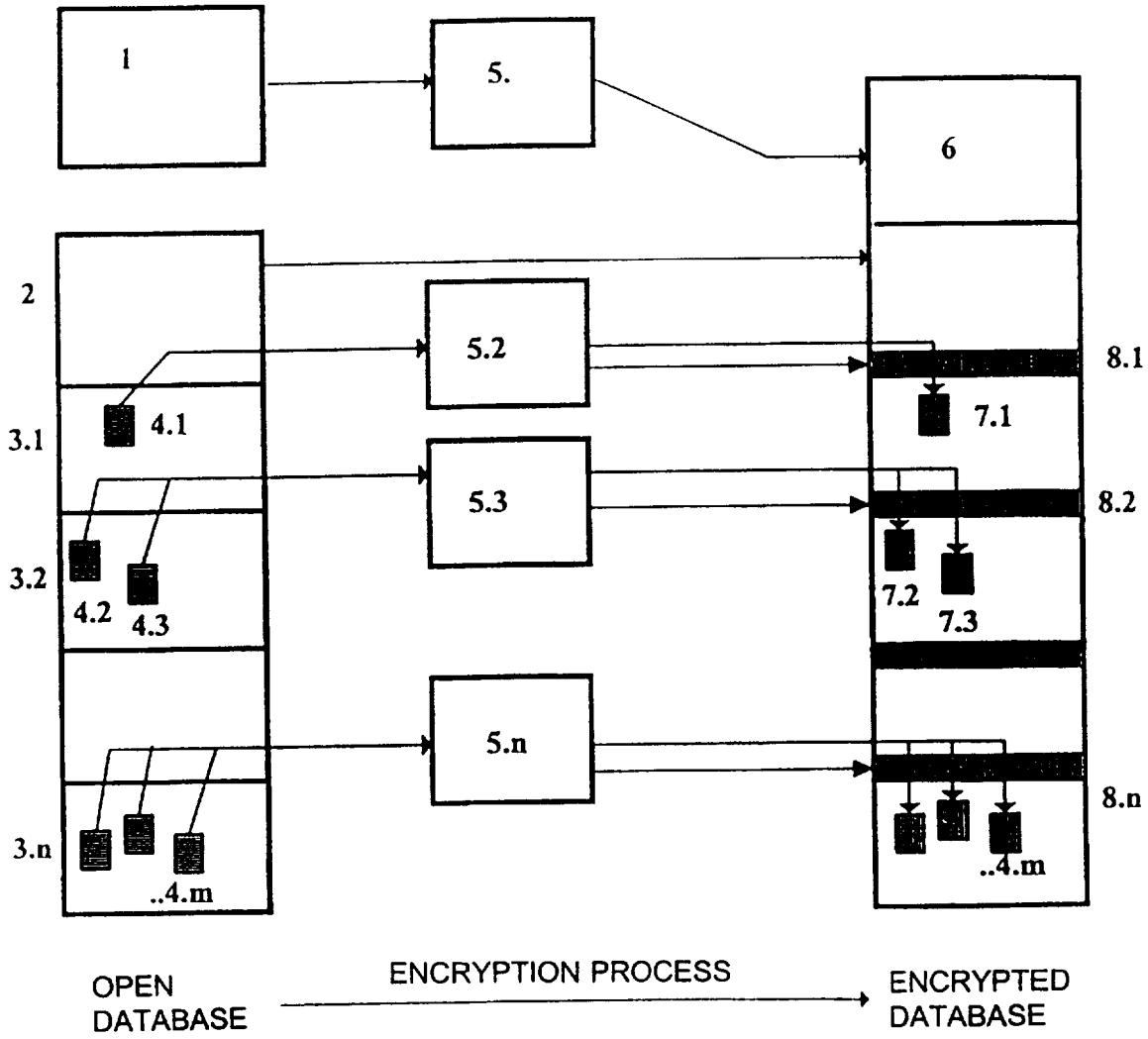
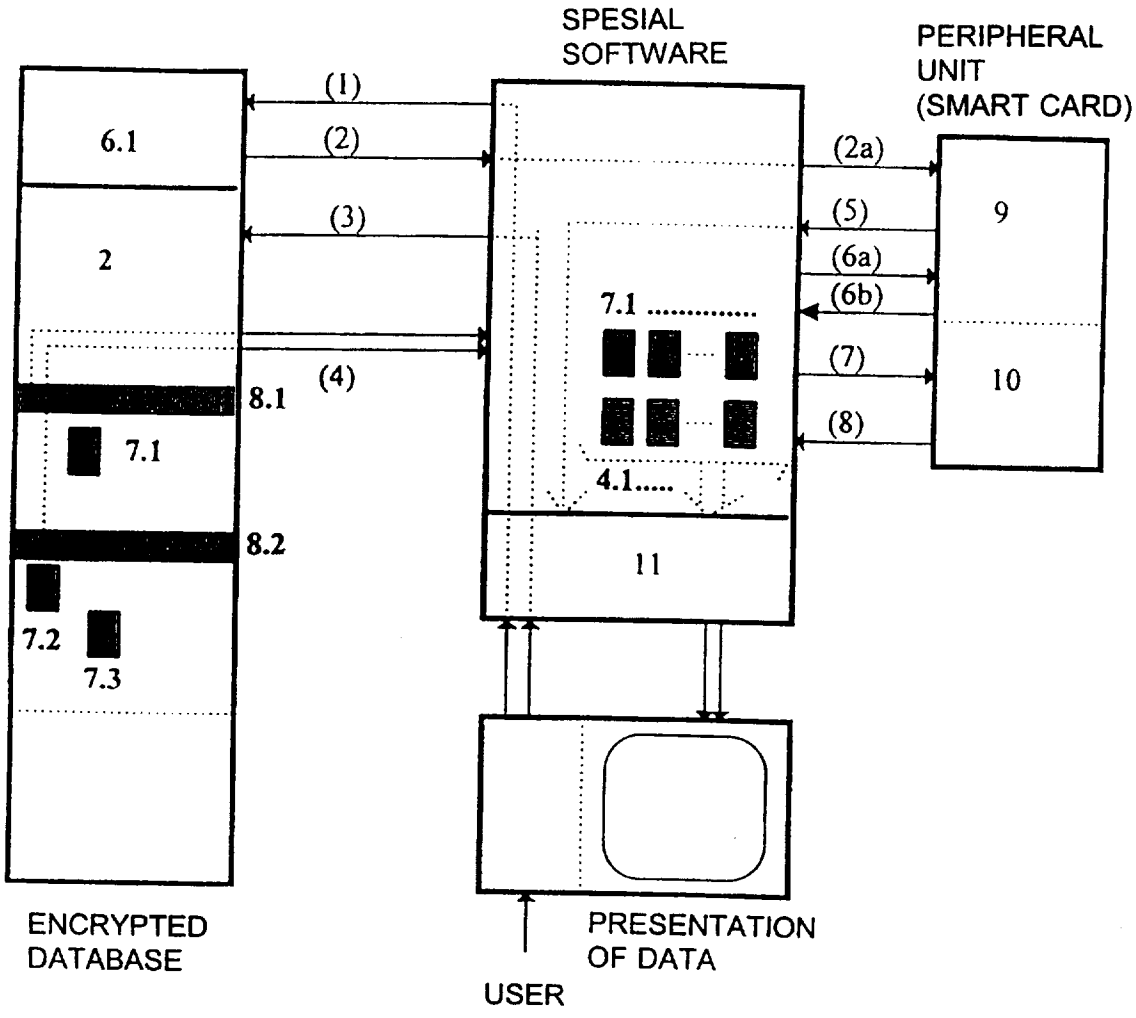

1
5.
6
2
5.2
8.1
4.1
7.1
3.1
5.3
8.2
3.2
4.2
4.3
7.2
7.3
5.n
8.n
3.n
..4.m
..4.m
OPEN DATABASE
ENCRYPTION PROCESS
ENCRYPTED DATABASE

Fig.6


SPESIAL SOFTWARE
PERIPHERAL UNIT (SMART CARD)
6.1
2
8.1
7.1
8.2
7.2
7.3
(1)
(2)
(3)
(4)
(2a)
(5)
(6a)
(6b)
(7)
(8)
9
10
7.1
4.1
11
ENCRYPTED DATABASE
PRESENTATION OF DATA
USER

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/NO 97/00185

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: G06F 1/00, G06F 17/30
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: G06F

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

SE,DK,FI,NO classes as above

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

CLAIMS, WPI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | EP 0715242 A1 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION), 5 June 1996 (05.06.96), column 8, line 45 - column 16, line 8, claims 1,2,5, abstract | 1-5,10-19 |
| Y | -- | 6-9 |
| X | GB 2228807 A (ESSELTE LETRASET LIMITED), 5 Sept 1990 (05.09.90), page 2, line 18 - page 5, line 35 | 1,2,4,12,13, 17,18 |
| | -- | |
| X | EP 0653695 A2 (AT & T CORP), 17 May 1995 (17.05.95), column 3, line 28 - column 7, line 57 | 1-4,10,12, 13,17,18 |
| Y | -- | 6-9 |

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

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 11 November 1997 | 13 -11- 1997 |
| Name and mailing address of the ISA/<br>Swedish Patent Office<br>Box 5055, S-102 42 STOCKHOLM<br>Facsimile No. +46 8 666 02 86 | Authorized officer<br>Bo Gustavsson<br>Telephone No. +46 8 782 25 00 |

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/NO 97/00185

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 5050213 A (SHEAR), 17 Sept 1991 (17.09.91), column 9, line 38 - column 12, line 52 | 1,2,4,12,13, 17,18 |
| | -- | |
| X | US 5319705 A (HALTER ET AL), 7 June 1994 (07.06.94), column 7, line 53 - column 10, line 16 | 1-4,12-14, 18,19 |
| A | | 5-11 |
| | -- | |
| P,X | SE 504085 C2 (GREG BENSON), 2 August 1996 (02.08.96), see the whole document. | 1,2,6,7, 11-14,17,18 |
| | -- | |
| | -------- | |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

01/10/97

International application No.
PCT/NO 97/00185

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| EP 0715242 A1 | 05/06/96 | JP 8160855 A | 21/06/96 |
| | | JP 8160856 A | 21/06/96 |
| GB 2228807 A | 05/09/90 | WO 9204670 A | 19/03/92 |
| EP 0653695 A2 | 17/05/95 | CA 2133237 A | 16/05/95 |
| | | CN 1139324 A | 01/01/97 |
| | | JP 7200286 A | 04/08/95 |
| | | US 5625690 A | 29/04/97 |
| US 5050213 A | 17/09/91 | US 5272750 A | 21/12/93 |
| | | US 5410598 A | 25/04/95 |
| | | US 4977594 A | 11/12/90 |
| | | AT 133305 T | 15/02/96 |
| | | DE 3751678 D,T | 14/11/96 |
| | | EP 0329681 A,B | 30/08/89 |
| | | SE 0329681 T3 | |
| | | US 4827508 A | 02/05/89 |
| | | WO 8802960 A | 21/04/88 |
| US 5319705 A | 07/06/94 | JP 7093148 A | 07/04/95 |
| SE 504085 C2 | 02/08/96 | AU 4681496 A | 21/08/96 |
| | | SE 9500355 A | 02/08/96 |
| | | WO 9624092 A | 08/08/96 |