



(19) **United States**  
(12) **Patent Application Publication**  
**WANG et al.**

(10) **Pub. No.: US 2015/0082453 A1**  
(43) **Pub. Date: Mar. 19, 2015**

(54) **METHOD AND APPARATUS FOR HIERARCHICAL ASSIGNMENT OF RIGHTS TO DOCUMENTS AND DOCUMENTS HAVING SUCH RIGHTS**

No. 7,162,633, which is a continuation of application No. 09/867,748, filed on May 31, 2001, now Pat. No. 6,895,503.

**Publication Classification**

(71) Applicant: **ContentGuard Holdings, Inc.**, Plano, TX (US)  
(72) Inventors: **Xin WANG**, Torrance, CA (US); **Aram NAHIDIPOUR**, Laguna Niguel, CA (US); **Michael C. RALEY**, Downey, CA (US); **Guillermo LAO**, Torrance, CA (US); **Thanh T. TA**, Huntington Beach, CA (US); **Bijan TADAYON**, Potomac, MD (US)

(51) **Int. Cl.**  
**G06F 21/10** (2006.01)  
**G06F 21/62** (2006.01)  
(52) **U.S. Cl.**  
CPC ..... **G06F 21/10** (2013.01); **G06F 21/62** (2013.01); **G06F 2221/0746** (2013.01)  
USPC ..... **726/26**

(21) Appl. No.: **14/552,048**

(57) **ABSTRACT**

(22) Filed: **Nov. 24, 2014**

A system and method for distribution of digital works in a tree-like structure of devices. A hierarchical right may include a first usage right governing a use for the digital work and a first delegation right governing distribution of the digital work to child nodes of the tree-like structure. A second usage right and/or a second delegation right may be generated based on the hierarchical right, the second usage right governing a use for the digital work and the second delegation right governing distribution of the digital work to child nodes of a first child node of the tree-like structure. The second usage right and/or the second delegation right may be assigned to a version of the digital work, and the second usage right and/or the second delegation right and the version of the digital work may be forwarded to the first child node.

**Related U.S. Application Data**

(60) Continuation of application No. 12/609,725, filed on Oct. 30, 2009, now abandoned, which is a continuation of application No. 11/584,590, filed on Oct. 23, 2006, now Pat. No. 8,869,293, which is a division of application No. 11/111,853, filed on Apr. 22, 2005, now Pat.

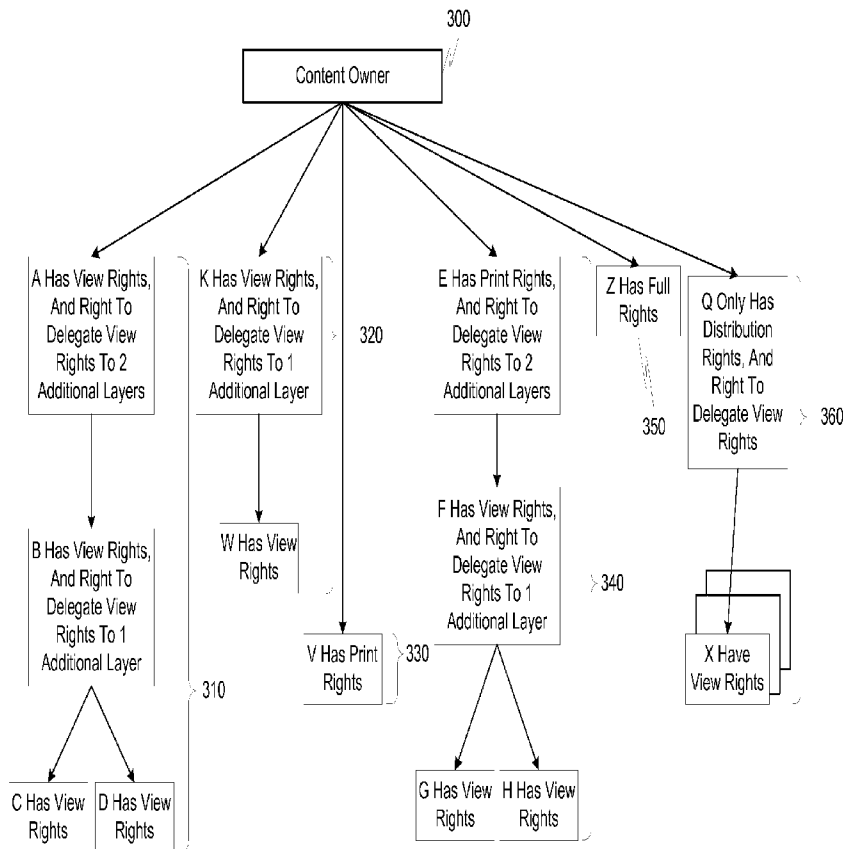


Fig. 1

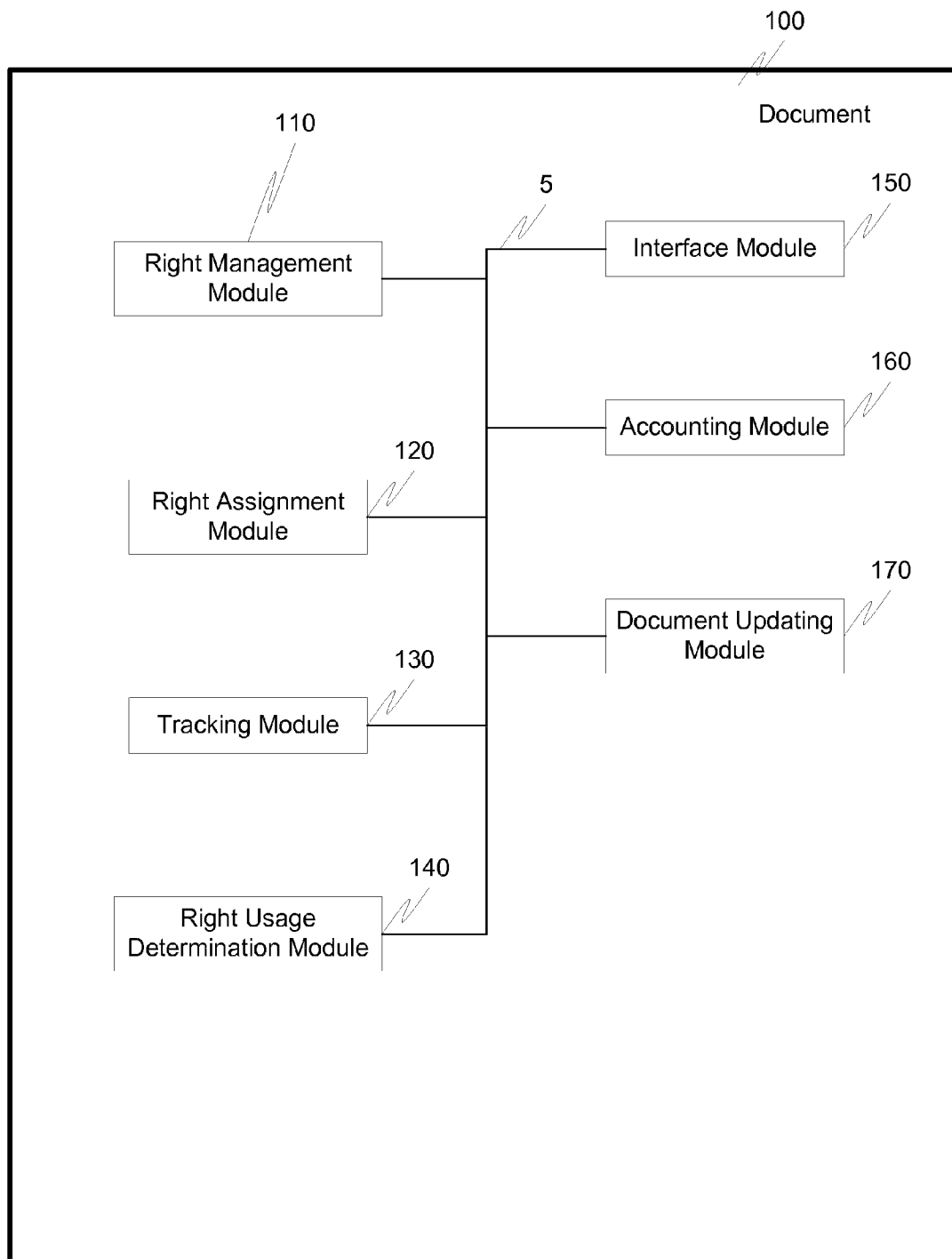


Fig. 2

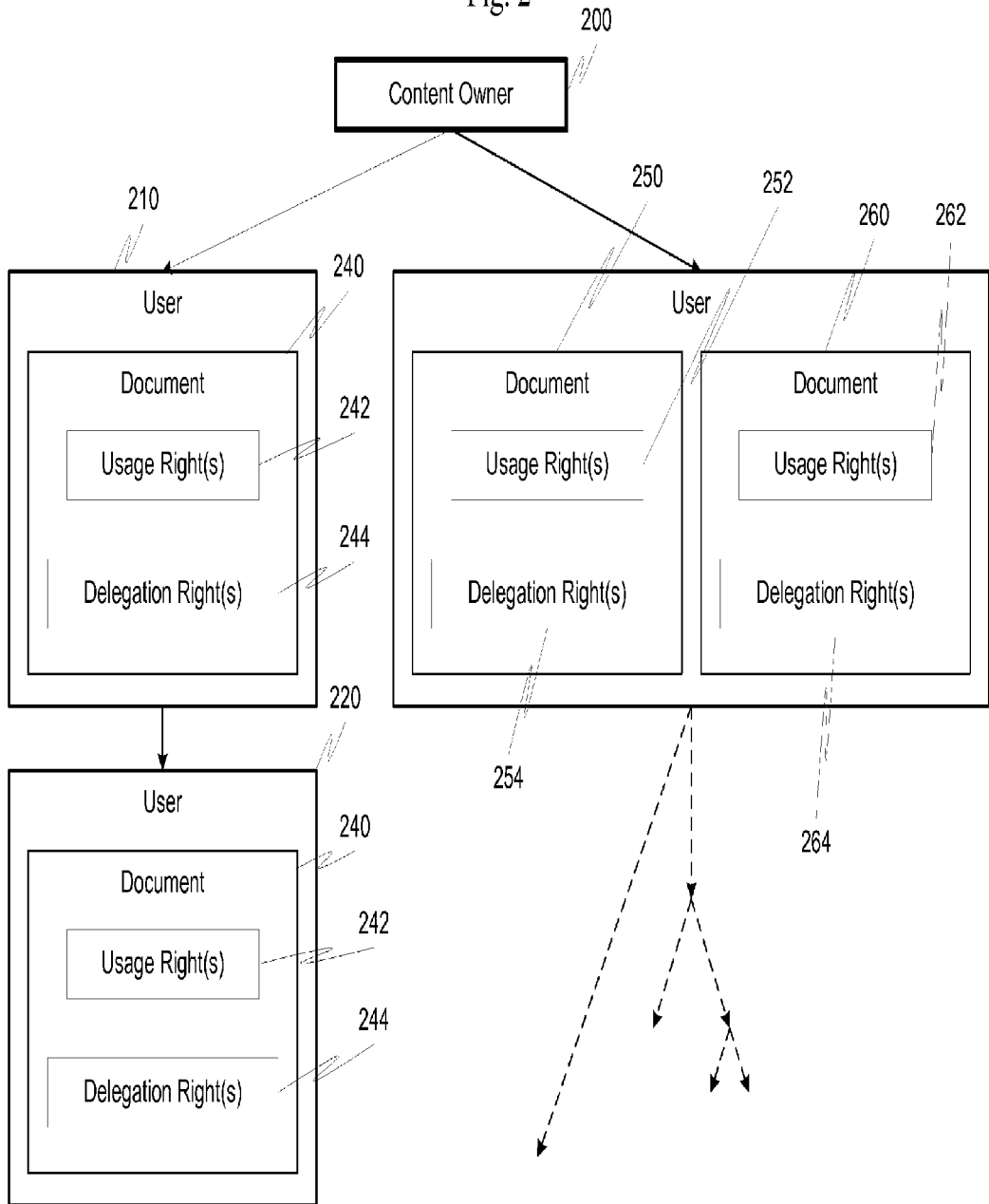


Fig. 3

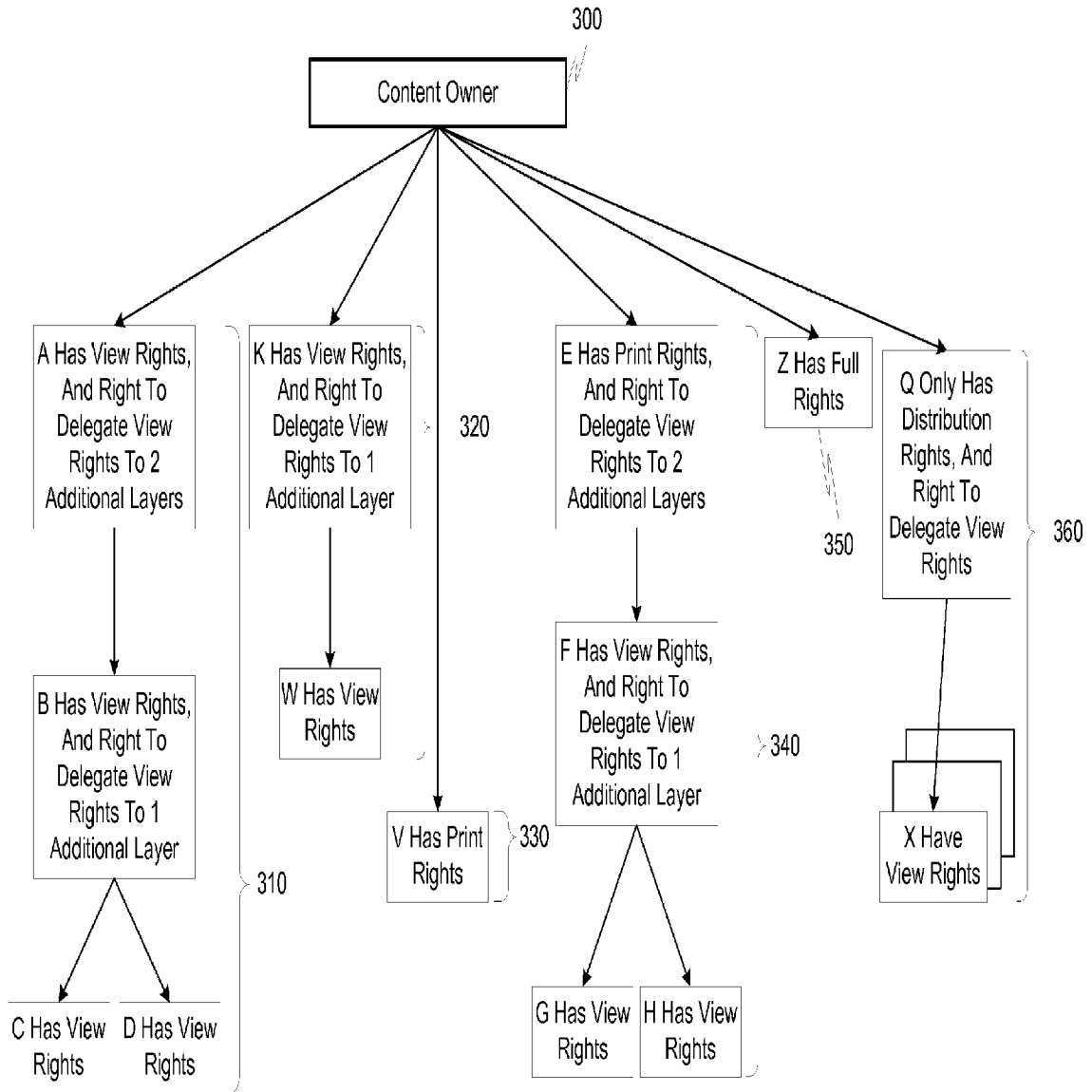


Fig. 4

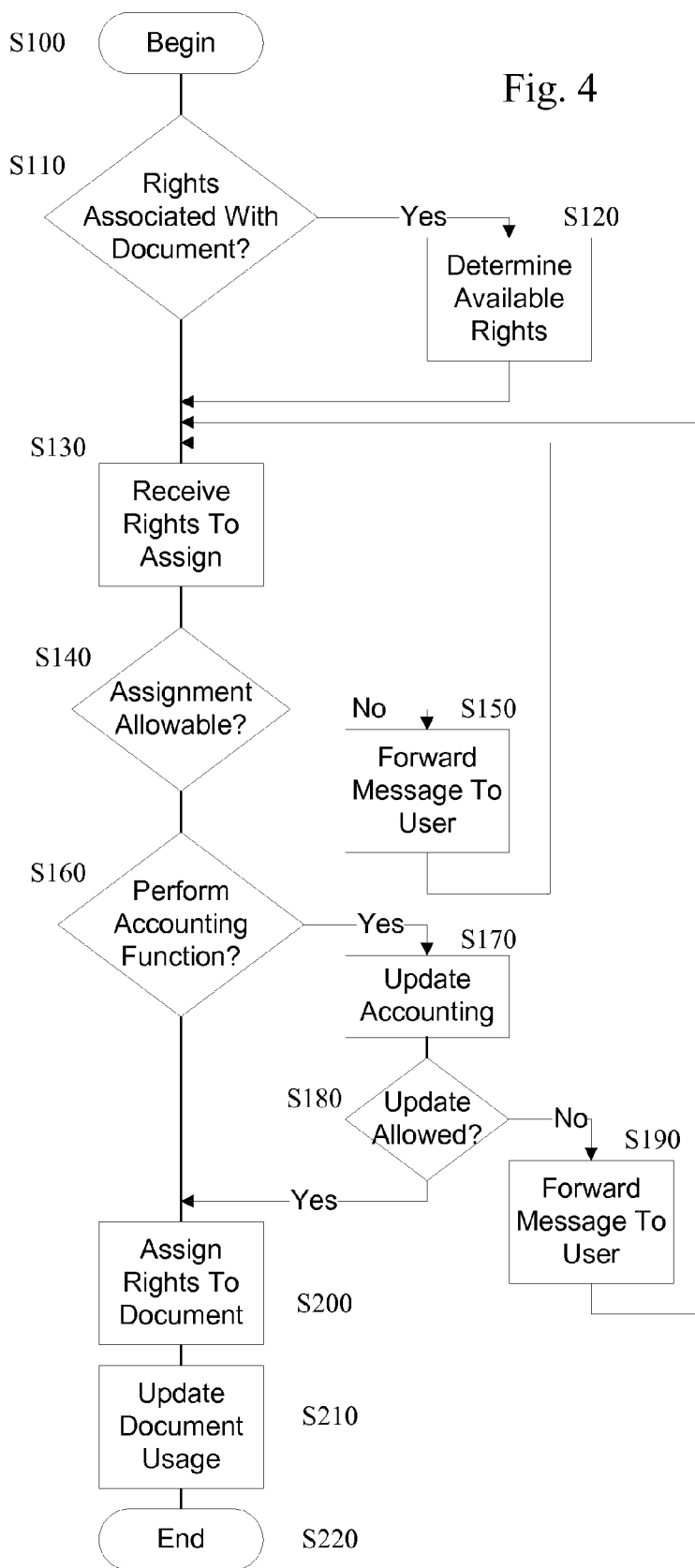
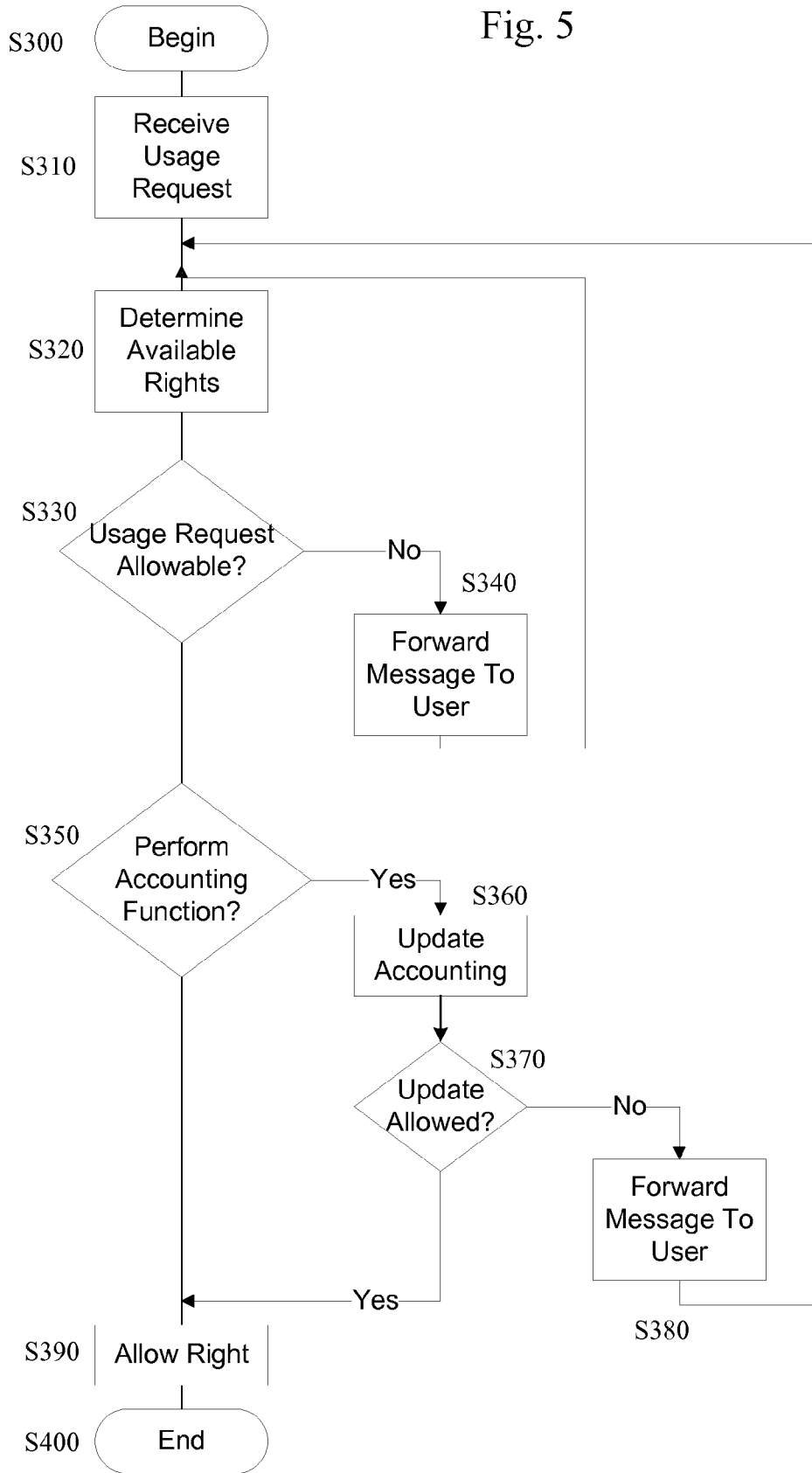


Fig. 5



**METHOD AND APPARATUS FOR  
HIERARCHICAL ASSIGNMENT OF RIGHTS  
TO DOCUMENTS AND DOCUMENTS  
HAVING SUCH RIGHTS**

**RELATED APPLICATION DATA**

**[0001]** This application is continuation application of U.S. patent application Ser. No. 12/609,725, filed Oct. 30, 2009, which is a continuation application of U.S. patent application Ser. No. 11/584,590, filed Oct. 23, 2006, now U.S. Pat. No. 8,869,293, which is a divisional application of U.S. patent application Ser. No. 11/111,853, filed Apr. 22, 2005, now U.S. Pat. No. 7,162,633, which is a continuation of U.S. patent application Ser. No. 09/867,748, filed May 31, 2001, now U.S. Pat. No. 6,895,503, the disclosures of which are incorporated herein by reference in their entirety, including related cases referenced therein.

**BACKGROUND OF THE INVENTION**

**[0002]** 1. Field of the Invention

**[0003]** In general, the systems and methods of this invention relate to documents having associated rights. In particular, the systems and methods of this invention relate to documents having a hierarchical right structure and a system and method of assigning those rights.

**[0004]** 2. Description of Related Art

**[0005]** Digital rights management (DRM) describes a process of attaching usage rights to a digital work, such as eContent, as well as managing and enforcing the same rights. In general, these digital works and eContent can include any type of content, such as music, books, multimedia presentations, eBooks, video information, or the like. In general, any information that is capable of being stored can be protected through the use of digital rights management. For example, a digital book could be accompanied by a license establishing conditions, such as viewing, printing, borrowing, or the like, governing the book's usage. These rights could then be controlled by, for example, an associated reader's software, and the allowable transactions, such as buying, printing, or the like, authorized by, for example, a clearinghouse.

**[0006]** One of the most important issues impeding the widespread distribution of digital works as documents via electronic means, such as the internet, is the lack of protection of intellectual property rights of content owners during the distribution, dissemination and use of those digital documents. Efforts to overcome this problem have been termed "intellectual property rights management" (IPRM), "digital property rights management" (DPRM), "intellectual property management" (IPM), "rights management" (RM) and "electronic copyright management" (ECM), which can be collectively referred to as Digital Rights Management (DRM). There are a number of issues in Digital Rights Management including authentication, authorization, accounting, payment and financial clearing, rights specifications, rights verification, rights enforcement, document protection, and the like.

**[0007]** In the world of printed documents, a work created by an author is typically provided to a publisher, which formats and prints numerous copies of the work. The copies are then distributed to bookstores or other retail outlets, from which the copies are purchased by end users. While the low quality of physical copying, and the high cost of distributing printed material have served as deterrents to unauthorized copying of most printed documents, digital documents allow

easy copying, modification, and redistribution if they are unprotected. Accordingly, digital rights management allows the protecting of digital documents to, for example, complicate copying, modifying and redistributing.

**[0008]** Similarly, it has been widely recognized that it is difficult to prevent, or even deter, individuals from making unauthorized distributions of electronic documents within current general-purpose computer and communication systems such as personal computers, workstations, and other devices connected via a distributed network, such as a local area network, an intranet and the Internet. Many attempts to provide hardware-based solutions to prevent unauthorized copying have proven to be unsuccessful. Furthermore, the proliferation of broadband communications technologies and the development of the "national information infrastructure" (NII) will likely make it even more convenient to distribute large documents electronically, thus removing most deterrents to any unauthorized distribution of documents. Therefore, digital rights management technologies provide one method of protecting digital documents distributed electronically.

**[0009]** Two basic schemes have been employed to attempt to solve the document protection problem. In particular, the two basic schemes are secure containers and trusted systems. A secure container, or simply an encrypted document, offers one method of keeping document contents encrypted until a set of authorization parameters are satisfied. After the various parameters are verified, for example, by the document provider, the document can be released to a user. Commercial products such as IBM's Cryptolopes® and InterTrusts Digi-boxes® fall into this category. While the secure container approach provides a solution to protect the document during delivery over unsecure channels, it does not provide any mechanism to prevent legitimate users from obtaining the unencrypted document, and then, for example, using and redistributing the unprotected document without authorization.

**[0010]** In the trusted system approach, the entire system that handles, for example, the distribution and viewing of a document, is responsible for preventing unauthorized use. Building such a trusted system usually entails introducing new hardware such as a secure processor, a secure storage, and secure rendering devices. The trusted system also requires that all software applications that run on the system be certificate to be trusted.

**[0011]** U.S. Pat. Nos. 5,530,235, 5,634,012, 5,715,403, 5,638,443 and 5,629,980, which are incorporated herein by reference in their entirety, generally discuss digital rights management. In general, an author creates a document and forwards it to a distributor for distribution. Typically, the author is the creator of the content, however, the author can be any one of the creator, the owner, the editor, or any other entity controlling a portion of content, or an agent of one of those entities. The author may distribute documents directly, without involving a secondary party such as a distributor. Therefore, the author and the distributor may be the same entity. A distributor can distribute documents to one or more users, for example, upon request. In a typical electronic distribution model, the content can be distributed as a document in encrypted form. For example, a distributor can encrypt the content with a random key, having encrypted the random key with a public key corresponding to one or more users. Thus, the encrypted document can be customized solely for a par-

particular user. The user is then able to use the private key to unencrypt the public key and use the public key to unencrypt and view the document.

**[0012]** Payment for the document can be passed from a user to a distributor by way of a clearinghouse which can collect requests from one or more users who wish to view a particular document. The clearinghouse can also collect payment information, such as debit transactions, credit transactions, credit card transactions, or other known electronic payment schemes and forward the collected payments to a distributor. Furthermore, the clearinghouse may retain a share of the payment as a fee for these services. The distributor may also retain a portion of the payment from the clearinghouse to cover, for example, distribution services and royalties due an author.

**[0013]** Each time the user requests a document, an accounting message can be sent to an accounting server that can, for example, ensure that each request by the user matches a document sent by the distributor. Additionally, the accounting information can be received by an accounting server and distributor to reconcile any inconsistencies.

#### SUMMARY OF THE INVENTION

**[0014]** Expanding on the above concepts, it may be beneficial to have hierarchical rights assigned to one or more digital works. For example, a first user can be granted the right to use a document which may, for example, involve a fee, and in addition, the user has the right to transfer the same or different rights to a second user. Expanding further, the second user may also have the right to assign specified rights to a third user. In general, the hierarchical rights can be distributed in steps similar to a pyramid scheme or tree structure, and the assigned rights in each branch of the structure could be the same or different from those in any other branch. In general, the closer the user would be to the document author, the higher the authority and more rights the user would have access to. However, depending on the particular implementation, the content owner may want to deviate from the general rule by limiting the power or rights of one or more of the nodes near the root. For example, a publisher may want a distributor to distribute a book and grant the rights to read the book to an end user for a fee. However, the publisher may not want to provide the distributor with the right to read the book, unless, for example, the distributor also pays for a view right comparable to the end user. This hierarchical rights scheme can be used in the distribution chain from content owners to distributors, to secondary distributors, to end users, or the like. In general, hierarchical rights can be associated with any information by anyone or any entity.

**[0015]** In an exemplary aspect of the invention, there is provided a self-contained device for protecting content, the content having usage rights associated therewith, including a usage rights portion having usage rights that control the use of the content; a rights management module that authorizes a request to access to the content based on the usage rights; a rights assignment module that generates and updates the usage rights based on the content access; and an interface module that allows accessing of the content.

**[0016]** Further aspects of the present invention relate to digital rights management. In particular, an exemplary embodiment of the invention provides for the management of hierarchical digital rights.

**[0017]** A further aspect of the invention provides users the ability to assign hierarchical rights, and the management of information having the associated hierarchical rights.

**[0018]** An additional aspect of the invention relates to determining a user's usage rights based on the hierarchical rights associated with the document.

**[0019]** An additional aspect of the invention relates to information having one or more associated hierarchical rights.

**[0020]** These and other features and advantages of this invention are described in or are apparent from the following detailed description of the embodiments.

#### BRIEF DESCRIPTION OF THE DRAWINGS

**[0021]** The embodiments of the invention will be described in detail, with reference to the following figures wherein:

**[0022]** FIG. 1 is functional block diagram illustrating an exemplary document according to this invention;

**[0023]** FIG. 2 is a diagram illustrating an exemplary embodiment of the distribution of documents having associated hierarchical rights according to this invention;

**[0024]** FIG. 3 is a second diagram illustrating an exemplary embodiment of the distribution of documents having associated hierarchical rights according to this invention;

**[0025]** FIG. 4 is a flow chart outlining an exemplary method of associating rights with a document according to this invention; and

**[0026]** FIG. 5 is a flow chart outlining an exemplary method of using hierarchical rights according to this invention.

#### DETAILED DESCRIPTION OF THE INVENTION

**[0027]** The assignment of hierarchical rights allows, for example, even greater control by an author over one or more documents. This hierarchical rights assignment further allows for greater control throughout the document distribution chain extending to, for example, distributors, secondary distributors, users, or the like. Therefore, a graphical representation of the rights associated with the document could appear as a series of interconnected nodes each having an associated portion of rights.

**[0028]** An exemplary embodiment of the systems and methods of this invention can also include a rights-on-rights scheme in which, for example, a counter or other system manages the various layers, nodes and branches to regulate, for example, the rights to change, edit, assign, revoke, transfer other rights, or the like, to one or more additional layers. Since rights can be treated as an object class, for example using XML, rights can include themselves and thus refer to itself as, for example, an iteration. For example, a user can transfer the rights-on-rights for a maximum of two layers of the right assignment tree which could, for example, further limit and control the overall distribution of both the rights and the document. Therefore, the rights of the user may be different from the rights a user can assign or transfer in the hierarchical structure.

**[0029]** Additionally, for example, the rights to change, edit, copy, sign, or the like, can be passed on from the owner to the user. Associated with one or more of these rights can be document tracking actions. For example, using a digital signature, a document can manage and record its path of distribution, recording each user's interactivity with the document, including, for example, any assignment and/or distribution action, or any other information that may be relevant. There-



fore, it is possible that a document will have associated therewith multiple signatures that represent, for example, a “snapshot” of the document as it was available to that particular user. For example, a second user can add, subtract, modify, edit, or the like, the content of a document which has already been signed by a first user. These modifications by the second user are then “signed,” recording that user’s interactions with the document. Both versions of the document then can be stored, for example, in a database, for reference, accounting, profiling, or the like.

**[0030]** Additionally, the right to use a document can be content-based or role-based, as is described in U.S. Pat. No. 6,976,009, entitled “Method and Apparatus for Assigning Conditional or Consequential Rights to Documents and Documents Having Such Rights,” incorporated herein by reference in its entirety. For example, the president of a company may want to be the only one authorized to use a particular document. If the president of the company changes, the new president can automatically become the right holder, assuming the president can verify, for example, their position using, for example, biometrics, a smart card, an identification card, or comparable identification device or scheme. This allows the assignment of rights to be separate from the assignment of the position.

**[0031]** Similarly, the systems and methods of this invention can be used in conjunction with rights editing tools and templates such as those discussed in U.S. Provisional Patent Application Ser. No. 60/261,753, entitled “Method and Apparatus for Editing and Specifying the Rights and Conditions Associated with Documents or Digital Contents,” incorporated herein by reference in its entirety. For example, rights can be assigned through the use of templates that can aid in the assignment of rights to one or more classes of users based on, for example, a job position, a geographic location, a profile, an identifier, or the like.

**[0032]** Furthermore, this concept extends itself into the medical field. For example, where medical records are used by a doctor, the medical records can contain usage rights for a certain class or field of individuals. This can, for example, satisfy both the concerns regarding the patient’s safety and the patient’s privacy by limiting access to one or more documents.

**[0033]** Additionally, for example, the role-based or content-based rights can be used for access to movies with, for example, adult content to restrict a particular class of individuals from viewing the content. An attempt to access the restricted content can be recorded and, for example, reported to the proper party. Furthermore, the parent can be viewed as a node in the hierarchical right assignment structure such that the parent can obtain a template or toolkit for right assignment, right modification and right customization, and then transfer the rights to one or more children. The parent could then update and modify, for example using an age-based right assignment scheme with or without corresponding templates, the child’s rights as, for example, the child grows.

**[0034]** FIG. 1 illustrates an exemplary document 100. The exemplary document 100 comprises a right management module 110, a right assignment module 120, a tracking module 130, a right usage determination module 140, an interface module 150, an accounting module 160, and a document updating module 170 interconnected by links 5. The document 100 can also be connected to a distributed network (not shown) which may or may not also be connected to one or more other documents, account processing systems, rights

management systems, or other distributed networks, as well as one or more input devices and display devices (not shown).

**[0035]** While the exemplary embodiment illustrated in FIG. 1 shows the document 100 and associated components collocated, it is to be appreciated that the various components of the document 100 can be located at distant portions of a distributed network, such as a local area network, a wide area network, an intranet and/or the internet, or within a dedicated document or document system. Thus, it should be appreciated that the components of the document 100 can be combined into one device or collocated on a particular node of distributed network. Furthermore, it should be appreciated that for ease of illustration, the various functional components of the document 100 have been divided as illustrated in FIG. 1. However, any of the functional components illustrated in FIG. 1 can be combined or further partitioned without affecting the operation of the system. As will be appreciated from the following description, and for reasons of computation efficiency, the components of the document can be arranged at any location within a distributed network without effecting the operation of the system. Furthermore, it is to be appreciated that the term module as used herein includes any hardware and/or software that provide the functionality as discussed herein. Likewise, the document 100 can be self contained, such as an E-Book, and comprise any necessary controllers, memory, and/or I/O interfaces that may be necessary given the particular embodiment and/or implementation of the document 100. Additionally, the document 100 can be any information to which hierarchical rights are associated.

**[0036]** Furthermore, the links 5 can be a wired or wireless link or any other known or later developed element(s) that is capable of supplying and communicating data to and from the connected elements. Additionally, the input devices can include, for example, a keyboard, a mouse, a speech to text converter, a stylus, a mouse, or the like. In general, the input device can be any device capable of communicating information to the document 100. Furthermore, the display device can be a computer monitor, a display on a PDA, an E-Book, or any other device capable of displaying information to one or more users.

**[0037]** In operation, a user, such as a document creator, associates rights with the document 100. In particular, via the interface module 150 and one or more of an input device and display device, a user inputs rights to associate with the document 100. In cooperation with the right management module 110 and the right assignment module 120, the rights are associated with the document 100. In this exemplary embodiment, it is assumed that the content owner, or author, is not responsible for any type of accounting procedure, e.g., crediting or debiting, associated with assigning rights to the document 100. However, it is to be appreciated that for a particular embodiment, it may be desirable to credit or debit a user based on the user associating rights with a document 100. However, as previously discussed, the association and assignment of rights can be performed by, for example, one or more external rights assignment system that associates one or more hierarchical rights with the document 100.

**[0038]** For example, an employee of a newspaper may be hired to write an article on a particular topic. On completion of the article, the journalist could assign view, edit and distribution rights to the publisher. Then, for example, upon assignment of these rights and distribution of the document to the publisher, the author could be credited for their work.

[0039] Alternatively, a user may receive a document 100 and wish to modify the rights associated with that document. Thus, the right management module 110 determines the available assignable rights associated with the document 100. Then, via the interface module 150, and one or more of the input and display devices, the rights that are to be assigned by the user are received. Next, a determination is made by the right management module 110 as to whether the assignment is allowable. For example, the rights associated with the document 100 can restrict based on, for example, the user, the distribution history, another users' interaction with the document, or the like, whether the current user's request to modify the associated rights is allowable. If the right assignment module 120 determines that the user's request is not allowed, a message can be forwarded to the user indicating the like. However, if the assignment is determined allowable by the right assignment module 120, an optional determination can be made by the accounting module 160 as to whether any accounting functions need be performed. If accounting functions need be performed, the accounting module 160 can perform any necessary crediting and/or debiting as appropriate. For example, the accounting module 160 can contact an accounting system (not shown) which could authorize the user's transaction. Alternatively, for example, the accounting module 160 can interface with a user, for example, via a smart card, a credit card interface, or the like, and correctly debit and/or credit a user's account. However, it is to be appreciated that the accounting module 160 need not perform any function whatsoever if the rights associated with the document so specify, for example, in a document that is available for inspection and comment. Furthermore, it is appreciated that the accounting module 160 need not perform the accounting functions in real time, but can perform them on an as needed basis, in a batch, or the like. For example, if the document 100 is an E-Book, the accounting module 160 could debit every user that views the contents of the E-Book as it is passed around. Then, upon return of the E-Book to, for example, a library, the accounting module 160 can synchronize with, for example, an accounting system that performs any necessary accounting functions.

[0040] In general, if the accounting is required and is successful, the rights chosen by the user are associated with the document. However, if, for example, the accounting function is not allowed, a message can be forwarded to a user indicating that there is a problem.

[0041] After the association of the updated rights with the document by the document updating module 170, the tracking module 130 can optionally maintain a history, for example, with the use of a digital signature, of the rights updates, or any other updates, such as edits, or the like, made by this particular user. This information can then be associated with the document with the cooperation of the tracking module 130.

[0042] In use, a user receives one or more documents 100 for viewing, editing, modifying, updating, distributing, or the like. Upon receipt of the document 100, the right management module 110 determines the rights available to that user. If the user's usage request corresponds to the rights available to that user, the right usage determination module 140, in cooperation with the right management module 110, allows the user's request. Furthermore, based on the user's usage request, the document updating module 170 can allow the user to, for example, edit, update, or otherwise modify the document 110.

[0043] However, if the user's usage request does not correspond to the usage rights available to that user, a message can be forwarded to the user requesting, for example, an alternative usage request be entered, or denying access to the document. Optionally, the tracking module 130 can also maintain a log of user access attempts and rights requests for the document.

[0044] FIG. 2 illustrates an exemplary tree of documents having associated hierarchical rights at each node of the tree. In particular, a user, such as a content owner 200, distributes one or more documents to users 210, 220 and 230. The documents 240, 250 and 260, respectively, comprise usage rights and delegation rights. The usage rights govern the extent to which the user can access the particular document. The delegation rights govern the ability for the user to assign rights, govern further distribution the document, and regulate the number of users to which the document can be distributed. In this exemplary embodiment, the content owner 200 distributes a first document to the user 210 who then distributes the document 240 to user 220. Additionally, the content owner distributes documents 250 and 260 to the user 230.

[0045] In this exemplary embodiment, the user 210, based on the delegation rights 244, has the ability to further distribute the rights to one or more additional users. In this example, the user 210 distributes the document 240 to user 220. Therefore, the user 220 will have a version of the document 240 that has associated usage rights 242 and delegation rights 244. These usage rights 242 and delegation rights 244 may be a subset of, or may comprise additional rights not present in the usage rights and/or delegation rights granted to the user 210.

[0046] User 230 possesses two documents 250 and 260. The document 250 comprises associated usage rights 252 and delegation rights 254. Likewise, the document 260 comprises usage rights 262 and delegation rights 264. The user 230 then has the ability, based on the available rights, to modify one or more of the usage rights and/or delegation rights and forward them to one or more additional parties. In this manner, a hierarchical structure of usage rights and delegation rights extends from the content owner in a tree-like structure through one or more users.

[0047] FIG. 3 illustrates various exemplary embodiments of usage rights and delegation rights associated with an exemplary document. In particular, content owner 300 distributes six documents 310-360. Document 310 allows user A to have view rights and the right to delegate view rights to two additional layers. User B has view rights and the right to delegate view rights to two users on one additional layer. Users C and D both have view rights granted by user B, but no delegation rights.

[0048] Document 320 allows user K to have view rights and the right to delegate view rights to one additional layer. Upon granting of these view rights, user W has view rights to the document.

[0049] For document 330, the content owner 300 granted user V a print usage right, and no delegation rights. Thus, the document 330 cannot be further delegated and may, for example, become inaccessible after V has exercised the print right.

[0050] Document 340 provides user E print rights, and the right to delegate view rights to two additional layers. Upon delegation of these rights, user F has view rights and the right to delegate view rights to two additional users on one further layer. Upon delegation of these rights, users G and H would both be able to view the document 340.

[0051] For document 350, the content owner 300 has provided user Z with full rights. Thus, user Z has the ability to assign any delegation and/or usage rights to the document 350. Thus, the document 350 can be further distributed and/or used based on the updated rights based on the rights user Z associates with the document.

[0052] Document 360 allows user Q to have distribution rights to unlimited users, and the ability to delegate view rights to each of these users. Thus, user Q can delegate view rights to one or more users X who can view the document, for example, on a pay-per-view basis.

[0053] While the exemplary embodiment illustrated in FIG. 3 shows specific usage rights and delegation rights, it is to be appreciated that any usage rights, such as editing, modifying, updating, copying, viewing, or the like, can be associated with one or more documents. Furthermore, it is to be appreciated that the rights associated with a document can include accounting rights, conditional or consequential rights, return rights, tracking rights, signature requirement rights, or the like. In general, the rights associated with a document can be any right granting or restricting access to one or more users, and can encompass at least all the rights specified in the XrML™ rights language and the associated usage rights and grammar.

[0054] FIG. 4 illustrates an exemplary embodiment of a method for associating rights with a document. In particular, control begins in step S100 and continues to step S110. In step S110, a determination is made whether rights are already associated with the document. If rights are associated with the document, control continues to step S120 where the usage and delegation rights available to the particular user are determined. Control then continues to step S130.

[0055] In step S130, the rights one or more users desire to have associated with the document are received. Next, in step S140, it is determined whether the assignment of these rights is allowable. If the assignment is allowable, control continues to step S160. Otherwise, control jumps to step S150. In step S150, a message can be forwarded to the user indicating the assignment is not available. Control then optionally continues back to step S130.

[0056] In step S160, an optional accounting function can be performed. If accounting is necessary, control continues to step S170. Otherwise, control jumps to step S200.

[0057] In step S170, any necessary accounting functions are attempted. Then, in step S180, a determination is made whether the accounting, e.g., any crediting and/or debiting, is allowed. If the accounting functions are successful, control jumps to step S200. Otherwise, control continues to step S190 where a message can be forwarded to the user and control returns back to step S130.

[0058] In step S200, the right as chosen by the one or more users are associated with the document. Then, in step S210, the document can be updated reflecting, for example, which usage rights were used, the effect of any of these usage rights, a signature of the user and, for example, any modifications to or assignment of delegation rights. Control then continues to step S200 where the control sequence ends.

[0059] FIG. 5 illustrates an exemplary method of using one or more of usage rights and delegation rights. In particular, control begins in step S300 and continues to step S310. In step S310, the usage request is received. This usage request can be one or more of a usage right requests or a delegation right request. Then, in step S320, the rights available to the particular user are determined. For example, as previously dis-

cussed, the rights can be based on the identity of the user, the position of the user, a status of the user, or the like. Control then continues to step S330.

[0060] In step S330, a determination is made whether the user's right request is allowable. If the usage request is not allowable, control continues to step S340. Otherwise, control jumps to step S350.

[0061] In step S340, a message can be forwarded to the user indicating the requested usage, i.e., the usage or the delegation request, is not allowable. Control then optionally jumps back to step S320.

[0062] In step S350, a determination is made whether an accounting function is to be performed based on, for example, the usage request or the delegation request. If accounting functions are to be performed, control continues to step S360. Otherwise, control jumps to step S390.

[0063] In step S360, the accounting functions are attempted. Then, in step S370, a determination is made whether the accounting functions are allowed. If the accounting functions are allowed, control continues to step S380. Otherwise, control jumps to step S390.

[0064] In step S380, a message can be forwarded to the user indicating, for example, that the crediting and/or debiting authorization failed. Control then can, for example, jump back to step S320 or, optionally, the user can be prompted for additional accounting information.

[0065] In step S390, one or more of the usage rights or delegation rights is allowed. Control then continues to step S400, where the control sequence ends.

[0066] As illustrated in FIG. 1, the document can be implemented either on a single programmed general purpose computer or a separate programmed general purpose computer. However, the document can also be implemented on a special purpose computer, a programmed microprocessor or microcontroller and peripheral integrated circuit element, an ASIC or other integrated circuit, a digital signal processor, a hard-wired electronic or logic circuit such as a discrete element circuit, a programmable logic device such as a PLD, PLA, FPGA, PAL, or the like. In general, any device capable of implementing a finite state machine that is in turn capable of implementing the flowcharts in FIGS. 4-5 can be used to implement the document and hierarchical rights management system according to this invention.

[0067] Furthermore, the disclosed method may be readily implemented in software using object or object-oriented software development environments that provide portable source code that can be used on a variety of computer or workstation hardware platforms. Alternatively, the disclosed document and right management system may be implemented partially or fully in hardware using standard logic circuits or VLSI design. Whether hardware or software is used to implement the systems and methods in accordance with this invention is dependent on the speed and/or efficiency requirements of the system, the particular function, and a particular software and/or hardware systems or microprocessor or microcomputer systems being utilized. The document and rights management systems illustrated herein, however, can be readily implemented in hardware and/or software using any known or later-developed systems or structures, devices and/or software by those of ordinary skill in the applicable art from the functional description provided herein and with a general basic knowledge of the computer arts.

[0068] Moreover, the disclosed methods may be readily implemented as software executed on a programmed general

purpose computer, a special purpose computer, a microprocessor or the like. In these instances, the methods and systems of this invention can be implemented as a program embedded in a personal computer, an E-Book, a secure container, or the like, such as a Java® or CGI script, as an XML document, as a resource residing on a server or graphics workstation, as a routine embedded in a dedicated electronic document, an electronic document viewer, or the like. The document and rights management system can also be implemented by physically incorporating the systems and methods into a hardware and/or software system, such as the hardware and software systems of a computer or dedicated electronic document.

[0069] It is, therefore, apparent that there has been provided, in accordance with the present invention, systems and methods for managing electronic documents. While this invention has been described in conjunction with a number of embodiments, it is evident that many alternatives, modifications and variations would be or are apparent to those of ordinary skill in the applicable art. Accordingly, applicants intend to embrace all such alternatives, modifications and variations that are within the spirit and scope of this invention.

What is claimed is:

1. A computer-implemented method executed by one or more computing devices for distribution of digital works in a tree-like structure comprising nodes of devices, the method comprising:

assigning, by at least one of the one or more computing devices, a hierarchical right to a digital work at a root node, the hierarchical right comprising a first usage right governing a use for the digital work and a first delegation right governing distribution of the digital work to child nodes of the tree-like structure;

generating, by at least one of the one or more computing devices, at least one of a second usage right and a second delegation right based on the hierarchical right, the second usage right governing a use for the digital work and the second delegation right governing distribution of the digital work to child nodes of a first child node of the tree-like structure;

assigning, by at least one of the one or more computing devices, the at least one of the second usage right and the second delegation right to a version of the digital work; and

transmitting, by at least one of the one or more computing devices, the at least one of the second usage right and the second delegation right and the version of the digital work to the first child node.

2. An apparatus for distribution of digital works in a tree-like structure comprising nodes of devices, the apparatus comprising:

one or more processors; and  
one or more memories operatively coupled to at least one of the one or more processors and having instructions stored thereon that, when executed by at least one of the one or more processors, cause at least one of the one or more processors to:

assign a hierarchical right to a digital work at a root node, the hierarchical right comprising a first usage right governing a use for the digital work and a first delegation right governing distribution of the digital work to child nodes of the tree-like structure;

generate at least one of a second usage right and a second delegation right based on the hierarchical right, the second usage right governing a use for the digital work and the second delegation right governing distribution of the digital work to child nodes of a first child node of the tree-like structure;

assign the at least one of the second usage right and the second delegation right to a version of the digital work; and

transmit the at least one of the second usage right and the second delegation right and the version of the digital work to the first child node.

3. At least one non-transitory computer-readable medium storing computer-readable instructions that, when executed by one or more computing devices, cause at least one of the one or more computing devices to:

assign a hierarchical right to a digital work at a root node, the hierarchical right comprising a first usage right governing a use for the digital work and a first delegation right governing distribution of the digital work to child nodes of the tree-like structure;

generate at least one of a second usage right and a second delegation right based on the hierarchical right, the second usage right governing a use for the digital work and the second delegation right governing distribution of the digital work to child nodes of a first child node of the tree-like structure;

assign the at least one of the second usage right and the second delegation right to a version of the digital work; and

transmit the at least one of the second usage right and the second delegation right and the version of the digital work to the first child node.

\* \* \* \* \*