PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 12/14	A1	(11) International Publication Number: WO 96/00942 (43) International Publication Date: 11 January 1996 (11.01.96)

(21) International Application Number: PCT/US95/06329

(22) International Filing Date: 19 May 1995 (19.05.95)

(30) Priority Data:
268,695 30 June 1994 (30.06.94) US

(71) Applicant: HUGHES AIRCRAFT COMPANY [US/US]; 7200 Hughes Terrace, Los Angeles, CA 90045-0028 (US).

(72) Inventors: GEORGIADES, Diane, E.; 19981 Fernglen Drive, Yorba Linda, CA 92686 (US). TAYLOR, Neal, E.; 18361 Avolinda Drive, Yorba Linda, CA 92686 (US).

(74) Agents: WALDER, Jeannette, M. et al.; Hughes Aircraft Company, Building C1, M/S A126, P.O. Box 80028, Los Angeles, CA 90080-0028 (US).

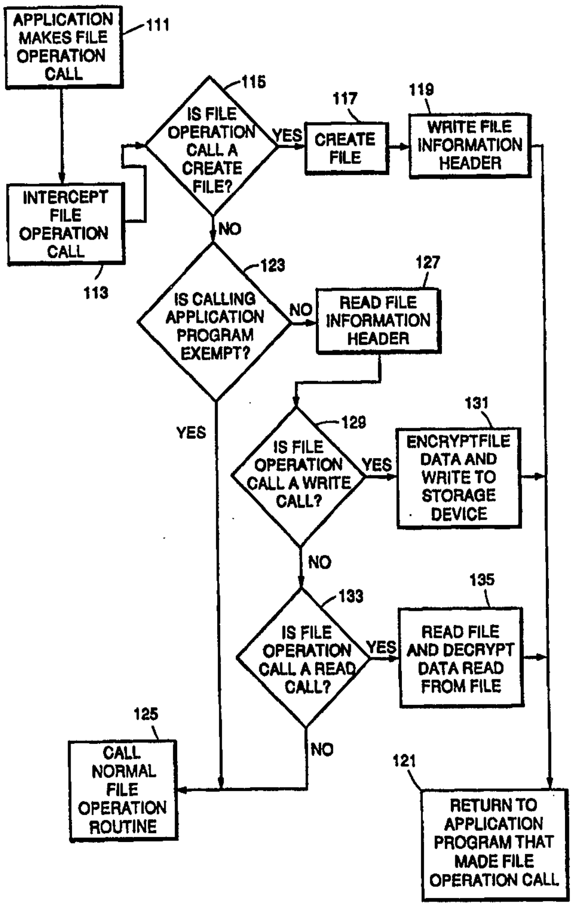
(81) Designated States: AU, CA, JP, KR, NO, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: FILE ENCRYPTION SCHEME

(57) Abstract

A computer data storage system that includes a data storage device, and a processor for encrypting file data to produce encrypted file data and writing the encrypted file data to a computer file on the data storage device, wherein the computer file includes a file information header that contains information indicating that the computer file contains encrypted file data.


APPLICATION MAKES FILE OPERATION CALL
111
INTERCEPT FILE OPERATION CALL
113
115
IS FILE OPERATION CALL A CREATE FILE?
YES
117
CREATE FILE
119
WRITE FILE INFORMATION HEADER
NO
123
IS CALLING APPLICATION PROGRAM EXEMPT?
NO
127
READ FILE INFORMATION HEADER
YES
129
IS FILE OPERATION CALL A WRITE CALL?
YES
131
ENCRYPTFILE DATA AND WRITE TO STORAGE DEVICE
NO
133
IS FILE OPERATION CALL A READ CALL?
YES
135
READ FILE AND DECRYPT DATA READ FROM FILE
NO
125
CALL NORMAL FILE OPERATION ROUTINE
121
RETURN TO APPLICATION PROGRAM THAT MADE FILE OPERATION CALL

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.

AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgystan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SI	Slovenia
SK	Slovakia
SN	Senegal
TD	Chad
TG	Togo
TJ	Tajikistan
TT	Trinidad and Tobago
UA	Ukraine
US	United States of America
UZ	Uzbekistan
VN	Viet Nam

FILE ENCRYPTION SCHEME

BACKGROUND OF THE INVENTION

The disclosed invention is generally directed to computer security systems, and more particularly to a computer system that wherein files stored on a data storage device are individually encrypted.

There is a recognized need for computer security such that confidential information stored in a computer system can be accessed only by authorized users. A commonly utilized element of computer security is encryption whereby information is encrypted in accordance with a predetermined "key" and decryption requires knowledge of the key. For example, a computer disk drive can be encrypted to make access to the information contained on the drive more difficult. Similarly, data communicated between computer systems can be encrypted so that the communication would be more difficult to understand if intercepted.

A consideration with known techniques of encryption at the level of a data storage device such as a disk drive, however, is the need to decrypt the entire contents of the data storage device, for example, as part of a startup process, so as to enable access to the contents of the data storage device, which would be time consuming and moreover would leave all of the contents of the data storage device unprotected. Also, the entire contents of the data storage device would have to be encrypted as part of a shutdown process, which would also be time consuming. Moreover, encryption of a data storage device is typically done with a single key, and thus the entire contents of a data storage device would be vulnerable if the encryption key became known to unauthorized users.

A consideration with known techniques of encryption at the communication level includes degraded performance due to the need for encryption of the information to be transmitted. Further, to the extent that the received information is to be stored on an encrypted data storage device, all of the information stored on the device including the received information would have to be encrypted, after the contents of the data storage device and the received information are initially decrypted.

SUMMARY OF THE INVENTION

It would therefore be an advantage to provide a secure computer system that allows for encryption and decryption of less than the entire contents of a data storage device.

Another advantage would be to provide a secure computer system that does not require a separate encryption process to transfer encrypted information to another computer system.

The foregoing and other advantages are provided by the invention in a computer data storage system that includes a data storage device, and a processor for encrypting file data to produce encrypted file data and writing the encrypted file data to a computer file on the data storage device, wherein the computer file includes a file information header that contains information indicating that the computer file contains encrypted file data. The processor further reads and decrypts the encrypted file data.

BRIEF DESCRIPTION OF THE DRAWINGS

The advantages and features of the disclosed invention will readily be appreciated by persons skilled in the art from the following detailed description when read in conjunction with the drawing wherein:

FIG. 1 is a schematic block diagram of a computer system in which file encryption in accordance with the invention can be implemented.

FIG. 2 is a schematic depiction of the logical organization of an encrypted computer file in accordance with the invention.

FIG. 3 is a simplified flow diagram that schematically depicts the logic flow of an illustrative example of file encryption in accordance with the invention.

DETAILED DESCRIPTION OF THE DISCLOSURE

In the following detailed description and in the several figures of the drawing, like elements are identified with like reference numerals.

Referring now to FIG. 1, schematically depicted therein by way of illustrative example is an overall block diagram of a computer hardware system in which file encryption in the invention can be implemented. The system includes a central processor unit 11 which performs general digital operations for the computer system and a primary storage memory 13 which stores data and programs including processes which when executed by the central processor unit 11 implement file encryption in accordance with the invention. By way of illustrative example, the primary storage memory 13 can include in accordance with conventional techniques random access memory as well as read only memory. The computer system further includes peripheral devices 15 such as a display 15a, a keyboard 15b, a data storage device 15c, a printer 15d, and a modem 15e. A data bus 17 provides for communication between the processor, the primary storage memory, and the peripheral devices.

In accordance with the invention, a computer file is stored on the data storage device 15c in encrypted form wherein encryption is performed at the file level such that encryption and decryption are performed on a file by file basis. As schematically illustrated in FIG. 2, an encrypted computer file is stored in a logical form of encrypted file data 51 (e.g., programs and user data) and a non-encrypted file header 53. By way of illustrative example, the file header 53 includes file control information such as operating system type 55 and a pointer 57 that points to the encryption key for the encrypted file data or one or more other pointers to the encryption key for the encrypted file data. The file data 51 contains user information such as a program or data, and can also contain further control information such as security access control labels.

Referring now to FIG. 3, set forth therein is a schematic flow diagram of the logic flow of an illustrative example of a file encryption procedure in accordance with the invention. The procedure of FIG. 3 is implemented by execution of one or more appropriately configured programs by the central processor unit 11 of FIG. 1. At 111 an application program makes a file operation call to the operating system utilized in the computer system of FIG. 1, and at 113 the file operation call is intercepted. A file operation call is typically a call to an operating system routine that performs a conventional file operation such as create, open, read, write, and close. Techniques for interception of operating system calls are well known in the art, and the particular nature of the intercept mechanism will depend on the particular operating system with which the invention is implemented, and can involve, for example, redirecting file operation calls to routines of the invention. At 115 a determination is made as to whether the intercepted file operation call is a create file call. If yes, at 117 a computer file is created conventionally, for example, by calling or invoking the normal create file routine that performs the operations involved in creating a file such as allocating data blocks, updating the operating system file control information, and inserting records into an appropriate directory or catalog that is conventionally utilized in operating systems to identify files stored on a data storage device and the data blocks allocated to the files. At 119, a file information header for the file is written on the data storage device in the data blocks allocated for the file, and at 121 control returns to the calling application program.

As used herein the term "normal" in the context of a file operation routine refers to a standard or built-in routine contained in a computer operating system for performing operations associated with or requested by a file operation call.

If the determination at 115 is no, at 123 a determination is made as to whether the application program making the intercepted file operation call is exempt from the need to decrypt the file that is the subject of the intercepted file operation call. For example, a file copy program or a file transfer program can operate on files without decryption. Further examples of exempt applications would include electronic mail applications, back-up applications, and an application that implements the subject invention. If the determination at 123 is yes, at 125 a call is made to the normal file operation routine that would have been called if the intercepted file operation call had not been intercepted.

If the determination at 123 is no, at 127 the file information header for the file that is the subject of the intercepted file operation call is read. At 129 a determination is made as to whether the intercepted file operation call is a write to file. If yes, at 131 the file data to be stored is encrypted to form encrypted file data, and the encrypted file data is written to the data storage device. As described earlier, such file data can include file control labels as well as user data such as a program or data. The encryption and write operations are performed, for example, by encrypting the file data one portion at a time, buffering each encrypted file data portion in a file buffer, which can be contained in the memory 13 of FIG. 1, and calling the normal write to file routine to write the buffered encrypted file data portion to the data storage device.

If the determination at 129 is no, at 133 a determination is made as to whether the intercepted file operation call is a read. If yes, at 129 the file that is the subject of the intercepted file operation call is read and decrypted. The reading and decryption of the file can be achieved, for example, by calling the normal read file routine to read the encrypted file data into a file buffer, which can be contained in the memory 13 of FIG. 1, and then decrypting the buffered encrypted file data to produce decrypted file data. In accordance with conventional techniques, the encrypted file data is read into the file buffer one portion at a time, wherein the portion read is of a fixed size. The buffered encrypted data is then decrypted and copied to a destination location in the memory 13, and the next portion of the encrypted file data is read into the file buffer. After all of the encrypted file data has been read and decrypted, at 121 control returns to the application program that made the intercepted file operation call.

If the determination at 133 is no, control is transferred to the normal file operation routine that would have been called had the intercepted file operation call not been intercepted.

The foregoing procedure essentially intercepts each file operation call and determines whether operations related to encryption and decryption of a file that is the subject of the file operation call are required. If not, the normal file operation routine that would have been invoked by the intercepted file operation call is invoked. If operations related to encryption and decryption are required, the procedure of the invention performs such operations which include encrypting file to be written to the data storage device, invoking the normal file operation routine to write encrypted file data to the data storage device, invoking the normal file routine to read the encrypted file data from the data storage device, and decrypting the encrypted file data read from the data storage device.

While the foregoing illustrative example of the invention is based on encrypting all files stored on an operating system, it should be appreciated that encrypted and non-encrypted files can be mixed, in which case the procedure of FIG. 3 would be modified to include checking for whether a file to be created is to be encrypted. If not, the normal create file routine is called, and a file information header is not written for the file. Also, as to file operations involving an existing file, a determination is made as to whether the existing file is encrypted, which can be determined, for example, from a catalog or directory record if a provision is made to include encryption status in the catalog or directory record, or alternatively, the file can be read to determine whether it includes a file information header as described above relative to FIG. 1. If the existing file is not encrypted, the normal file operation is invoked by a call to the file operation routine that would have been called had the intercepted file operation call not been intercepted.

Effectively, all file operation requests are intercepted, and procedures necessary to achieve file encryption and decryption are inserted between the file operations calls and the file operation routines that would normally be called by the intercepted file operation calls. Such inserted procedures, for example, generate the data required for the file information header and then call to the normal write to file routine to write the file information header on the data storage device. Further, the inserted procedures generate the encrypted file data that is to be written on the data storage device, and then invoke the normal write to file routine to write the encrypted file data on the data storage device. For read purposes the inserted procedures invoke the normal read file routine to read the encrypted file data from the data storage device, and then decrypt the encrypted file data that has been read. The encryption and decryption procedures are transparent to the calling application program since the application program makes normal file operation calls and receives normal responses thereto.

The foregoing has been a disclosure of a computer file encryption scheme that encrypts files on a file by file basis, which advantageously allows files to be individually encrypted and decrypted without the need to encrypt and decrypt the entire contents of a data storage device, and without intervention by the user. The encryption scheme of the invention allows different files on the same storage device to have different encryption keys, which provides for increased security and reduces the amount of information that becomes vulnerable should an encryption key become inappropriately known. Also, only selected computer files are decrypted at any given time, which maintains the security of the remaining files.

Although the foregoing has been a description and illustration of specific embodiments of the invention, various modifications and changes thereto can be made by persons skilled in the art without departing from the scope and spirit of the invention as defined by the following claims.

CLAIMS

What is claimed is:

1. A computer data storage system comprising:

a data storage device;

means for encrypting file data to produce encrypted file data;

means for writing said encrypted file data to a computer file on said data storage device, wherein said computer file includes a file information header that contains information indicating that the computer file contains encrypted file data; and

means for reading and decrypting said encrypted file data.

2. A method for storing data on a computer data storage device, comprising the steps of:

writing to the computer data storage device a file information header for a computer file on the computer data storage device, wherein the file information header contains (a) information indicating that computer file includes encrypted file data and (b) information that refers to an encryption key;

encrypting file data to be stored in the computer file to produce encrypted file data;

writing the encrypted file data to the computer file;

reading the file information header and obtaining the encryption key;

reading the encrypted file data of the computer file; and

decrypting the encrypted file data read from the computer file.

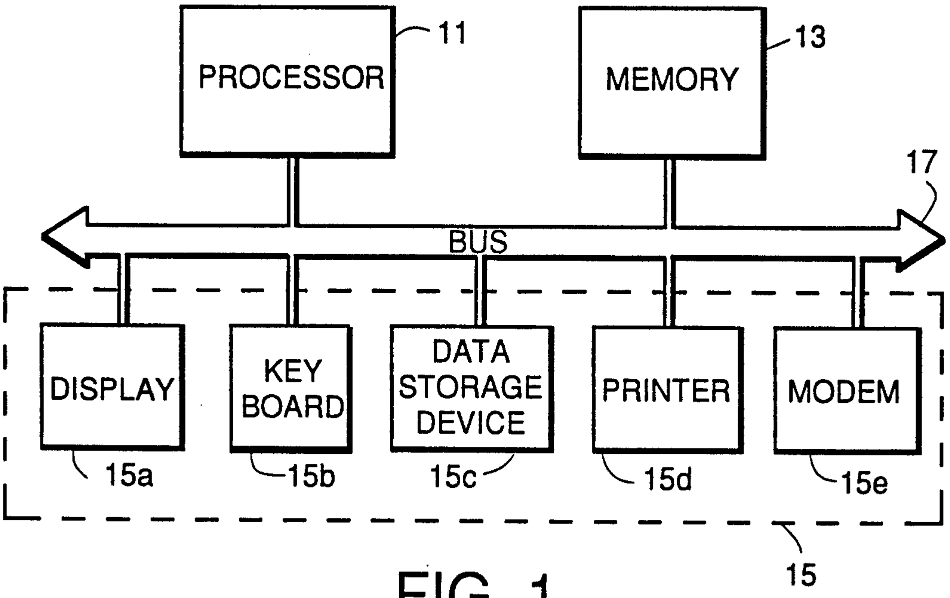

PROCESSOR
11
MEMORY
13
17
BUS
DISPLAY
KEY BOARD
DATA STORAGE DEVICE
PRINTER
MODEM
15a
15b
15c
15d
15e
15

FIG. 1.

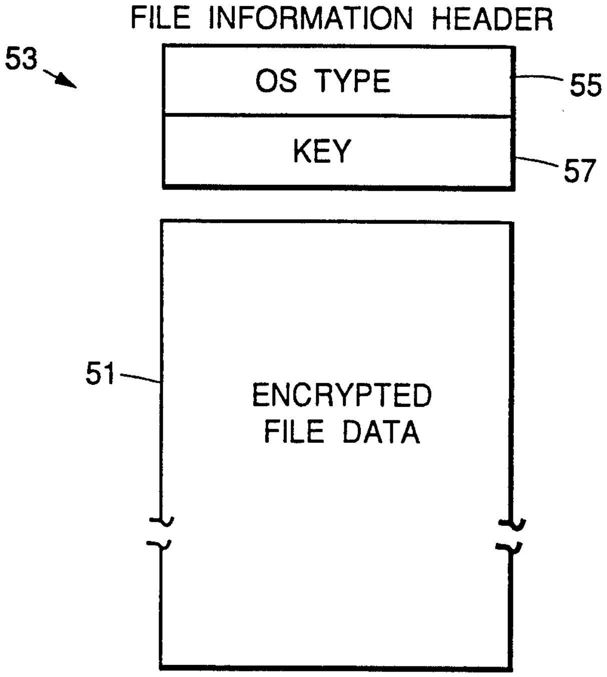

FILE INFORMATION HEADER
53
OS TYPE
55
KEY
57
51
ENCRYPTED FILE DATA

FIG. 2.

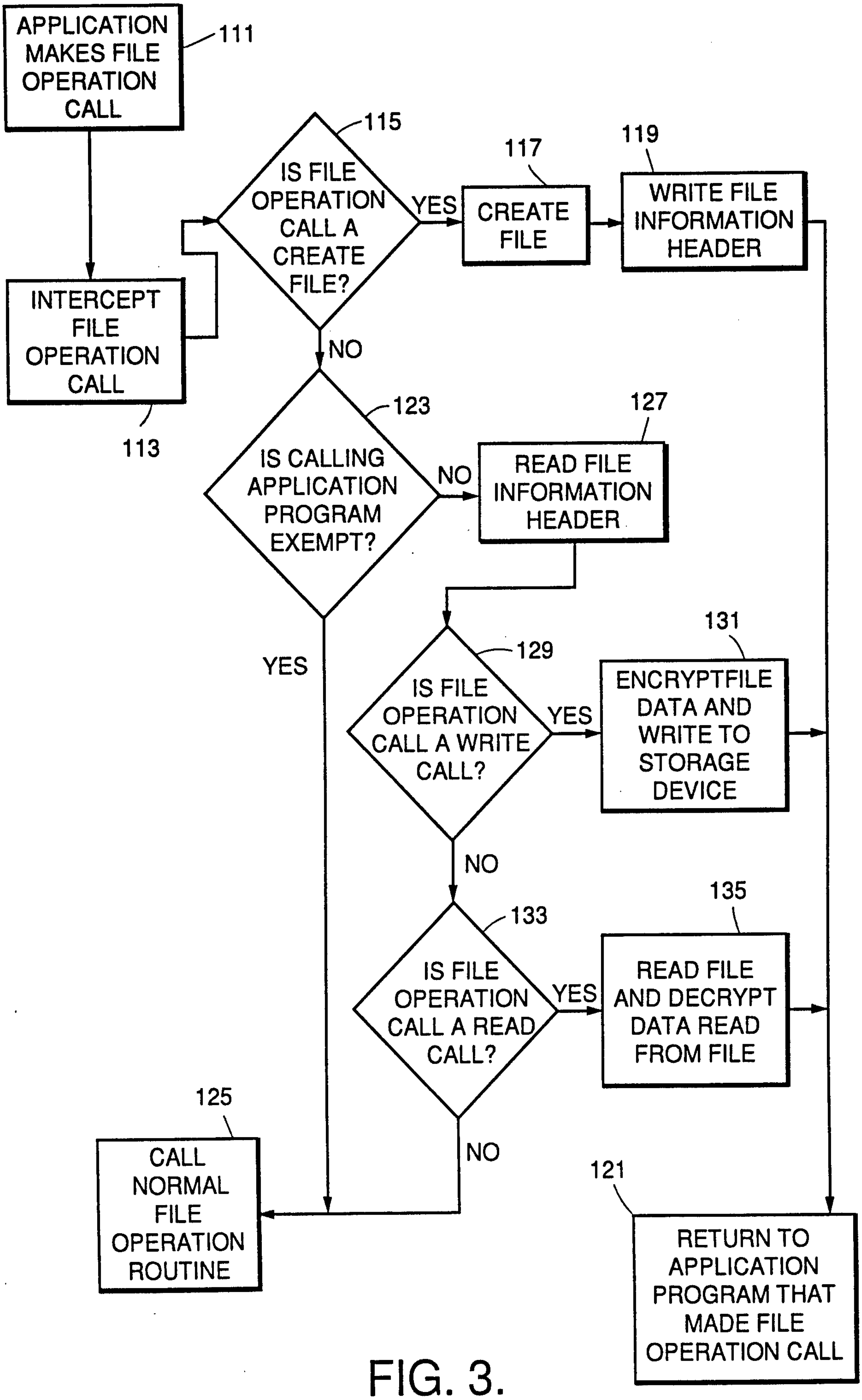

APPLICATION MAKES FILE OPERATION CALL
111
INTERCEPT FILE OPERATION CALL
113
IS FILE OPERATION CALL A CREATE FILE?
115
YES
CREATE FILE
117
WRITE FILE INFORMATION HEADER
119
NO
IS CALLING APPLICATION PROGRAM EXEMPT?
123
NO
READ FILE INFORMATION HEADER
127
YES
IS FILE OPERATION CALL A WRITE CALL?
129
YES
ENCRYPTFILE DATA AND WRITE TO STORAGE DEVICE
131
NO
IS FILE OPERATION CALL A READ CALL?
133
YES
READ FILE AND DECRYPT DATA READ FROM FILE
135
NO
CALL NORMAL FILE OPERATION ROUTINE
125
RETURN TO APPLICATION PROGRAM THAT MADE FILE OPERATION CALL
121

FIG. 3.

INTERNATIONAL SEARCH REPORT

Intern .al Application No
PCT/US 95/06329

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F12/14

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US,A,4 864 616 (POND ET AL) 5 September 1989 see abstract; figures 2,4 see column 6, line 6 - line 34 see column 8, line 21 - line 58 ---	1,2
A	US,A,4 757 533 (ALLEN ET AL) 12 July 1988 -----	

□ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in 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" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another 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

1

Date of the actual completion of the international search 21 September 1995	Date of mailing of the international search report 12. 10. 95
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Powell, D

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern.. ,nal Application No

PCT/US 95/06329

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A-4864616	05-09-89	NONE	
US-A-4757533	12-07-88	NONE	