OPIC
Office de la propriété intellectuelle du Canada

CIPO
Canadian Intellectual Property Office

(12) (19) (CA) **Demande-Application**

(21) (A1) **2,332,962**

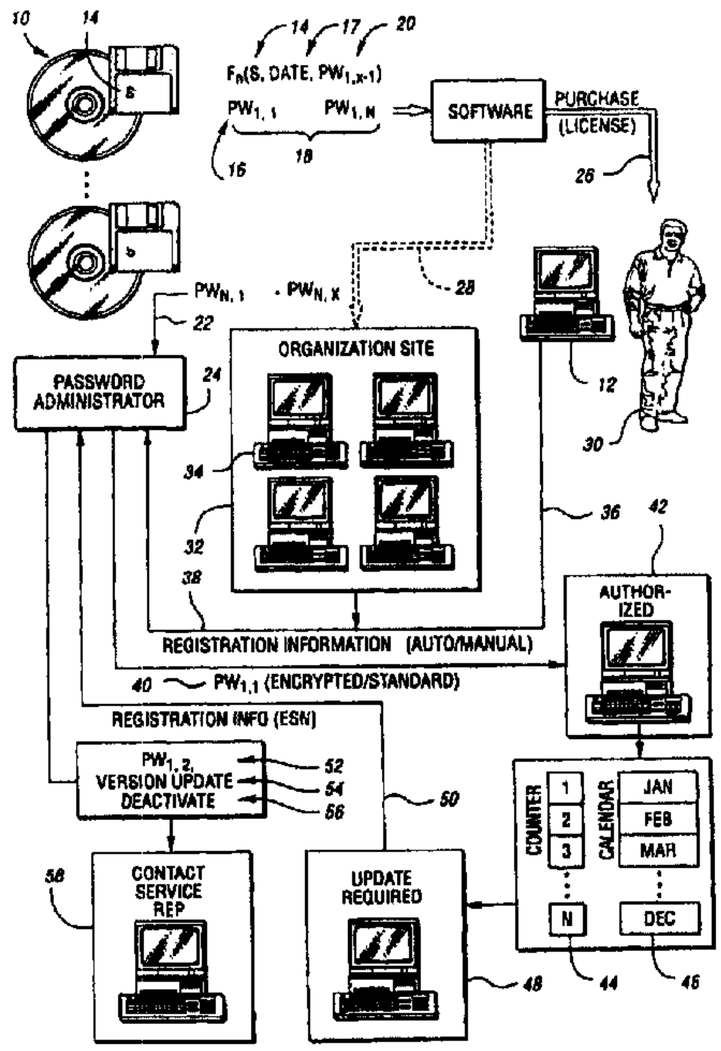
(86) 1999/05/27
(87) 1999/12/09

(72) COLVIN, DAVID S., US
(71) Z4 TECHNOLOGIES, INC., US

(51) Int.Cl.[6] H04L 9/00, H04L 9/06
(30) 1998/06/04 (09/090,620) US

(54) **PROCEDE ET DISPOSITIF DE SECURISATION D'UN LOGICIEL, DESTINES A REDUIRE UN USAGE NON AUTORISE DE CELUI-CI**

(54) **METHOD AND APPARATUS FOR SECURING SOFTWARE TO REDUCE UNAUTHORIZED USE**



(57) L'invention concerne un procédé et un dispositif de sécurisation d'un logiciel, destinés à réduire un usage non autorisé du logiciel, le procédé consistant à associer un mot de passe (16) ou une série de mots de passe (18) à chaque copie ou groupe de logiciels autorisés, et à exiger l'entrée d'un premier mot de passe obtenu à partir du développeur du logiciel ou du représentant autorisé (24) de celui-ci, après échange d'informations d'enregistrement (38). Ce procédé et ce dispositif peuvent également exiger l'entrée d'un second mot de

(57) A method and apparatus for securing software to reduce unauthorized use include associating a password (16) or series of passwords (18) with each copy or group of authorized software and requiring entry of a first password obtained from the developer or authorized representative (24) of the software after exchanging registration information (38). The method and apparatus may also require entry of a second password from the series associated with the software to continue using the software. A password (16) or authorization code series

OPIC
Office de la propriété intellectuelle du Canada

CIPO
Canadian Intellectual Property Office

(21) (A1) 2,332,962

(86) 1999/05/27
(87) 1999/12/09

passe à partir de la série associée au logiciel pour la continuation de l'utilisation du logiciel. Un mot de passe (16) ou une série de codes d'autorisation peut être associé à chaque copie autorisée ou à un groupe de copies, tel ceux distribués à une organisation ou à un site (32) en particulier. De préférence, des mots de passe (16) ou codes d'autorisation ultérieurs sont obtenus à partir d'un développeur (24), fabricant ou distributeur de logiciels autorisé, lequel recueille des informations actuelles à partir de l'utilisateur (30) afin de pouvoir surveiller si cet utilisateur observe les restrictions de l'octroi de licence. Le nombre et la fréquence des mises à jour des mots de passe exigés peuvent être réguliers ou non. Un code mettant hors service le logiciel peut être communiqué si le fabricant détermine que l'utilisateur (30) est un utilisateur non autorisé.

may be associated with each authorized copy or with a group of copies such as those distributed to a particular organization or site (32). Preferably, subsequent passwords (16) or authorization codes are obtained from an authorized software developer (24), manufacturer, or distributor which gathers current information from the user (30) to monitor compliance with licensing restrictions. The number and frequency of required password updates may be regular or irregular. A code which disables the software may be communicated if the manufacturer determines that the user (30) is an unauthorized user.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00, 9/06 — A1

(11) International Publication Number: WO 99/63705

(43) International Publication Date: 9 December 1999 (09.12.99)

(21) International Application Number: PCT/US99/11647

(22) International Filing Date: 27 May 1999 (27.05.99)

(30) Priority Data:
09/090,620 — 4 June 1998 (04.06.98) — US

(63) Related by Continuation (CON) or Continuation-in-Part (CIP) to Earlier Application
US — 09/090,620 (CON)
Filed on — 4 June 1998 (04.06.98)

(71)(72) Applicant and Inventor: COLVIN, David, S. [US/US]; 3786 Ranya Drive, Commerce Township, MI 48382 (US).

(74) Agents: BIR, David, S. et al.; Brooks & Kushman, 22nd floor, 1000 Town Center, Southfield, MI 48075 (US).

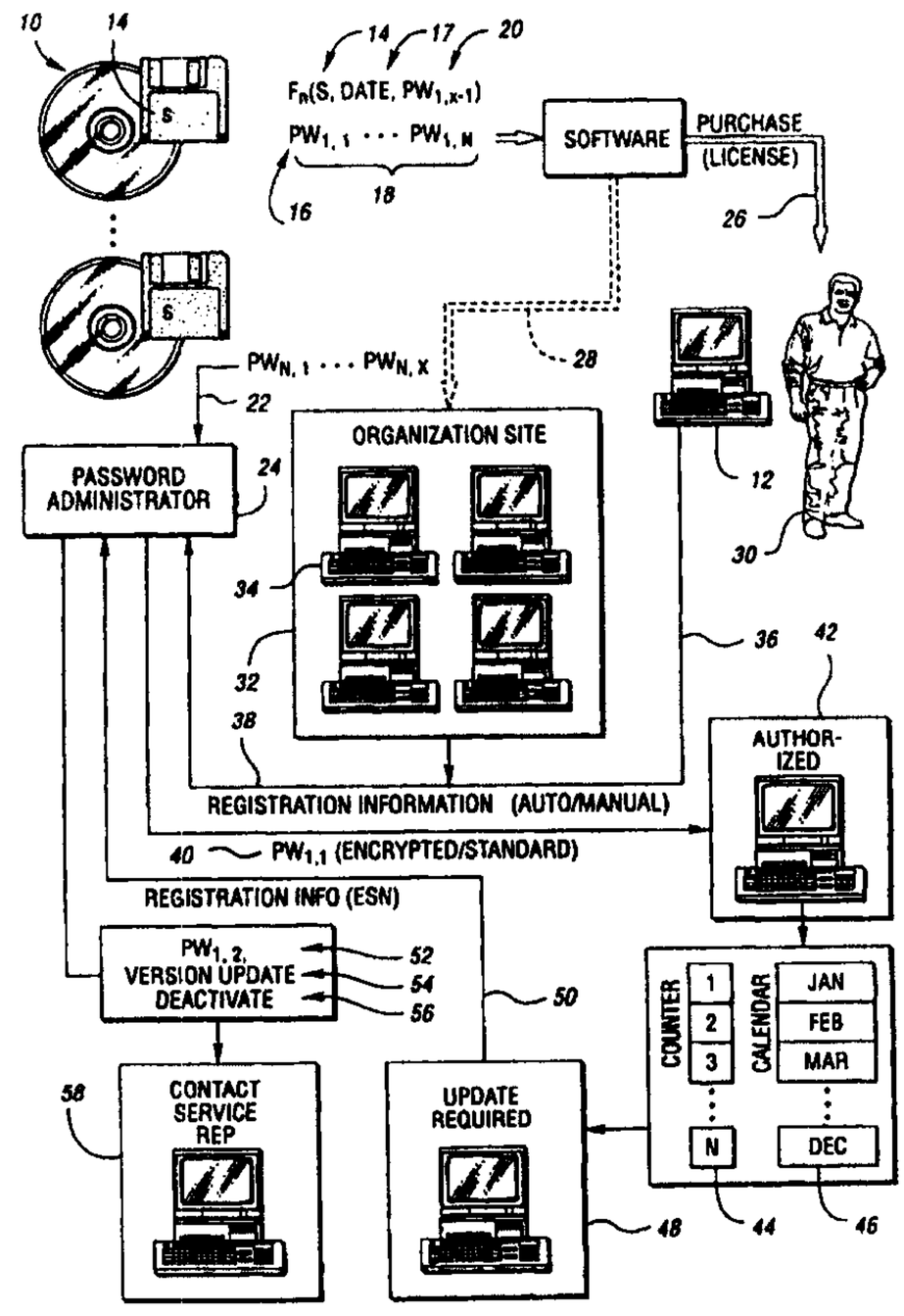
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US,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

Published
With international search report.

(54) Title: METHOD AND APPARATUS FOR SECURING SOFTWARE TO REDUCE UNAUTHORIZED USE

(57) Abstract

A method and apparatus for securing software to reduce unauthorized use include associating a password (16) or series of passwords (18) with each copy or group of authorized software and requiring entry of a first password obtained from the developer or authorized representative (24) of the software after exchanging registration information (38). The method and apparatus may also require entry of a second password from the series associated with the software to continue using the software. A password (16) or authorization code series may be associated with each authorized copy or with a group of copies such as those distributed to a particular organization or site (32). Preferably, subsequent passwords (16) or authorization codes are obtained from an authorized software developer (24), manufacturer, or distributor which gathers current information from the user (30) to monitor compliance with licensing restrictions. The number and frequency of required password updates may be regular or irregular. A code which disables the software may be communicated if the manufacturer determines that the user (30) is an unauthorized user.



METHOD AND APPARATUS FOR SECURING SOFTWARE TO REDUCE UNAUTHORIZED USE

Technical Field

The present invention relates to apparatus and methods for reducing unauthorized use of software.

Background Art

Software developers are often victims of illicit copying and unauthorized use of their software in violation of contractual obligations imposed by licensing agreements and subject to civil and criminal penalties under various domestic and foreign laws. Unauthorized entities range from a relatively small percentage of the total users to an overwhelming majority of illegal users. Such unauthorized use not only amounts to theft of the developers' intellectual property, but also reduces the number of programs sold and therefore the associated profitability of the developer. This may ultimately diminish the creative effort expended by the software developers due to the reduced financial incentive. The advent of the internet has contributed to the proliferation of pirated software, known as "warez", which is easily located and readily downloaded.

Various strategies have been employed to make unauthorized duplication and use of software more difficult. One such approach is to provide a hardware "key" which is typically installed in the parallel port

of the computer to provide a software interlock. If the key is not in place, the software will not execute. This method is relatively expensive for the developer and cumbersome for the authorized user while remaining vulnerable to theft by duplication of the hardware key.

Another approach requires the user to enter a serial number or customer identification number during installation of the software. Missing or invalid registration information prevents installation of the software. This approach is easily defeated by transferring the serial number or customer identification number to one or more unauthorized users.

Yet another approach requires registering the software with the manufacturer or distributor to obtain an operational code or password necessary for installation of the software. Again, once the operational code or password is obtained, it may be perpetually transferred along with pirated copies to numerous unauthorized users.

Various copy protection strategies have been employed to reduce the number of unauthorized copies available. This approach is generally disfavored by users who may have a legitimate need to make backup or archival copies or transfer a copy to a new computer or hard drive.

While prior art strategies have enjoyed various levels of success in reducing unauthorized use of software, they often impose a significant burden on the authorized users or are easily defeated by unauthorized users. As such, software developers need an apparatus and/or method for reducing unauthorized use.

of software which does not burden the authorized users to dissuade them from purchasing and using the protected software.

Summary Of The Invention

Thus, one object of the present invention is to provide an apparatus and method for improving software security throughout the lifetime of the software.

Another object of the present invention is to provide an apparatus and method for monitoring the number of users of a software product, both authorized and unauthorized.

Yet another object of the present invention is to provide an apparatus and method for the software manufacturer to maintain contact with the user over an extended period of time.

A further object of the present invention is to provide a method and apparatus for reducing unauthorized use of software which facilitate periodic software updates and forwarding of information, when and if desired.

A still further object of the present invention is to identify those entities responsible for unauthorized copying or use of software so that appropriate action may be taken, such as disabling the software, requesting payment from the user, or seeking civil or criminal penalties.

Another object of the present invention is to provide a method and apparatus for reducing unauthorized software use which deactivates unauthorized copies when an unauthorized user attempts to obtain a password.

In carrying out the above objects and other objects, features, and advantages of the present invention, a method for securing software includes associating a series of passwords or authorization codes with each copy or group of authorized software, requiring entry of a first password from the series associated with the software upon first use of the software, and subsequently requiring entry of a second password from the series associated with the software to continue using the software. A password or authorization code series may be associated with each authorized copy or with a group of copies such as those distributed to a particular organization or site. Preferably, subsequent passwords or authorization codes are obtained from an authorized software developer, manufacturer, or distributor which gathers current information from the user to monitor compliance with licensing restrictions. The number and frequency of required password updates may be regular or irregular depending upon the application, user, or software manufacturer.

The present invention contemplates, but does not require, more frequent password updates for more complex software because it is generally more costly to develop (and therefore more valuable to users) whereas less costly software would require fewer password updates to reduce administrative costs associated with password maintenance.

Password or authorization code updates may be obtained automatically or manually. Automatic updates are accomplished using electronic communication between the manufacturer's computer (or an authorized representative) and the user's computer. Updates may be performed by a direct modem connection, via email, a web browser, or the like. The particular time and nature of updates and the user interface utilized to implement the updates may vary by manufacturer or product. Manual updates are performed by advance or periodic notifications generated by the software to alert the user that password updates are required or will be required in the near future. The user may then contact the manufacturer for the specific password update via telephone, mail, email, or the like. Password advisories normally occur prior to the periodic termination of the operating period which may be measured by program starts, elapsed running time, calendar period, etc. Password updates may be in the form of alphanumeric and/or encrypted passwords or of any other conventional type.

Preferably, the user must provide registration information prior to receiving the original or updated password or authorization code. Registration information may be entered by the user or automatically acquired (and transmitted for automatic updates) by the software. Registration information may include a serial number, registration number, TCP/IP address, user name, telephone number, computer specific information, etc. This information may be encoded and/or encrypted to make it less susceptible to tampering by unauthorized users. The registration information is preferably monitored and compared to previously captured information to control the number of authorized copies of software and/or

identify unauthorized users. If unauthorized use is suspected, a password or authorization code may be provided which subsequently disables the software, either immediately or after some period of time so that an authorized user is provided an opportunity to rectify the information which caused deactivation.

A number of advantages result from various implementations of the present invention. For example, the present invention reduces unauthorized use of software without imposing a significant burden on authorized users. The present invention controls the number of copies of authorized software by monitoring registration information and deactivation of suspected pirated copies. Requiring authorized users to periodically update a password or authorization code provided by a password administrator improves accuracy of contact information for marketing related products and distribution of product updates. The present invention also provides a variable level of software security which can be tailored to the particular application depending upon the value of the application to potential software pirates.

The above advantages and other advantages, objects, and features of the present invention will be readily apparent from the following detailed description of the best mode for carrying out the invention when taken in connection with the accompanying drawings.

Brief Description Of The Drawings

Fig. 1 is a block diagram illustrating various features of a method and apparatus for securing software according to the present invention;

Fig. 2 is a flow diagram illustrating generally a method for securing software according to the present invention; and

Fig. 3 is a more detailed flow diagram illustrating representative embodiments of a method and apparatus for securing software according to the present invention.

Best Mode(s) For Carrying Out The Invention

Referring now to Fig. 1, a block diagram illustrating various features of a method and apparatus for securing software according to the present invention is shown. Manufacturers or developers create application programs or software which is stored in the form of data representing program instructions executable by a computer on computer readable media 10. Computer readable media 10 may include any medium capable of storing such instructions which is directly or indirectly readable by a computer, such as computer 12. Computer readable media may include floppy disks, hard drives, CD-ROMs, floptical disks, magnetic tape, and the like. Each copy or group of copies of the software may have an associated serial number, indicated generally by reference numeral 14, and an associated password 16 which may be one of a series of associated passwords 18 as explained in greater detail below. Each password 16 may be an alphanumeric character string which may be encoded or encrypted or a binary or hexadecimal machine readable string to resist tampering by unauthorized users. Passwords 16 within series 18 may be randomly assigned or may be generated using a suitable algorithm, many of which are known in the art. Likewise, passwords 16 may be based on serial number 14,

a current date or version date 17, and/or a previous password 20 from the series of passwords.

After the password or passwords are created and associated with one or more serial numbers or copies of the software, they may be transferred to an authorized representative of the software, as represented by arrow 22, such as a password administrator 24. Of course, the original manufacturer or developer of the software may also function as password administrator 24. The software may be distributed by purchase or more commonly it is licensed as represented by arrows 26 and 28 to individuals 30 and groups 32, respectively. Preferably, the software is distributed to the end users without its associated password 16 which must be obtained from password administrator 24. Alternatively, computer readable media 10 may be distributed with the first password 16 of a series of passwords 18. Each authorized user preferably has software with a unique identifier, such as a serial number, whether the authorized user is an individual, such as user 30, or a group or region, indicated generally by reference numeral 32. However, the same password or series of passwords may be associated with a number of serial numbers to reduce the administrative burden for password administrator 24. For example, each end user 34 associated with organization or site 32 may have the same password or series of passwords. Preferably, not more than one password is distributed with each authorized copy so that the end users will need to contact password administrator 24 to obtain additional passwords for continued use of the software as explained in greater detail below.

During the initial use or installation of the software on computers 12,34, a password or authorization code will be required by the software to function properly. The end user must contact the authorized representative for the software, such as password administrator 24, to obtain the appropriate authorization code or password as indicated generally by arrows 36. Password administrator 24 obtains registration information 38 from the end user and provides an appropriate password or authorization code to the software as indicated by reference numeral 40. Communication of registration information and the authorization code may be accomplished either manually or automatically depending upon the particular application and configuration of the software. Manual communication may be by email, regular mail, telephone, automated voice response system, web browser, direct modem transfer, or the like but requires a varying level of intervention by the end user depending upon the particular type of communication. Automatic communication may use similar methods or means to communicate the information but is performed without user intervention, although the user may be advised or notified that the process is occurring or has occurred.

Registration information 38 may include traditional contact information, such as name, address, email, phone, etc. but preferably includes information which can be obtained without intervention by the end user to improve its veracity. Such information may include identification of a TCP/IP address, originating telephone number, or computer-specific information associated with the end user. Computer-specific information may include an electronic serial number (ESN) which uniquely characterizes the hardware

configuration of the computer based on information stored in the computer's non-volatile CMOS, registry, motherboard serial number, or the like. Password administrator 24 preferably stores the registration information to be used for various purposes according to the present invention to reduce unauthorized use of software. For example, password administrator 24 may use the registration information to monitor compliance with licensing terms by determining whether a particular serial number has been installed on more than one computer or by more than one end user. Administrator 24 may compare the registration information with previously received registration information to determine whether to issue an authorization code or password, or to provide a code which disables further operation of the software. The registration information may also be used to contact the end users for marketing new products or versions, or providing software updates.

The password or authorization code is communicated to the software as represented by reference numeral 40. Depending upon the particular implementation, the password may be provided to the end user who manually enters the information into the computer 42 to begin or continue using the software. The password or authorization code may be encoded as an alphanumeric string using various numbers and letters which represent meaningful information to the administrator but appear to be randomly generated to the end user. Alternatively, an encryption algorithm may be used to transmit the information. Preferably, the password authorizes the software to execute on computer 42 for a first predetermined period as represented by counter 44 or calendar 46. The predetermined period may vary based on the particular authorized user, the cost

of the software, the number of estimated unauthorized copies, etc. For example, it is anticipated that more expensive software would provide a shorter period of authorization to provide a higher level of security. The higher revenue generated by the software offsets any increased administrative expense of password administrator 24 due to the increased frequency of updates required.

As indicated by counter 44 and calendar 46, the authorized period of use may be measured either in calendar days (months, years, etc.) or in execution hours, number of accesses, or the like. Once the authorized period expires, the software requires a new password or authorization code as indicated by reference numeral 48. This may be accomplished automatically and transparently to the end user by electronically contacting password administrator 24 and exchanging current registration information 50. Administrator 24 may compare the current registration information 50 with previously received registration information to determine if at least a portion of the information matches for that particular serial number or group of serial numbers. This comparison may be used to determine whether the end user is an authorized user or an unauthorized user.

The information provided to the software by administrator 24 may depend upon whether the user is determined to be authorized or unauthorized. For example, if the user is determined to be an authorized user, a subsequent password 52 from the series of passwords associated with the software serial number or group may be communicated which authorizes the software for an additional operation period. As the software

becomes less valuable, such as when new versions are released, the authorization period may increase and preferably eventually allows indefinite use of the software. Of course, an exceedingly long period (10 years for example) may be essentially equivalent to an indefinite period of operation. In addition to a subsequent password, an updated version 54 of the software may be transferred or offered to the end user. If the user is determined to be an unauthorized user, an appropriate message may be transmitted to alert the user to a discrepancy in the registration information, and the operational password may be withheld. Alternatively or in addition, a code 56 which deactivates the software may be communicated. As another alternative, a shortened authorization period may be provided along with a password and a message which indicates the end user must contact administrator 24 or another customer service representative to verify the user's status as represented by reference numeral 58. In the event the user is determined to be unauthorized, password administrator 24 may decline to download a password at which time the software may automatically become inoperative after the current operational period has lapsed.

Referring now to Fig. 2, a flow diagram generally illustrating a method for securing software according to the present invention is shown. A password or series of passwords is associated with a particular copy or group of copies of software prior to distribution (without the password or with only one of a series of passwords) as represented by block 80. A series of passwords may be associated with the software using an appropriate password generation algorithm with parameters which vary based on the particular copy. For

example, a algorithm or mathematical equation or formula may be used to generate passwords with one or more of the parameters of the equation corresponding to letters or characters in the serial number of the software.

For applications which have only a single password for each copy or group of copies, the password may not be distributed with the software so the end user must contact the developer or authorized representative as represented by block 82. For applications with two or more passwords, an initial password may be provided or the software may operate without a password for a first period to provide ample opportunity for the end user to acquire the initial/subsequent password. Registration information may be required as a precondition to providing a valid authorization code or password. This allows the developer or authorized representative to monitor compliance with licensing terms and/or take appropriate action for unauthorized users.

The password or authorization code is communicated to the software as represented by block 84 to make the software operational on the end user's computer. This may be performed automatically, without user intervention, or manually when initiated by the user using various communication channels, such as regular mail, email, web browser, direct modem connection, etc. The method may optionally require periodic updates at regular, irregular, or random intervals based on elapsed running time, calendar time, or the like, as represented by block 86. The software may prompt the user when the end of the authorization period is approaching to provide an opportunity to obtain a subsequent authorization code for continued use

of the software.

Referring now to Fig. 3, a more detailed flow diagram illustrating a method and/or apparatus for securing software according to the present invention is shown. The software manufacturer or developer (source) produces software which requires initial and/or periodic password updates to become or to remain operational as depicted in box **112**. Software may be associated with individual end users, a regional (geographic) or other group of users, or users associated with a particular organization or site. Providing passwords or authorization codes for groups rather than each individual significantly reduces the number of passwords required and the corresponding administrative overhead including electronic storage and transmission requirements.

Following production by the software manufacturer, the source electronically stores the password information for future transmission to the user as shown in box **114**. The password information may be the actual passwords or information used to generate subsequent passwords based on the individual copy or group of copies of the software. The embodiment depicted in Fig. 3 is intended to interlock specific pieces or groups of software with corresponding passwords or authorization codes.

Once the software is acquired by the user **116**, the user installs (partially or fully) the software in his computer or computer network **118**. Following installation of the software, the user is prompted to register the software and obtain the necessary

operational password which may be an alphanumeric string which is encoded or encrypted, or a binary (machine readable) code. The user is allowed to choose between automatic or manual registration **120**. If automatic registration is selected **122**, the program automatically contacts the source via a modem or other connection to obtain the operational password following registration **124**.

Once contacted, the source searches for previous registration of the software with the registration number or user identification **126**. If the software has not been previously registered **128**, the source transmits the necessary password **130** wherein the software becomes operational **134**. If registration information has been previously entered and does not match the current registration information, the source notifies the user of a previous registration of the same software **132** and thereafter takes appropriate action **136**. Such action can either include denying the necessary operational password **138**, continuing the password download if the source desires **130** or other appropriate action or actions.

Following the initial registration of the software and downloading of the first operational password, the software remains operational for a given interval which may be an operation period or time period (random, regular, or irregular). Once the first interval expires, the program notifies the user of the necessity to obtain the next operating password **140**. The user's computer contacts the source via modem **142** and the source determines if previous inquiries have

been made for the same user **144** based on the registration information. These step(s) may be fully automated, thereby eliminating the need for user intervention or notifying the user.

The source either transmits the password **148** or notifies the user of a duplicate inquiry **149**. If a duplicate inquiry has been made, the source either declines to download **150** the password so that the software becomes non-operational **152** after the current operational period elapses or the source transmits the password **148** if desired. During any of the contact periods between the source and the user, the source may elect to download software updates or additional information **154**. Following the downloading or the necessary operational password, the software becomes or remains operational **156**. This sequence is selectively repeated **158** as determined by the authorization interval selected by the source and communicated to the software.

As shown in Fig. 3, the user may have the option of manual registration **160** and password input as opposed to automatic registration. Alternatively, the source may require manual registration to verify the accuracy of at least some of the registration information since it will be used to send the authorization code or password to the user. If the user provides inaccurate information, the password will not be transmitted and the software will not be operational. After initial registration, optionally the user may elect to convert to automatic electronic contact at any time. Where manual registration is selected **160** (or required), the user contacts the source via telephone,

mail, email, internet, or the like to obtain the operational password following registration **162**.

Once contacted, the source searches for previous registration of the software with the same serial number, registration number or user identification **164**. If the software has not been previously registered **166**, the source transmits the necessary password **168** wherein the software becomes operational **172**. If a duplicate registration occurs, the source notifies the user of a previous registration of the same software **170** and thereafter takes appropriate action **174**. Such action can either include not providing the necessary operational password **176** or continuing the password transmission if the source desires **168**.

Following the initial registration of the software and transmission of the first operational password, the software remains operational for a given operation interval after which the software notifies the user of the necessity to obtain the next operating password **178**. The user contacts the source via telephone or by mail **182** and the source determines if previous inquiries have been made for the same user **184**. The user may elect to convert to automatic electronic registration during this period **180**, however, this step is optional.

The source either transmits the password **188** or notifies the user of a duplicate inquiry **190**. If a duplicate inquiry has been made, the source either

declines to download the password **196** (after which the software becomes non-operational **198**) or the source transmits the password **188** if desired. During any of the contact periods between the source and the user, the source may elect to transmit software updates or additional information **192**. Following the downloading or the necessary operational password the software becomes or remains operational **194**. The sequence for successive operation intervals may then be repeated at the source's discretion **200**.

It is understood that the representative methods of the present invention do not need to continue after initial registration and password transmission. Likewise, the process may me discontinued at some point in time by downloading a lifetime password which authorizes the software indefinitely. For example, this may be desirable after the software is deemed obsolete. It is further understood that the specific sequencing of events is not necessary for the proper implementation of the present invention. The invention further allows for compatibility with existing software or other security measures.

While the best modes for carrying out the invention have been described in detail, those familiar with the art to which this invention relates will recognize various alternative methods for carrying out the invention as described by the following claims.

What Is Claimed Is:

1. A method for securing software to reduce unauthorized use of the software, the method comprising:

requiring entry of a first password upon first use of the software;

subsequently requiring entry of another password to continue using the software; and

periodically repeating the step of subsequently requiring entry of another password for continued operation of the software.

2. The method of claim 1 further comprising:

associating a series of passwords with the software for each authorized user prior to distribution of the software.

3. The method of claim 2 wherein the authorized user is a group having a separate copy of the software for each of at least two end users.

4. The method of claim 1 further comprising including not more than one of the passwords with the software for distribution to each authorized user.

5. The method of claim 1 further comprising obtaining at least one password from an authorized representative of the software.

6. The method of claim 5 wherein the step of obtaining comprises electronically communicating with the authorized representative.

7. The method of claim 1 further comprising repeating the step of subsequently requiring entry of another password at regular intervals.

8. The method of claim 1 further comprising:

requiring communication of registration information associated with the end user to an authorized representative of the software prior to communicating the password to the software.

9. A method of securing software to reduce unauthorized use, the method comprising:

associating a series of passwords with the software;

requiring an end user to contact a representative to obtain a password previously associated with the software; and

communicating a password previously associated with the software to the software, wherein the software is not functional until the password has been communicated.

10. The method of claim 9 wherein the step of communicating comprises electronically communicating the password.

11. The method of claim 9 wherein the step of communicating is performed automatically by the software and the authorized representative.

12. The method of claim 9 further comprising:

obtaining registration information associated with the end user as a precondition for performing the step of communicating the password.

13. The method of claim 12 wherein the step of obtaining registration information is performed substantially simultaneously with the step of communicating the password.

PCT/US 99/11647
IPEA/US 11 OCT 2000

14. The method of claim 12 wherein the step of obtaining registration information comprises obtaining registration information from a computer on which the software has been installed.

15. The method of claim 9 further comprising:

obtaining registration information associated with the end user; and

encoding the registration information so it is not readily discernible.

16. The method of claim 9 wherein the step of communicating comprises communicating the password to the end user enabling the end user to supply the password to the software.

17. The method of claim 9 further comprising:

periodically requiring a new password, the new password being obtained from the series of passwords previously associated with the software.

18. The method of claim 17 wherein the step of periodically requiring a new password is performed at regular intervals.

19. The method of claim 17 wherein the step of periodically requiring a new password is performed at intervals based on elapsed execution time of the software.

20. The method of claim 17 wherein the step of periodically requiring a new password is performed at intervals based on elapsed time.

21. The method of claim 17 wherein the step of periodically requiring a new password is performed at predetermined intervals.

22. The method of claim 9 further comprising:

periodically requiring registration information associated with the end user to obtain a new password, the new password being obtained from the series of passwords previously associated with the software.

23. The method of claim 22 further comprising:

comparing the registration information with previously obtained registration information associated with the software to determine whether the end user is an authorized user.

24. The method of claim 23 further comprising:

providing a new password only if at least a portion of the registration information matches previously obtained registration information.

25. The method of claim 9 further comprising:

periodically requiring a new password for continued operation of the software, the new password being obtained from the representative.

PCT/US 99/11647
IPEA/US 11 OCT 2000

26. The method of claim 9 further comprising:

periodically requiring a new password for continued operation of the software, the new password being obtained from the representative after providing registration information associated with the end user;

comparing the registration information with previously obtained registration information;

providing a new password which allows continued operation of the software if the step of comparing indicates the end user is an authorized user; and

providing a new password which disables the software if the step of comparing indicates the end user is an unauthorized user.

27. The method of claim 9 further comprising:

obtaining registration information associated with the end user as a precondition for performing the step of communicating the password; and

modifying the password based on the registration information.

28. The method of claim 9 further comprising determining a new password using a previous password.

29. A computer readable storage medium having data stored therein representing software executable by a computer, the software including instructions to reduce use of the software by unauthorized users, the storage medium comprising:

instructions for requiring an end user to contact an authorized representative to obtain a password associated with the software;

instructions for disabling the software until the password has been communicated to the software; and

PCT/US 99/11647
IPEA/US 11 OCT 2000

instructions for automatically contacting an authorized representative of the software to communicate registration information and obtaining authorization for continued operation of the software.

30. The computer readable storage medium of claim 29 further comprising:

instructions for obtaining registration information associated with the end user.

31. The computer readable storage medium of claim 29 further comprising:

instructions for periodically requiring entry of a new password for continued operation of the software.

32. The computer readable storage medium of claim 29 further comprising:

instructions for disabling the software after a predetermined password is communicated to the software.

33. The computer readable storage medium of claim 29 further comprising:

instructions for encoding the registration information.

34. A method of securing software to reduce use of the software by unauthorized users, the method comprising:

associating a series of passwords with each unit of software;

requiring communication of registration information to an authorized representative for the software to receive a first password from the series of

AMENDED SHEET

passwords associated with the software, the registration information being associated with an end user of the software;

periodically repeating the step of requiring communication of registration information to obtain a subsequent password from the series of passwords for continued operation of the software.

35. A method of securing software to reduce unauthorized use, the method comprising:

associating a plurality of passwords with the software and distributing one of the plurality of passwords concurrently with the software;

requiring an end user to contact a representative another one of the passwords previously associated with the software; and

communicating one of the passwords previously associated with the software to the software, wherein the software remains functional only until the password expires.

36. The method of claim 35 wherein the step of communicating comprises electronically communicating the password.

37. The method of claim 35 wherein the step of communicating is performed automatically by the software and the representative.

38. The method of claim 35 further comprising:

obtaining registration information associated with the end user as a precondition for performing the step of communicating the password.

39. The method of claim 35 further comprising:

periodically requiring a new password for continued operation of the software, the new password being obtained from the representative.

40. The method of claim 35 further comprising:

periodically requiring a new password for continued operation of the software, the new password being obtained from the representative after providing registration information associated with the end user;

comparing the registration information with previously obtained registration information;

providing a new password which allows continued operation of the software if the step of comparing indicates the end user is an authorized user; and

providing a new password which disables the software if the step of comparing indicates the end user is an unauthorized user.

41. The method of claim 35 further comprising:

obtaining registration information associated with the end user as a precondition for performing the step of communicating the password; and

modifying the password based on the registration information.

42. The method of claim 35 further comprising determining a new password using a previous password.

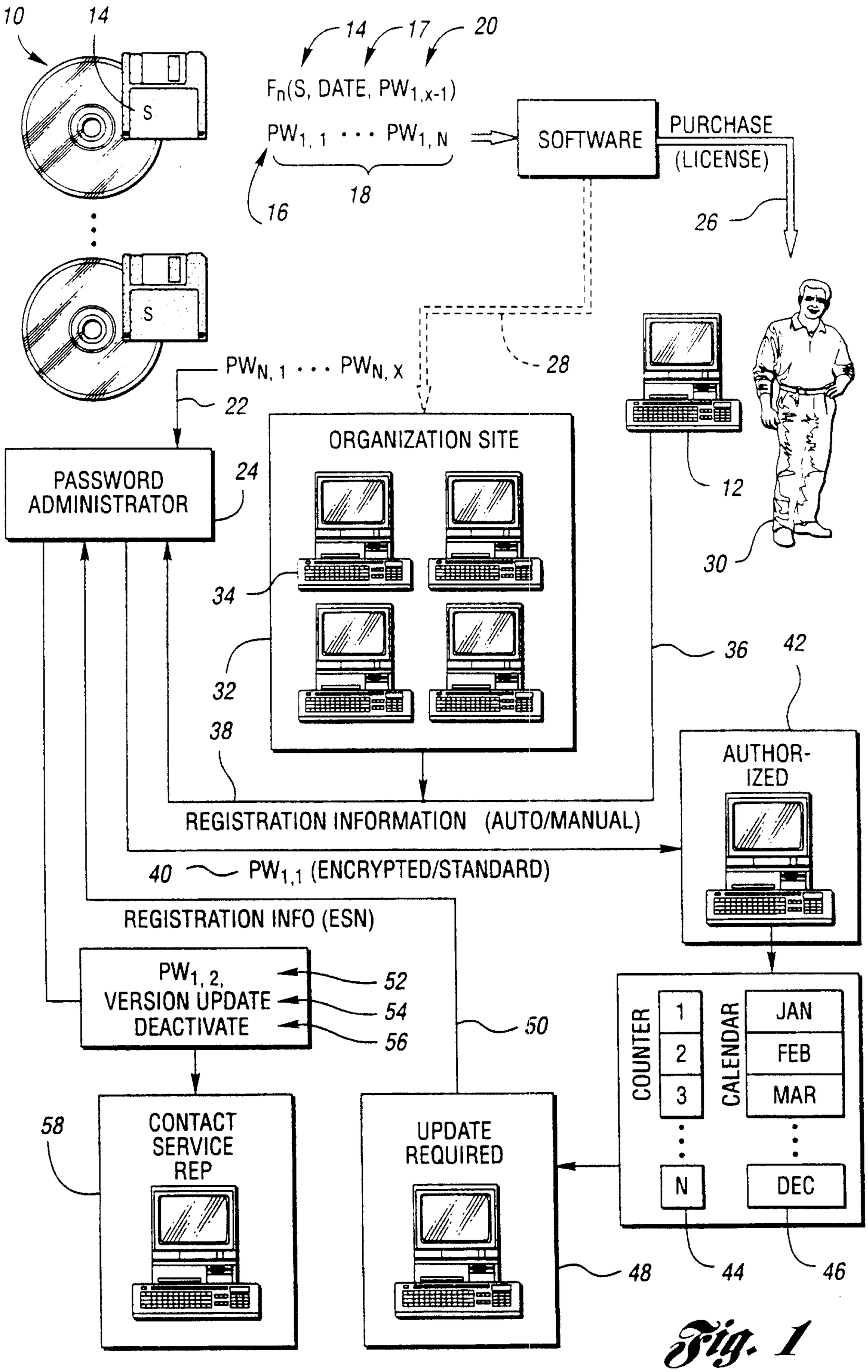

10
14
S
14
17
20
F_n(S, DATE, $PW_{1,x-1}$)
$PW_{1,1}$ ··· $PW_{1,N}$
18
16
SOFTWARE
PURCHASE
(LICENSE)
26
28
$PW_{N,1}$ ··· $PW_{N,X}$
22
PASSWORD ADMINISTRATOR
24
ORGANIZATION SITE
34
32
38
12
30
36
42
AUTHOR-IZED
REGISTRATION INFORMATION (AUTO/MANUAL)
40
$PW_{1,1}$ (ENCRYPTED/STANDARD)
REGISTRATION INFO (ESN)
$PW_{1,2,}$
VERSION UPDATE
DEACTIVATE
52
54
56
50
COUNTER
1
2
3
N
CALENDAR
JAN
FEB
MAR
DEC
58
CONTACT SERVICE REP
UPDATE REQUIRED
48
44
46

Fig. 1

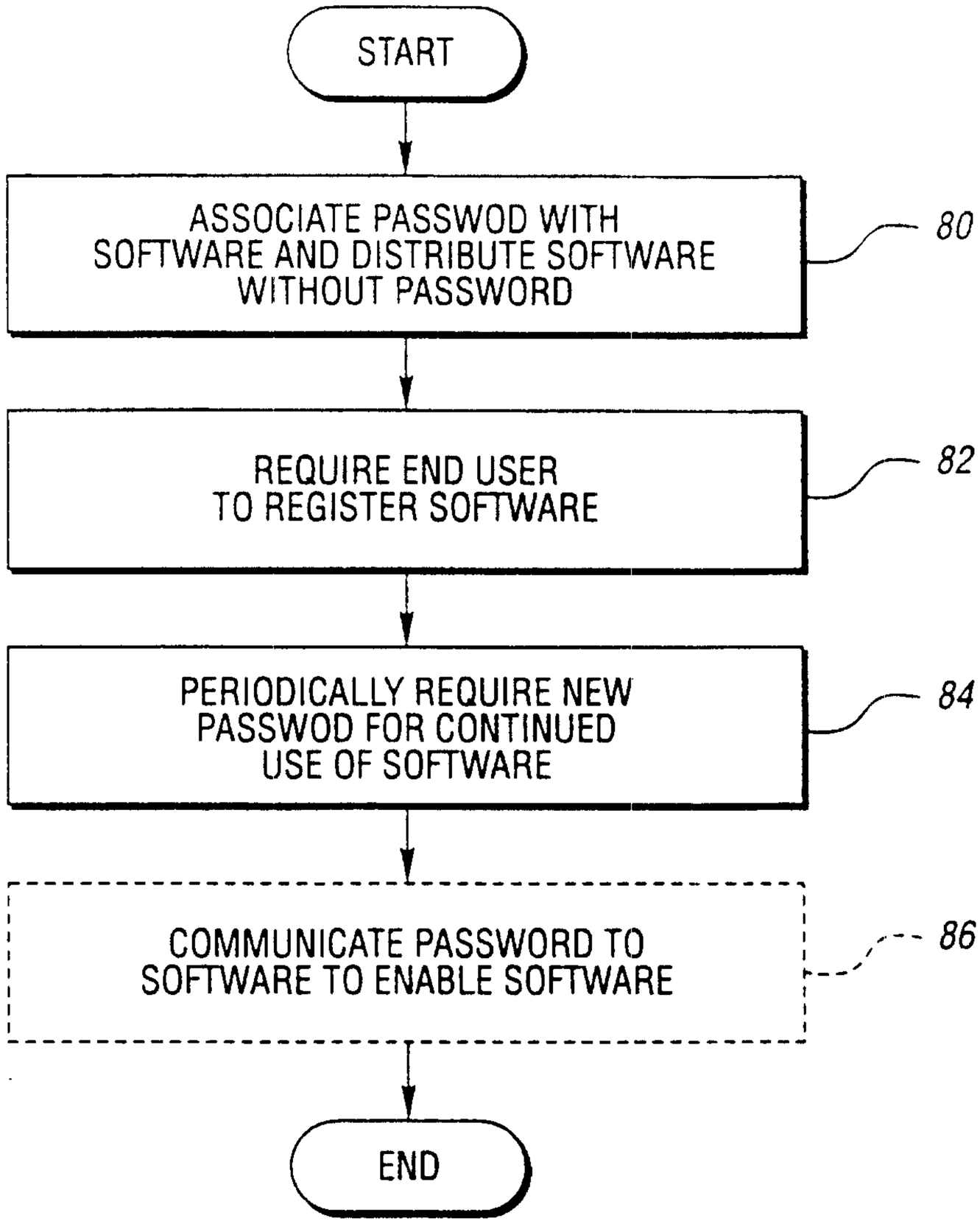

START
ASSOCIATE PASSWOD WITH SOFTWARE AND DISTRIBUTE SOFTWARE WITHOUT PASSWORD
80
REQUIRE END USER TO REGISTER SOFTWARE
82
PERIODICALLY REQUIRE NEW PASSWOD FOR CONTINUED USE OF SOFTWARE
84
COMMUNICATE PASSWORD TO SOFTWARE TO ENABLE SOFTWARE
86
END

Fig. 2

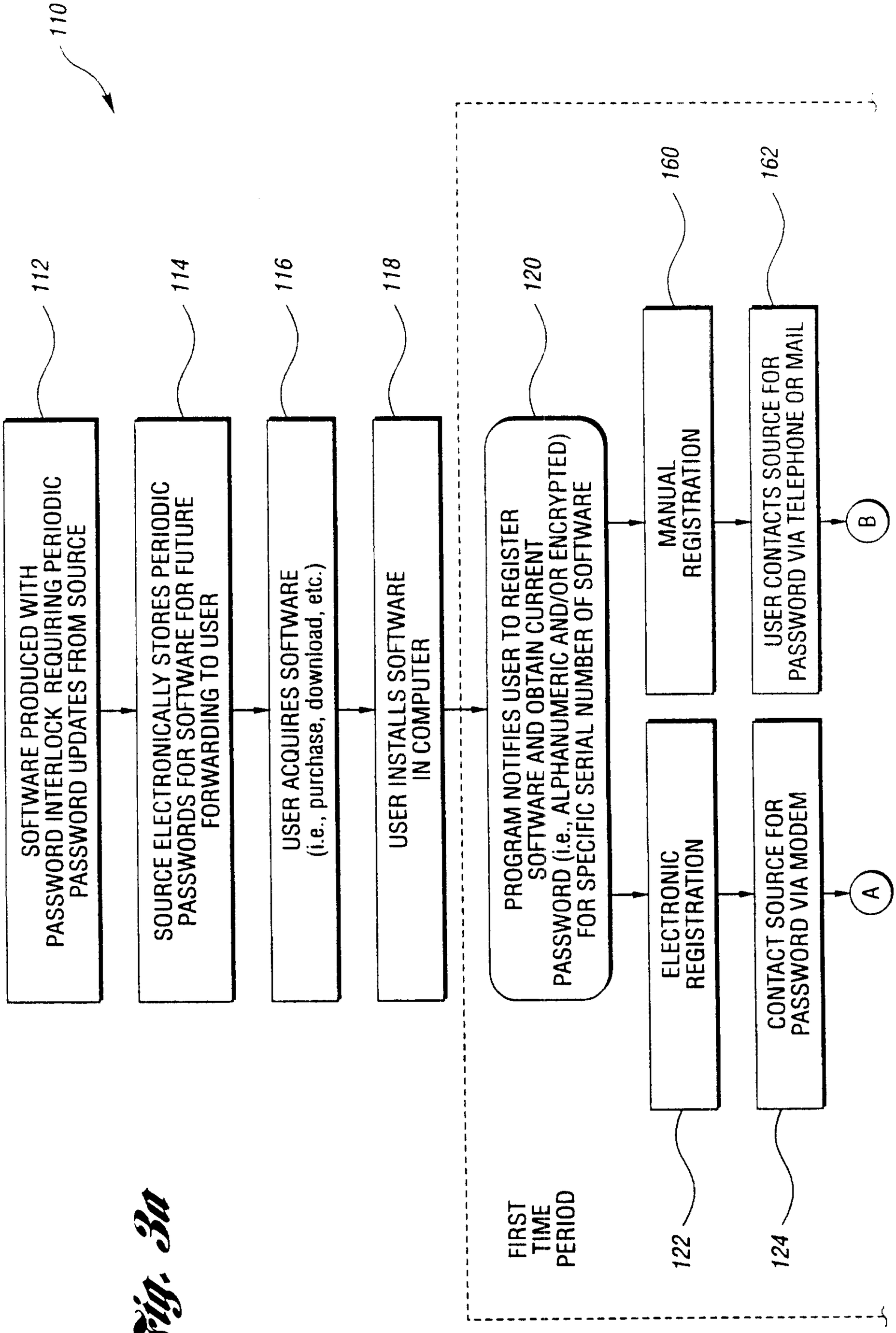

110
SOFTWARE PRODUCED WITH PASSWORD INTERLOCK REQUIRING PERIODIC PASSWORD UPDATES FROM SOURCE
112
SOURCE ELECTRONICALLY STORES PERIODIC PASSWORDS FOR SOFTWARE FOR FUTURE FORWARDING TO USER
114
USER ACQUIRES SOFTWARE (i.e., purchase, download, etc.)
116
USER INSTALLS SOFTWARE IN COMPUTER
118
PROGRAM NOTIFIES USER TO REGISTER SOFTWARE AND OBTAIN CURRENT PASSWORD (i.e., ALPHANUMERIC AND/OR ENCRYPTED) FOR SPECIFIC SERIAL NUMBER OF SOFTWARE
120
ELECTRONIC REGISTRATION
MANUAL REGISTRATION
160
CONTACT SOURCE FOR PASSWORD VIA MODEM
USER CONTACTS SOURCE FOR PASSWORD VIA TELEPHONE OR MAIL
162
A
B
FIRST TIME PERIOD
122
124

Fig. 3a

Fig. 3b

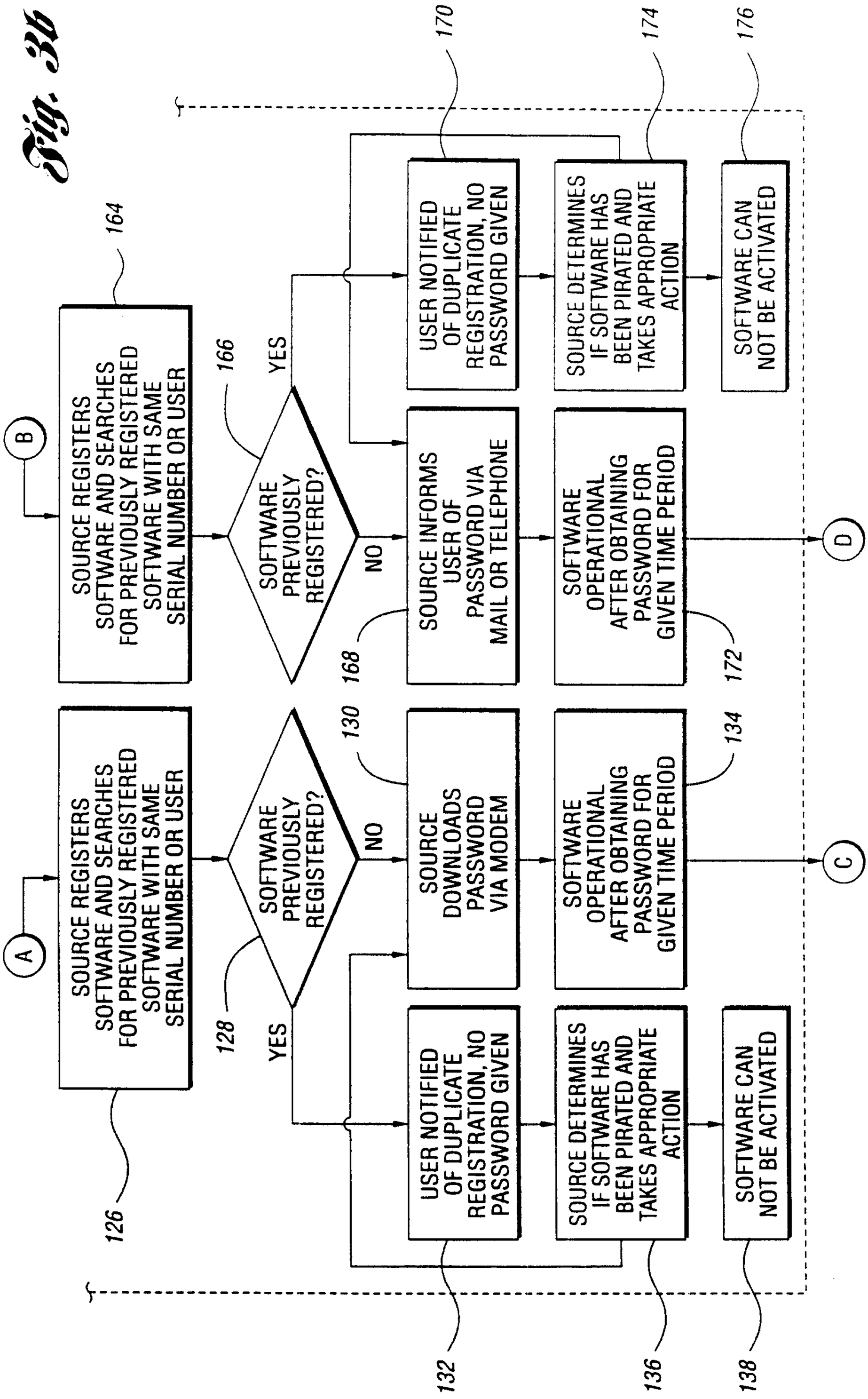

A
B
C
D
126
SOURCE REGISTERS SOFTWARE AND SEARCHES FOR PREVIOUSLY REGISTERED SOFTWARE WITH SAME SERIAL NUMBER OR USER
128
SOFTWARE PREVIOUSLY REGISTERED?
YES
NO
130
SOURCE DOWNLOADS PASSWORD VIA MODEM
132
USER NOTIFIED OF DUPLICATE REGISTRATION, NO PASSWORD GIVEN
134
SOFTWARE OPERATIONAL AFTER OBTAINING PASSWORD FOR GIVEN TIME PERIOD
136
SOURCE DETERMINES IF SOFTWARE HAS BEEN PIRATED AND TAKES APPROPRIATE ACTION
138
SOFTWARE CAN NOT BE ACTIVATED
164
SOURCE REGISTERS SOFTWARE AND SEARCHES FOR PREVIOUSLY REGISTERED SOFTWARE WITH SAME SERIAL NUMBER OR USER
166
SOFTWARE PREVIOUSLY REGISTERED?
YES
NO
168
SOURCE INFORMS USER OF PASSWORD VIA MAIL OR TELEPHONE
170
USER NOTIFIED OF DUPLICATE REGISTRATION, NO PASSWORD GIVEN
172
SOFTWARE OPERATIONAL AFTER OBTAINING PASSWORD FOR GIVEN TIME PERIOD
174
SOURCE DETERMINES IF SOFTWARE HAS BEEN PIRATED AND TAKES APPROPRIATE ACTION
176
SOFTWARE CAN NOT BE ACTIVATED

Fig. 3c

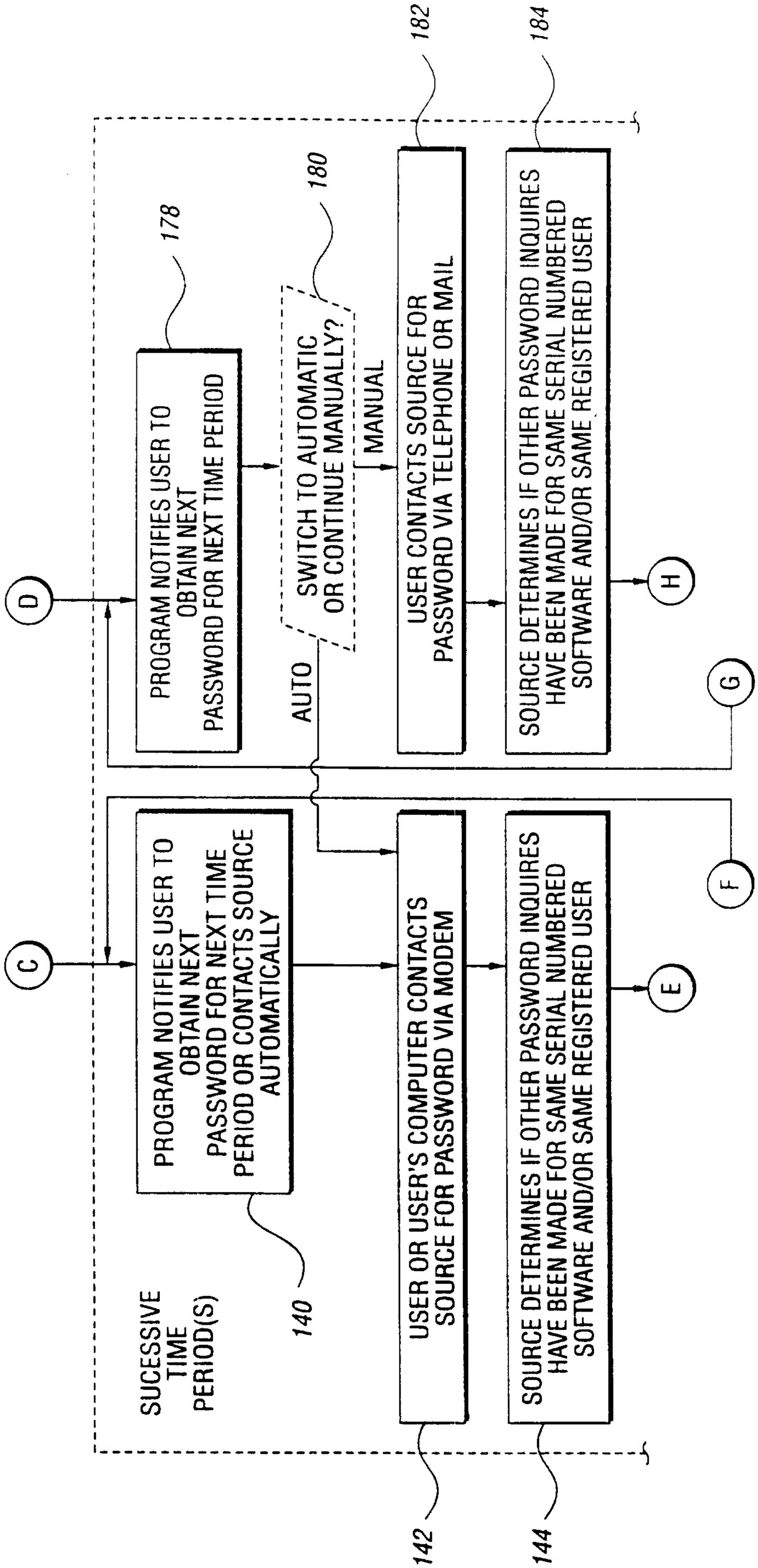
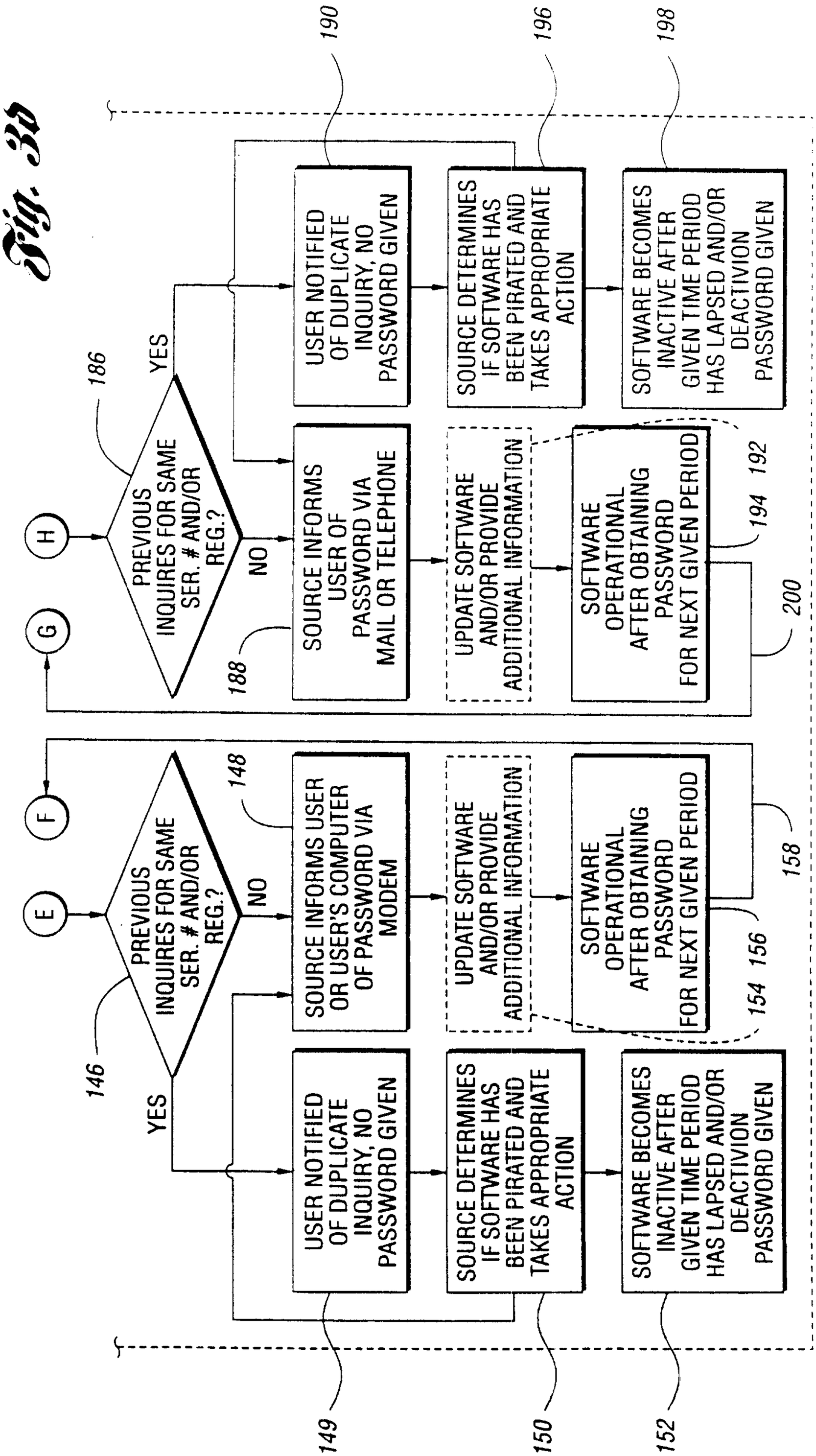
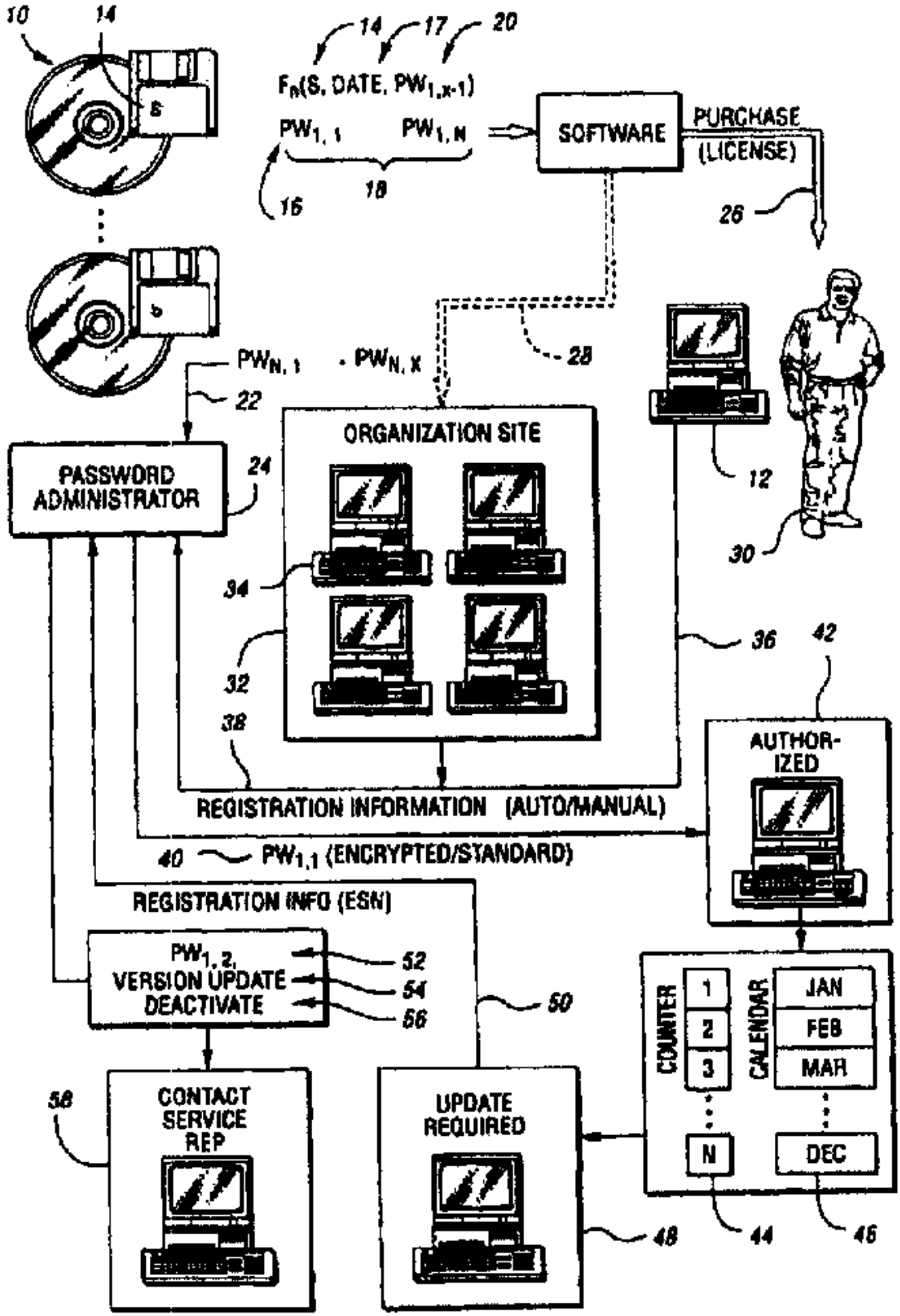

182
184
180
178
PROGRAM NOTIFIES USER TO OBTAIN NEXT PASSWORD FOR NEXT TIME PERIOD
SWITCH TO AUTOMATIC OR CONTINUE MANUALLY?
AUTO
MANUAL
USER CONTACTS SOURCE FOR PASSWORD VIA TELEPHONE OR MAIL
SOURCE DETERMINES IF OTHER PASSWORD INQUIRES HAVE BEEN MADE FOR SAME SERIAL NUMBERED SOFTWARE AND/OR SAME REGISTERED USER
D
H
G
C
F
E
PROGRAM NOTIFIES USER TO OBTAIN NEXT PASSWORD FOR NEXT TIME PERIOD OR CONTACTS SOURCE AUTOMATICALLY
USER OR USER'S COMPUTER CONTACTS SOURCE FOR PASSWORD VIA MODEM
SOURCE DETERMINES IF OTHER PASSWORD INQUIRES HAVE BEEN MADE FOR SAME SERIAL NUMBERED SOFTWARE AND/OR SAME REGISTERED USER
SUCESSIVE TIME PERIOD(S)
140
142
144

Fig. 3b


190
196
198
186
YES
H
PREVIOUS INQUIRES FOR SAME SER. # AND/OR REG.?
NO
G
188
USER NOTIFIED OF DUPLICATE INQUIRY, NO PASSWORD GIVEN
SOURCE DETERMINES IF SOFTWARE HAS BEEN PIRATED AND TAKES APPROPRIATE ACTION
SOFTWARE BECOMES INACTIVE AFTER GIVEN TIME PERIOD HAS LAPSED AND/OR DEACTIVION PASSWORD GIVEN
SOURCE INFORMS USER OF PASSWORD VIA MAIL OR TELEPHONE
UPDATE SOFTWARE AND/OR PROVIDE ADDITIONAL INFORMATION
SOFTWARE OPERATIONAL AFTER OBTAINING PASSWORD FOR NEXT GIVEN PERIOD
194
192
200
F
E
148
PREVIOUS INQUIRES FOR SAME SER. # AND/OR REG.?
NO
SOURCE INFORMS USER OR USER'S COMPUTER OF PASSWORD VIA MODEM
UPDATE SOFTWARE AND/OR PROVIDE ADDITIONAL INFORMATION
SOFTWARE OPERATIONAL AFTER OBTAINING PASSWORD FOR NEXT GIVEN PERIOD
158
154
156
146
YES
USER NOTIFIED OF DUPLICATE INQUIRY, NO PASSWORD GIVEN
SOURCE DETERMINES IF SOFTWARE HAS BEEN PIRATED AND TAKES APPROPRIATE ACTION
SOFTWARE BECOMES INACTIVE AFTER GIVEN TIME PERIOD HAS LAPSED AND/OR DEACTIVION PASSWORD GIVEN
149
150
152


10
14
14
17
20
F_N(S, DATE, $PW_{1,x-1}$)
$PW_{1,1}$
$PW_{1,N}$
16
18
SOFTWARE
PURCHASE
(LICENSE)
26
28
$PW_{N,1}$
$PW_{N,X}$
22
ORGANIZATION SITE
PASSWORD ADMINISTRATOR
24
12
30
34
32
36
42
38
AUTHOR-IZED
REGISTRATION INFORMATION (AUTO/MANUAL)
40
$PW_{1,1}$ (ENCRYPTED/STANDARD)
REGISTRATION INFO (ESN)
$PW_{1,2}$,
VERSION UPDATE
DEACTIVATE
52
54
56
50
COUNTER
1
2
3
N
CALENDAR
JAN
FEB
MAR
DEC
58
CONTACT SERVICE REP
UPDATE REQUIRED
48
44
46