

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
4 September 2008 (04.09.2008)

PCT

(10) International Publication Number
WO 2008/104020 A1

(51) International Patent Classification:
G06F 12/14 (2006.01)

(21) International Application Number:
PCT/AU2008/000249

(22) International Filing Date:
26 February 2008 (26.02.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2007901066 1 March 2007 (01.03.2007) AU

(71) Applicant (for all designated States except US): **HOME ENTERTAINMENT SUPPLIERS PTY LTD** [AU/AU]; 126 Bonds Road, Riverwood, New South Wales 2210 (AU).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **STANBOROUGH, Zachariah** [AU/AU]; 17/57 Nesca Parade, The Hill, New South Wales 2300 (AU).

(74) Agent: **FREEHILLS PATENT & TRADE MARK ATTORNEYS**; Level 38, MLC Centre, 19-29 Martin Place, Sydney, NSW 2000 (AU).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

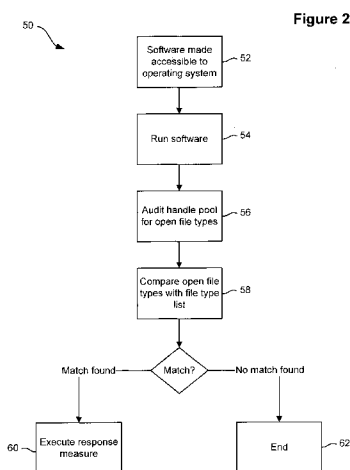
Declaration under Rule 4.17:

— of inventorship (Rule 4.17(iv))

Published:

— with international search report

(54) Title: DEVICE AND METHOD FOR DETECTING SOFTWARE PIRACY



(57) Abstract: The present invention provides software (13) to be run by an operating system (14) on a computing system (10), the software (13) including instructions for determining whether the software (13) is unauthorised and, if unauthorised, instructions relating to one or more response measures, wherein the instructions are configured to cause the operating system (14) to audit the types of files open on the operating system (16) against the types of files in a list of file types (15) and, if the type of a file open on the computing system matches a type of file appearing in the list (15), causing the operating system (14) to execute one or more response measures (60).

WO 2008/104020 A1

Device and method for detecting software piracy

Field of the invention

The present invention relates to a device and method for detecting software piracy.

Background of the invention

5 Software is often distributed on read only memory devices. Such devices include, for example, compact discs (CD's), digital versatile discs (DVD's), and cartridges or propriety discs. It is well known that a significant problem concerning software is that of piracy and illegal copying of the software. As technology develops so too does the ability to make and distribute illegal copies of what was originally legitimately obtained
10 digital content.

One way of attempting to prevent such piracy is by providing software on special or proprietary media such as discs or cartridges. By providing software on a proprietary media the number of people with access to hardware that can create copies of the software is limited compared to the number of people who can create copies of simple
15 CD's and DVD's.

A further problem, however, arises in the ease and speed with which a single copy of a piece of software can be distributed to multiple people over the Internet. Due to this it takes only a single person to make a copy and make that copy available for download to reduce or negate most of the advantages associated with distribution on a proprietary
20 disc or cartridge.

Accordingly, it would be desirable to provide a device and method to aid in the prevention of software piracy or to provide a device and method that dissuades software piracy.

Summary of the invention

25 In one aspect the present invention provides a method for determining whether software being run by an operating system on a computing system is an unauthorised copy, the

method including the steps of auditing the types of files open on the operating system against a list of file types and, if the type of a file open on the operating system matches a type of file appearing in the list determining the software to be unauthorised and executing one or more response measures.

- 5 In one embodiment, the operating system maintains in a memory of the computing system a handle pool in which file handles of all open files are recorded, and the step of auditing the types of files open on the operating system includes auditing all files appearing in the handle pool.

10 In one embodiment the list includes types of files known to be used in the distribution and/or running of unauthorised software.

In one embodiment, the software includes instructions which, when the software is run by the operating system, initiate the auditing step. The software may also include the list of file types.

15 Alternatively, the operating system includes instructions which, when the software is run by the operating system, initiate the auditing step. The operating system may also include the list of file types.

20 Further alternatively, the system on which the operating system and software is being run includes a system memory accessible by the operating system and the instructions for initiating the auditing step and/or the list of file types are stored on the system memory. The system memory may be an embedded memory such as a BIOS chip.

The one or more response measures may include discontinuing running the software, deleting the software, storing a record of the software, and/or notifying a third party via a network of the software.

25 In a second aspect the present invention provides software to be run by an operating system on a computing system, the software including instructions for determining whether the software is unauthorised and, if unauthorised, instructions relating to one or more response measures, wherein the instructions are configured to cause the

operating system to audit the types of files open on the operating system against the types of files in a list of file types and, if the type of a file open on the computing system matches a type of file appearing in the list, causing the operating system to execute one or more response measures.

- 5 In one embodiment the list of file types is included in the software instructions, however the list of file types may be stored on a system memory accessible by the operating system.

In a third aspect the present invention provides a medium on which software is recorded, the software including instructions as discussed above.

- 10 In a fourth aspect the present invention provides a method for determining whether software being run by an operating system on a computing system is an unauthorised copy, the computing system including a processing system for running an operating system, a BIOS, a first memory device and a communication interface for interfacing with one or more second memory devices, wherein if the software is run from the one or
15 more second memory devices connected to the communication interface one or more files must be opened, the method including the steps of auditing the types of files opened on the operating system against a list of file types and, if the type of a file open on the operating system matches a type of file appearing in the list determining the software to be unauthorised and executing one or more response measures.
- 20 In one embodiment, the operating system maintains a handle pool in which file handles of all open files are recorded, and the step of auditing the types of files open on the operating system includes auditing all files appearing in the handle pool.

In one embodiment the list includes types of files known to be used in the distribution and/or running of unauthorised software.

- 25 In one embodiment, the software includes instructions which, when the software is run by the operating system, initiate the auditing step. The software may also include the list of file types.

Alternatively, the operating system includes instructions which, when the software is run by the operating system, initiate the auditing step. The operating system may also include the list of file types.

Further alternatively, the instructions for initiating the auditing step and/or the list of file types are stored on the BIOS.

The one or more response measures may include discontinuing running the software, deleting the software, storing a record of the software, and/or notifying a third party via a network of the software.

Further aspects of the present invention, which should be considered in all its novel aspects, will become apparent from the following description.

Brief description of the drawings

The invention will now be described with reference to the accompanying drawings which show embodiments of the invention. It is to be understood, however, that the invention is not limited to the features of the embodiments shown in the drawings in which:

Figure 1 provides a simplified depiction of a generic computing system suitable for use in the preferred embodiment of the present invention;

Figure 2 provides a flow chart of the preferred method for detecting certain types of content being run by the computing system of figure 1; and

Figure 3 provides a high level flow chart of the instructions to be included in a software program or operating system in accordance with an embodiment of the invention.

Detailed description of the embodiments

Referring to figure 1, a simplified depiction of a generic computing system suitable for use in the embodiments of the present invention is shown. The components represented in the system may be found as part of any number of computing devices

such as desktop computers, portable computers such as laptops, personal digital assistants (PDA's), digital book reading screens, and hand held gaming units.

The system 10 includes a central processing unit (CPU) 11 and a basic input output system 12 (BIOS) which stores and executes initial startup instructions to be run by the CPU 11 when the computing system is first switched on. The BIOS 12 is generally provided on an embedded memory such as a BIOS chip. The system 10 also includes an operating system 14 configured to execute various programmed instructions and software and control operation of the central processing unit. Amongst other things the operating system 14 controls the CPU in respect of accessing an internal memory 16, controlling input devices 18, and controlling output devices 20.

The input devices 18 controllable by the operating system 14 may include a keyboard or keypad 22, a communication receiver 24 such as a wireless receiver or network interface card and one or more disk readers 26 (e.g. a CD drive, DVD drive, memory card reader, cartridge reader). The output devices 20 controllable by the operating system may, for example, include a screen or monitor 28, a speaker 30, a communication transmitter 32 (such as a wireless transmitter or network interface card), and disc writer 34 (such as a CD/DVD writer or memory card slot). In the physical system the communication receiver 24 and communication transmitter 32 may be incorporated in the same physical device for example a connection to a DSL line, as may be the disc reader 26 and disc writer 34. Other input and output devices may also be used, and, of course, not all input and output devices will be available on all computing systems.

In order to run software 13 on the system 10 the software 13 must be accessible to the operating system 14. This access may be achieved by storing the digital content in the internal memory 16, by making the content accessible to the operating system 14 over a network (through the communication receiver 24), or by inserting a disc/card/cartridge into an appropriate disc reader 26.

Operating system 14 manages file access by use of file handles and a handle pool 17. Each time a new file is opened the operating system 14 creates a file handle which

uniquely identifies that file and can be used by the operating system 14 to access and manipulate that file. The operating system 14 then stores that file handle in a handle pool 17. When a file is closed the operating system removes the associated file handle from the handle pool 17. Accordingly, at any given time the open files on a system can
5 be determined by reference to the handle pool 17.

Referring now to figure 2, a method 50 for determining whether an unauthorised copy of software 13 is being run by the operating system 14 is described. As an initial step, and as discussed above, the software 13 is made accessible 52 to the operating system 14. Through the operating system 14 a user of the system 10 then directs the software 13
10 to be run 54 which causes the operating system 14 to begin executing instructions contained within the software 13.

As discussed below, the software 13 includes auditing instructions along with a list of file types 15. When the digital content is run 54 the auditing instructions cause the operating system 14 to undertake an audit 56 of files concurrently open by the operating
15 system. This is done by review of the handle pool 17 as discussed above which provides a list of file handles by which all files open on the operating system 14 may be ascertained and accessed. While in this embodiment the list of file types 15 has been described as part of the software 13, the list of file types 15 could equally be stored elsewhere and accessed by the software 13 during the auditing process. The list of file
20 types 15 could, for example, be stored on a BIOS chip, on the memory 16 of the system 10, or be provided as part of the operating system 14.

Once the concurrently open files are identified, the types of those files are compared 58 to the file types in the list of file types 15. If the type of an open file matches a file type appearing in the list of file types 15, the auditing instructions of the software 13 cause
25 the operating system 14 to execute one or more response measures 60. If none of the open file types match any of the file types appearing in the list 15 the digital content continues running 62.

The appropriate file types to include in the list of file types 15 will depend on the intended application and target of the present invention. For example, software 13 is

often illegally copied, distributed and run by providing disc images of the original version of the software. Such images may, for example, be a .ISO file type or .CISO file type, and may be distributed either on a physical memory disc/memory card or over a network. In order to run a .ISO or .CISO file that file must be opened (causing the
5 operating system to create a file handle for that file and record it in the handle pool 17) to access the executable file relating to the software intended to be run.

In light of this the file types included in the list could include .ISO and .CISO files, and in the event that an open file is identified as being of that type, the operating system interprets the existence of this open file as an indicator that a file from which the
10 instructions are presently being executed is unauthorised and executes the response measures 60.

The response measures 60 may include instructions to log a record of the software 13 and the file type in the list that was open while the software 13 was being run. If the system 10 is, for example, connected to the internet, the instructions in the digital
15 content may also cause the operating system 14 to send a record of this to a third party. Finally, the instructions may cease the running of the software 13 and or cause the software 13 to be deleted.

Referring to figure 3, and as mentioned above, the software 13 is written to include instructions and a list of file types 15. While it is advantageous that the instructions 70
20 are written to be executed shortly or immediately on the execution of the software 13 itself, it is of course possible to include the instructions to be executed at any point during the execution of the software 13 or at multiple points. The instructions should include instructions to access the handle pool 17 to obtain file handle details of currently open files 72, review the files associated with the file handles to determine their type 74,
25 and compare 76 those file types with the list of file types 15. If a match between the currently open file types and a file type in the list 15 occurs, the instructions should further log the event 78 and then exit 80. If no match between the types of files open and the types of files in the list of file types 15 occurs, the instructions should continue processing as normal and proceed 82 the software 13 to those instructions for running
30 the main program.

The following is psuedocode appropriate for use where the file handles of a system are accessed as integers. All handles from 0 to 100 inclusive are tested. If known identifier data is present at a known identifier location then a flag gets set. If this flag is found to be set after the file_handle testing has completed, then appropriate action can be taken.

5

Begin

copy_detected_flag := 0
file_handle := 0

10

loop while(file_handle <= 100)
 seek(file_handle, known_identifier_location)
 test_identifier := read(file_handle, known_identifier_size)
 if(test_identifier = known_identifier)
15 copy_detected_flag := 1
 break from loop
 endif

20

 file_handle := file_handle + 1
endloop

if(copy_detected_flag = 1)
 respond to detected copy
endif

25

Use of the method in relation to a PlayStation® Portable (PSP) handheld gaming device from Sony® will now be described by way of a specific but non-limiting example.

Authorised software such as games are generally provided for the PSP on proprietary memory devices which are inserted into a device reader of the PSP to be run. The PSP
30 also, however, includes a memory stick reader which allows a user to store digital content on a memory stick and have that content read by the operating system of the PSP.

A common way of obtaining and running pirated games is by modifying the BIOS of the PSP to allow executable files to be run from a memory stick. Once this modification has
35 occurred, users can upload game file images (such as .ISO or .CISO files) onto a

memory stick and run the game from the memory stick reader. When the game is run from the memory stick reader the operating system must first open the .ISO or .CISO file (causing the creation and recordal of a file handle) on the memory stick to be able to access the actual game executable file. As discussed above, this executable file
5 includes instructions which upon execution cause the operating system to audit the types of open files and compare them with a list of file types. When the operating system matches the .ISO or .CISO file (which has been opened to allow access to the game) to a file in the list, it determines that the executable file is being run from a pirated copy of the game and executes appropriate response measures, for example
10 completing the execution of the software and/or closing the file.

While the above has been described with the instructions and list of file types being included in a software program, it will be appreciated that the instructions and/or list may be run from alternate locations. For example, the instructions may be included in the software but the list of file types stored in the internal memory 16 or even BIOS 12
15 of the system 10. This is advantageous in that the types of files recorded in the list may be easily updated without having to re-write the software code.

Alternatively, the software itself may not include either the list of file types or the instructions. In this case the operating system 14 or BIOS 12 would include the instructions and list in such a way that any time an executable file is run the instructions
20 are also run.

It will be understood that the invention disclosed and defined in this specification extends to all alternative combinations of two or more of the individual features mentioned or evident from the text or drawings. All of these different combinations constitute various alternative aspects of the invention.

CLAIMS

1. A method for determining whether software being run by an operating system on a computing system is an unauthorised copy, the method including the steps of
auditing the types of files open on the operating system against a list of file types
5 and,
if the type of a file open on the operating system matches a type of file appearing in the list of file types determining the software to be unauthorised and executing one or more response measures.
2. A method according to claim 1, wherein the operating system maintains in a
10 memory of the computing system a handle pool in which file handles of all open files are recorded, and the step of auditing the types of files open on the operating system includes auditing all files appearing in the handle pool.
3. A method according to either claim 1 or claim 2, wherein the list of file types includes types of files known to be used in the distribution and/or running of
15 unauthorised software.
4. A method according to any one of the preceding claims, wherein the software further includes instructions which, when the software is run by the operating system, initiate the auditing step.
5. A method according to any one of claims 1 to 3, wherein the operating system
20 includes instructions which, when the software is run by the operating system, initiate the auditing step.
6. A method according to any one of the preceding claims, wherein the software includes the list of file types.
7. A method according to any one of claims 1 to 4, wherein the operating system
25 includes the list of file types.

8. A method according to any one of claims 1, 2, 3, 5, or 7, wherein the system on which the operating system and software is run includes a system memory accessible by the operating system, and the instructions for initiating the auditing step and/or the list of file types are stored on the system memory.
- 5 9. A method according to claim 8, wherein the system memory is an embedded memory.
10. A method according to claim 8 wherein the embedded memory is a BIOS chip.
11. A method according to any one of the preceding claims, wherein the one or more response measures are selected from the list: discontinuing running the software;
10 deleting the software; storing a record of the software; and/or notifying a third party via a network of the software.
12. Software to be run by an operating system on a computing system, the software including instructions which when run determine whether the software is unauthorised and, if unauthorised, instructions relating to one or more response measures, wherein
15 the instructions are configured to cause the operating system to audit the types of files open on the operating system against the types of files in a list of file types and, if the type of a file open on the computing system matches a type of file appearing in the list, cause the operating system to execute one or more response measures.
13. Software according to claim 12, wherein the list of file types is included in the
20 software instructions
14. Software according to claim 12, wherein the list of file types is stored on a system memory accessible by the operating system.
15. Software according to claim 14, wherein the system memory is an embedded memory.
- 25 16. Software according to claim 15, wherein the embedded memory is a BIOS chip.

17. Software according to any one of claims 12 to 16, wherein the one or more response measures are selected from the list: discontinuing running the software; deleting the software; storing a record of the software; and/or notifying a third party via a network of the software.

5 18. A medium on which software according to any one of claims 12 to 17 is recorded.

19. A method for determining whether software being run by an operating system on a computing system is an unauthorised copy, the computing system including

a processing system for running an operating system,

a BIOS,

10 a first memory device and a communication interface for interfacing with one or more second memory devices, wherein if the software is run from a said second memory device, one or more files is be opened, the method including auditing the types of files opened on the operating system against a list of file types and, if the type of a file open on the operating system matches a type of file appearing in the list, determining
15 the software to be unauthorised and executing one or more response measures.

20. A method according to claim 19, wherein the operating system maintains a handle pool in which file handles of all open files are recorded, and the step of auditing the types of files open on the operating system includes auditing all files appearing in the handle pool.

20 21. A method according to claim 19 or 20, wherein the list of file types includes types of files known to be used in the distribution and/or running of unauthorised software.

22. A method according to any one of claims 19 to 21, wherein the software further includes instructions which, when the software is run by the operating system, initiate the auditing step.

23. A method according to any one of claims 19 to 21, wherein the operating system includes instructions which, when the software is run by the operating system, initiate the auditing step.

24. A method according to any one of the claims 19 to 23, wherein the software
5 includes the list of file types.

25. A method according to any one of claims 19 to 23, wherein the operating system includes the list of file types.

26. A method according to any one of claims 19, 20, 21, 23, or 25, wherein the
10 system on which the operating system and software is run includes a system memory accessible by the operating system, and the instructions for initiating the auditing step and/or the list of file types are stored on the system memory.

27. A method according to claim 26, wherein the system memory is an embedded memory.

28. A method according to claim 27 wherein the embedded memory is a BIOS chip.

15 29. A method according to any of claims 19 to 28, wherein the one or more response measures are selected from the list of: discontinuing running the software; deleting the software; storing a record of the software; and/or notifying a third party via a network of the software.

30. A method according to any one of claims 1 to 11 or 19 to 33, wherein the list of
20 file types includes ISO and/or CISO file types.

31. Software according to any one of claims 12 to 17, wherein the list of file types includes ISO and/or CISO file types.

Figure 1

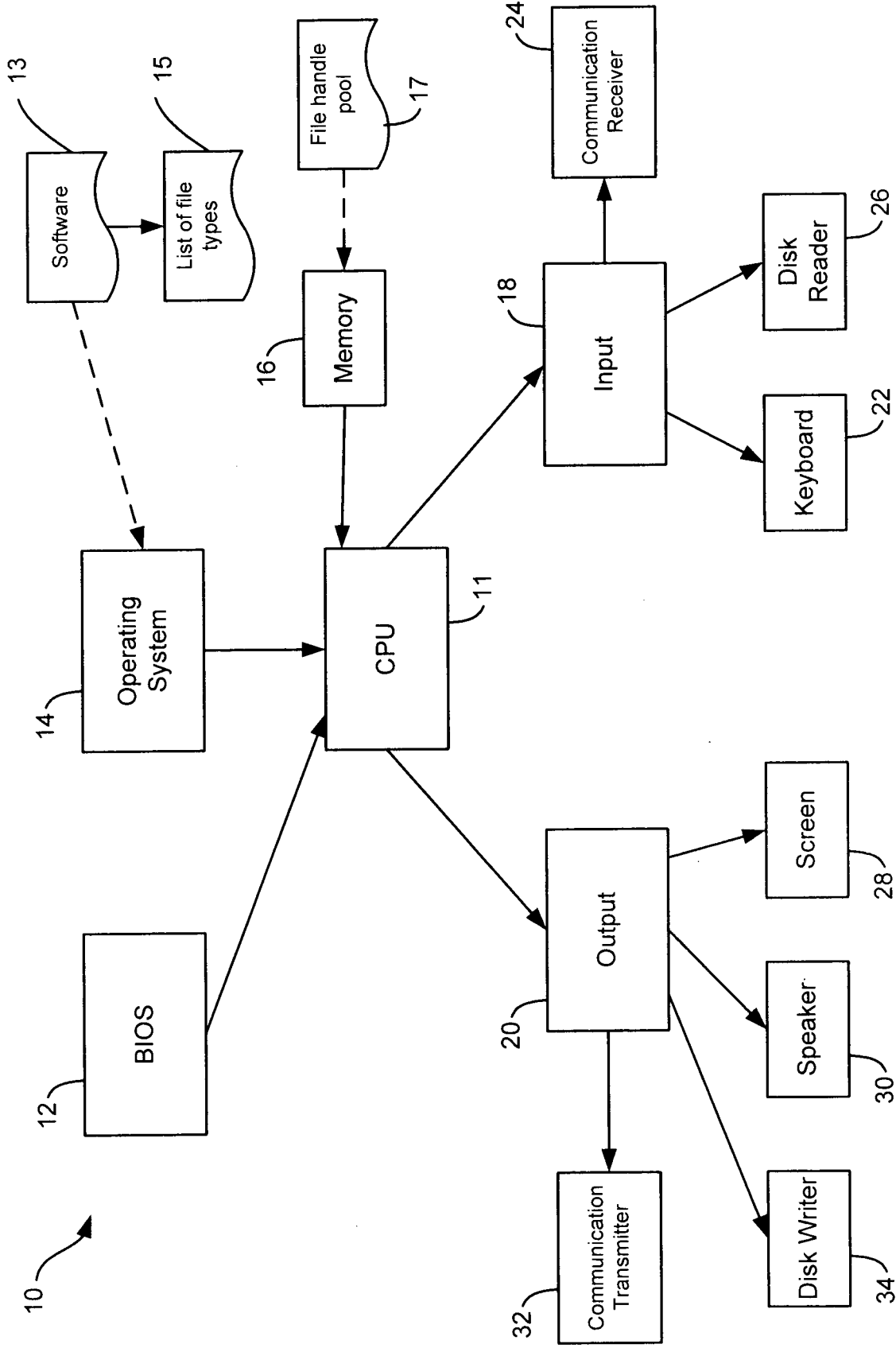


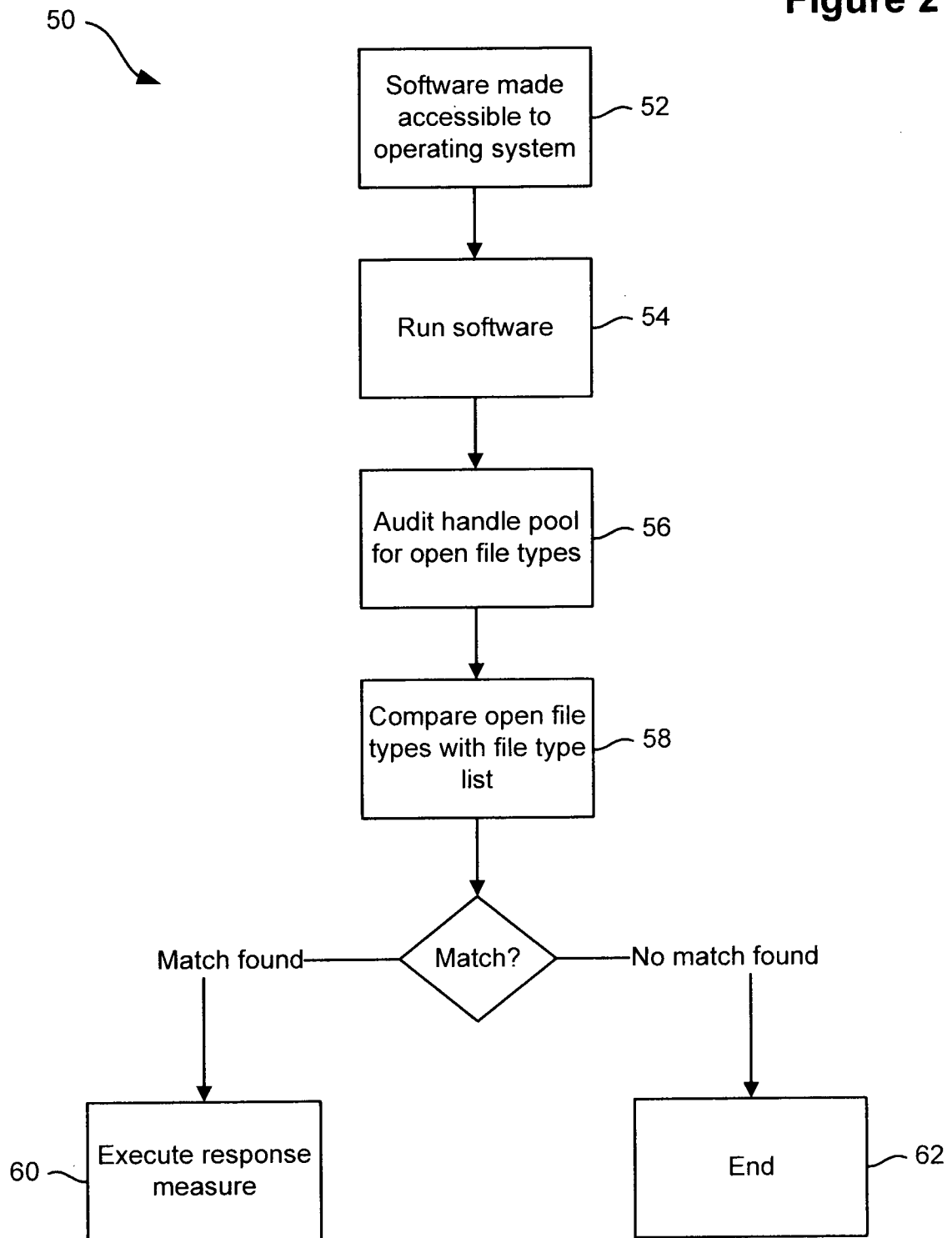
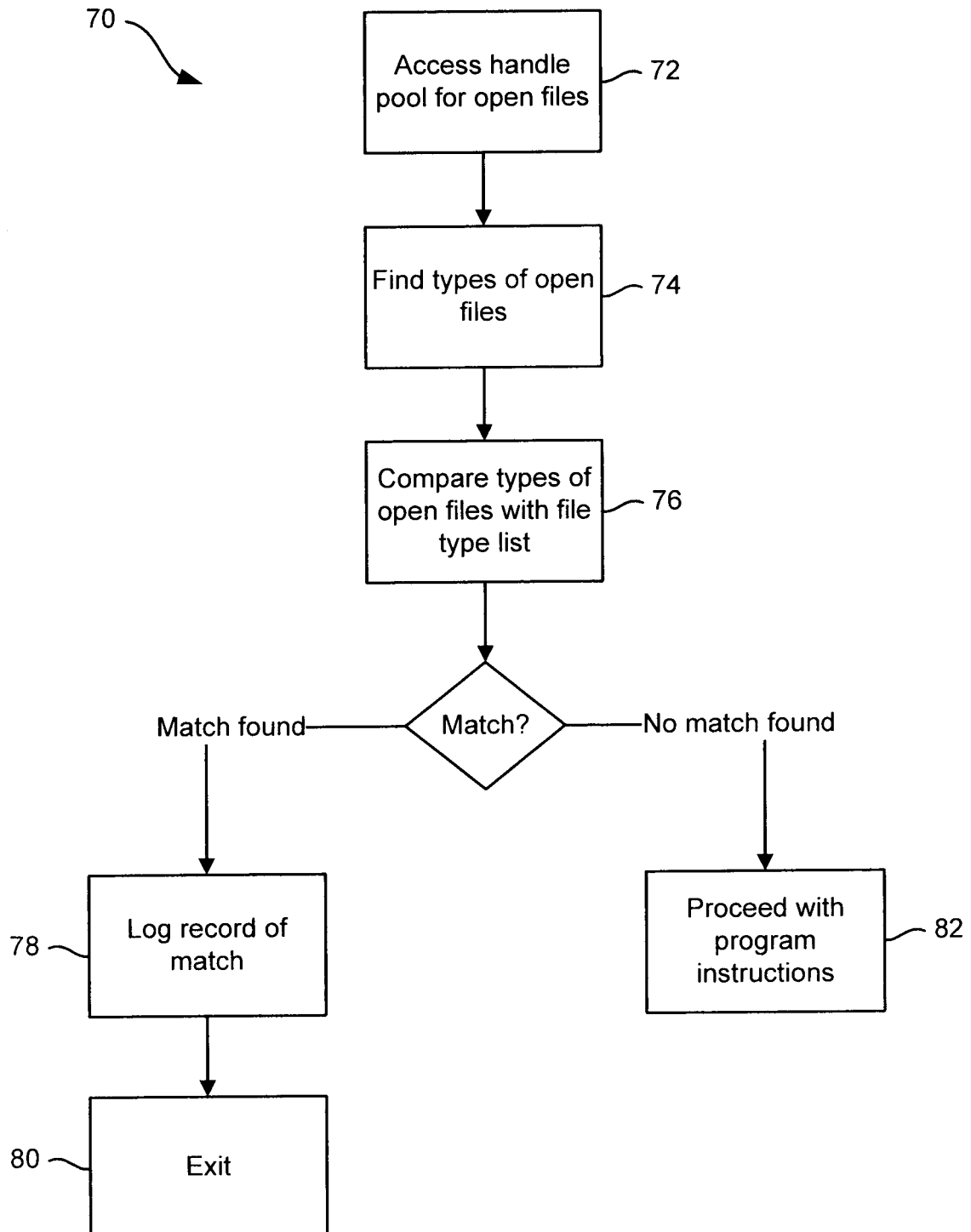
Figure 2

Figure 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2008/000249

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

G06F 12/14 (2006.01)

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)
IPC8: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 practicable, search terms used)

USPTO, DWPI & keywords: DRM, digital right management, audit, detect, software, piracy, pirate, illegal and similar terms

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5483658 A (GRUBE ET AL.) 9 January 1996 Entire document (see particularly figure 2; column 6, lines 9-19; column 7, lines 11-27)	1-31
Y	US 2002/0099952 A1 (LAMBERT ET AL.) 25 July 2002 Entire document (see particularly figures 1-9; paragraphs 0011, 0013, 0014, 0030, 0031, 0048, 0058, 0066)	1-31
Y	US 2004/0133801 A1 (PASTORELLI ET AL.) 8 July 2004 Entire document (see particularly figures 2, 3a; paragraphs 0015, 0020, 0066, 0074)	1-31
A	US 2006/0179486 A1 (BAHAR) 10 August 2006 Entire document	1-31

☐

Further documents are listed in the continuation of Box C

☒

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

"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

"E" earlier application or patent but published on or after the international filing date

"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

"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)

"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

"O" document referring to an oral disclosure, use, exhibition or other means

"&" document member of the same patent family

"P" document published prior to the international filing date but later than the priority date claimed

Date of the actual completion of the international search
26 March 2008Date of mailing of the international search report
07 APR 2008Name and mailing address of the ISA/AU
**AUSTRALIAN PATENT OFFICE
PO BOX 200, WODEN ACT 2606, AUSTRALIA
E-mail address: pct@ipaustralia.gov.au
Facsimile No. +61 2 6283 7999**Authorized officer
Benjamin Lam
AUSTRALIAN PATENT OFFICE
(ISO 9001 Quality Certified Service)
Telephone No : (02) 6225 6121

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/AU2008/000249

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member	
US 5483658	US 5388212 US 5507009	US 5469569 US 5745677	US 5502831
US 2002099952	NONE		
US 2004133801	CN 1582421	EP 1466228	WO 03038570
US 2006179486	US 7024696		
Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.			
END OF ANNEX			