

METHOD AND APPARATUS FOR PUBLISHING WORK IN NETWORK

TECHNICAL FIELD

[0001] The present application relates to the field of network communications
5 technologies, and in particular, to a method and an apparatus for publishing a work in
a network.

BACKGROUND

[0002] Reading habits change with development of Internet technologies and
popularization of intelligent end-user devices. People now read news, learn
10 knowledge, and appreciate literary works mainly on the Internet, instead of on printed
materials. More authors directly publish their articles on the Internet for public
reading. Similarly, forwarding of and comments on published articles are also directly
published on the Internet without using any paper media.

[0003] However, because electronic data is easy to intercept and modify, after an
15 article is published, others can randomly select some content of the article to comment
on, or even make modifications to the original article during forwarding. Once a
damaging effect is caused by certain commenting or forwarding behaviors, the author
of an article can only clarify or explain his or her original idea to refute a rumor.
Because the author cannot prove an original feature of the article, such clarification or
20 explanation cannot achieve good result in practice.

SUMMARY

[0004] In view of this, the present application provides a method for publishing a
work in a network, including: obtaining, by an end-user device, a prior work file that
is not published by a current user in a network, where the prior work file includes a
25 digital signature of a prior author and a prior work; generating, by the end-user device
based on an operation of the current user, a new work file that includes the used prior

work, where the new work file includes the digital signature of the prior author, the prior work, and content added based on the operation of the current user; and publishing, by the end-user device, the new work file in the network.

[0005] The present application further provides an apparatus for publishing a work in a network, including: a prior-work-file acquisition unit, configured to obtain a prior work file that is not published by a current user in a network, where the prior work file includes a digital signature of a prior author and a prior work; a new-work-file generation unit, configured to generate, based on an operation of the current user, a new work file that includes the used prior work, where the new work file includes the digital signature of the prior author, the prior work, and content added based on the operation of the current user; and a new-work-file publishing unit, configured to publish the new work file in the network.

[0006] It can be seen from the previous technical solutions that in the implementations of the present application, the prior author appends a digital signature to the prior work of the prior author, and then publishes the prior work, and when generating, based on the operation of the current user other than the prior author, the new work file that includes the used prior work, the end-user device adds the prior work and the digital signature of the prior author to the new work file. Therefore, the prior work cannot be used out of context, and modifications to the prior work are easy to identify, thereby improving integrity and authenticity of a work propagated on the Internet.

BRIEF DESCRIPTION OF DRAWINGS

[0007] FIG. 1 is a network structure diagram illustrating an application scenario, according to an implementation of the present application;

[0008] FIG. 2 is a flowchart illustrating a method for publishing a work in a network, according to an implementation of the present application;

[0009] FIG. 3 is a schematic flowchart illustrating publishing an original work file and generating a new work file that includes a used work of another person, according to an application example of the present application;

[0010] FIG. 4 is a hardware structure diagram illustrating an end-user device, according to an implementation of the present application; and

[0011] FIG. 5 is a logical structural diagram illustrating an apparatus for

publishing a work in a network, according to an implementation of the present application.

DESCRIPTION OF IMPLEMENTATIONS

[0012] Implementations of the present application provide a new method for publishing a work in a network. An author who publishes a prior work file publishes both a prior work and a digital signature of the author in a network. When generating a new work file by using the prior work based on an operation of a current user, an end-user device adds the prior work and the digital signature of the prior author to the new work file. As such, after the new work file is published, an audience of a new work can know an original feature of the prior work, and the digital signature of the prior author can ensure that the prior work is not tampered with, thereby improving integrity and authenticity of a work forwarded on the Internet, and alleviating a problem in the existing technology.

[0013] An application scenario of the implementations of the present application is shown in FIG. 1. The prior author publishes the prior work file that includes the digital signature of the prior author in the network by operating a browser or application program client software running on an end-user device of the prior author. A specific process is as follows: The end-user device of the prior author uploads the prior work file to a server (a server accessed by the browser of the end-user device of the prior author or a server run by a serving end of the application program client software), and the server publishes the prior work file in the network (for example, adding a link of the prior work file to a web page, or pushing the prior work file to the application program client software). The current user (a user other than the prior author) can view the prior work on the end-user device used by the current user. In addition, the current user can further perform the method in the implementations of the present application on the end-user device of the current user, create a new work by using the prior work, and publish the new work by using the server.

[0014] The implementations of the present application can be run on any device with a computing and storage capability, for example, a physical device or a logical device such as a mobile phone, a tablet computer, a personal computer (PC), a notebook computer, a server, or a virtual machine. The physical device or the logical device is used by the current user as an end-user device.

[0015] In an implementation of the present application, a flowchart of a method for publishing a work in a network is shown in FIG. 2. The method is applied to an end-user device operated by a current user (a party responsible for a use behavior, such as a person or an organization that uses a work of another person in a work of the person or the organization).

[0016] Step 210: The end-user device obtains a prior work file that is not published by the current user in a network, where the prior work file includes a digital signature of a prior author and a prior work.

[0017] The current user can query and browse, in any way on the end-user device operated by the current user from various networks such as a public network and a private network, a work published by another person. The end-user device used by the current user obtains the prior work file from the network in a way corresponding to an operation of the current user, and the present implementation is not limited thereto. In the present implementation of present application, the prior work file is a work file that is published by another author (the prior author) other than the current user in the network, and the prior work file includes the prior work and the digital signature of the prior author for a part or all of the prior work.

[0018] The prior work can be any form that can be propagated in the network, such as an article, an image, an animation, audio, or a video, and the present implementation is not limited thereto. The prior work can be an original work, namely, a work created by an original author (without using a work of another person), or can be a work generated by using a work of another person, and the work is referred to as a work of a prior user.

[0019] If the prior work is an original work, there is only one party that is prior author, and a digital signature of the prior author is a digital signature appended by the prior author to the original work by using a private signature key of the prior author. If the prior work is a work of a prior user, the prior author includes an original author and one or more prior users, and a digital signature of the prior user can be one or more of a digital signature of the original author and digital signatures of the prior users.

[0020] Step 220: Generate, based on an operation of the current user, a new work file that includes the used prior work, where the new work file includes the prior work, the digital signature of the prior author, the prior work, and content added based on the operation of the current user.

[0021] After browsing the obtained prior work, the current user can generate a new work by using a device of the current user and the prior work. Using the prior work includes forwarding, commenting, quoting, annotating, etc. The present implementation of the present application is not limited thereto.

5 **[0022]** Based on a specific application environment, the end-user device receives a corresponding operation instruction of the current user, and generates the new work file based on the prior work file. Generally, the end-user device adds some content based on the operation of the current user when generating the new work file. The content can be content related to a use method (for example, when the prior work is
10 forwarded, a word "forwarding" is usually added, and sometimes a source of the forwarded prior work is further added), or can be content created by the current user (for example, when the prior work is annotated, interpretations of some content in the prior work by the current user are added). The new work file includes the content added based on the operation of the current user, and further includes the prior work
15 and digital signatures of all prior authors in the prior work file.

[0023] The prior work in the new work file can enable a user who browses the new work to know an original feature of the used prior work, and to understand the prior work and the new work based on a complete expression of the prior work. The digital signature of the prior author can be used to verify whether the prior work used
20 in the new work file is modified, to protect authenticity of the prior work.

[0024] After the end-user device publishes the new work file of the current user in the network, the new work can also be used as a prior work for another person to use. If the current user wants to protect integrity and authenticity of the new work in use, a digital signature of the current user can be added to the new work file by using the
25 end-user device of the current user. The end-user device can append, by using a private signature key used by the current user for identity authentication, a digital signature to the content added based on the operation of the current user in the new work file, or can append, by using a private signature key of the current user, a digital signature to the content added based on the operation of the current user and the prior
30 work in the new work file, and encapsulate the digital signature of the current user into the new work file.

[0025] In an implementation, the end-user device can perform signature verification on the prior work by using the digital signature of the prior author when generating the new work file. If the signature verification succeeds, the end-user

device generates the new work file that includes the content added based on the operation of the current user, the digital signature of the prior author, and the prior work. Otherwise, the end-user device refuses to generate a new work file, or generates a work file with a signature verification failure mark. Specific implementation of the signature verification failure mark can be determined based on an actual application environment. For example, the signature verification failure mark can be a mark field in the generated work file. When the mark field is a certain value, it indicates that the signature verification fails. For another example, in an application scenario in which all authors (including the original author, all the prior users, and the current user) append digital signatures to the published work, a digital signature whose signature verification fails may not be included in the generated work file when the signature verification fails. As such, after the generated work file is published, an audience of the work can learn of a time at which the used prior work may be modified.

[0026] In addition, the new work file can further include a publishing address of the prior work file in the network, so that an audience of the new work can further know the prior author, background information of the prior work, a related author, a related work, etc.

[0027] Step 230: The end-user device publishes the new work file in the network.

[0028] The end-user device publishes, based on an operation instruction of the current user, the generated new work file at a predetermined network address, a network address determined by a serving end, or a network address designated by the current user.

[0029] In some application scenarios, an end-user device used by an author of a work can encrypt content of the work by using a private encryption key of the author.

A propagation range of a public encryption key corresponding to the private encryption key is controlled, so that only a specific audience who obtains the public encryption key of the author can browse and use the work of the author. For example, the prior work in the prior work file can be ciphertext encrypted by an end-user device of the prior author by using a private encryption key of the prior author. For another example, the end-user device can first encrypt, by using a private encryption key of the current user, the prior work and the content added based on the operation of the current user, and then encapsulate the ciphertext into the new work file.

[0030] It is worthwhile to note that the private encryption key and the private signature key of the prior author or the current user can be the same private key, or

different private keys can be used for encryption and signature.

[0031] It can be seen that in the present implementation of the present application, the author of the prior work publishes both the digital signature of the author and the prior work in the network, and when generating, based on the operation of the current user, the new work file that includes the used prior work, the end-user device adds the prior work and the digital signature of the prior author to the new work file, so that the audience of the new work can know complete content of the prior work, and the digital signature of the prior author is used to ensure that the prior work is not tampered with. Therefore, the prior work cannot be used out of context, and modifications to the prior work are easy to identify, thereby improving integrity and authenticity of a work propagated on the Internet.

[0032] The present implementation of the present application can be applied by using different mechanisms based on a traceable requirement on integrity and authenticity of a work in an actual application environment. Two methods are used as examples below for description.

[0033] In the first method, authors (including an original author and a user who uses a work of another person) determine whether to append a digital signature. When generating the new work file that includes the used prior work, the end-user device needs to add the prior work and the digital signature of the prior author to the generated new work file if the prior work file includes the digital signature, otherwise, may not add the prior work and the digital signature of the prior author. The current user can choose whether to append a digital signature to the generated new work file.

[0034] In the second method, all works include digital signatures of authors. As such, the prior work file usually includes the original work, content added by all the prior users, the digital signature of the original author, and the digital signatures of all the prior users. On this basis, the content added by the current user and the digital signature of the current user are usually added to the new work file. In this method, authenticity and integrity of a work in the network is traceable in the whole process.

[0035] In an application example of the present application, each article published on the Internet includes a digital signature of an author of the article, and content of the article is encrypted by using a private key of the author. Referring to FIG. 3, for example, original author A publishes an original work file on the Internet. The original work file includes ciphertext obtained by encrypting an original work by using a private key of original author A and a digital signature appended to the original work

by using the private key of original author A. After original author A publishes the original work file on the Internet, all users who can obtain a public key of original author A can read the original work.

[0036] Assume that reader B is permitted to obtain the public key of original author A. After reading the original work by using a mobile phone (an end-user device) of reader B, reader B wants to publish a review article of the original work. Based on an operation of current user B, the mobile phone of reader B (current user B) performs signature verification on the decrypted original work by using the public key of original author A. If the signature verification succeeds, current user B appends a digital signature to the original work and comment content of current user B by using a private key of current user B, and the mobile phone encrypts the original work and the comment content of current user B by using the private key of current user B, encapsulates the ciphertext, the digital signature of original author A, and the digital signature of current user B into a comment work file, and publishes the comment work file on the Internet based on an instruction of current user B. If the signature verification fails, the mobile phone appends a digital signature to the original work and comment content of current user B by using a private key of current user B, encrypts the original work and the comment content of current user B by using the private key of current user B, encapsulates the ciphertext and the digital signature of current user B into a comment article, and publishes the comment article based on an instruction of current user B.

[0037] Assume that reader C is permitted to obtain a public key of current user B. If a mobile phone of reader C finds that the comment work file does not include the digital signature of original author A, when displaying the comment content and the original work to reader C, the mobile phone can notify reader C that signature verification on the original work fails.

[0038] Corresponding to the previous procedure implementation, an implementation of the present application further provides an apparatus for publishing a work in a network. The apparatus can be implemented by software, can be implemented by hardware, or can be implemented by a combination of hardware and software. In an example of software implementation, a logical apparatus is formed in the following way: A central processing unit (CPU) of an end-user device reads a corresponding computer program instruction to a memory, and the computer program instruction runs to form the apparatus. In terms of hardware, in addition to a CPU, a

memory, and a nonvolatile memory shown in FIG. 4, the end-user device where the apparatus for publishing a work in a network is located usually includes other hardware such as a chip configured to receive and send a radio signal and/or other hardware such as a card configured to implement a network communication function.

5 **[0039]** FIG. 5 illustrates an implementation apparatus for publishing a work in a network, according to an implementation of the present application, including a prior-work-file acquisition unit, a new-work-file generation unit, and a new-work-file publishing unit. The prior-work-file acquisition unit is configured to obtain a prior work file that is not published by a current user in a network, where the prior work
10 file includes a digital signature of a prior author and a prior work. The new-work-file generation unit is configured to generate, based on an operation of the current user, a new work file that includes the used prior work, where the new work file includes the digital signature of the prior author, the prior work, and content added based on the operation of the current user. The new-work-file publishing unit is configured to
15 publish the new work file in the network.

[0040] Optionally, the prior work in the prior work file is encrypted by using a private encryption key of the prior author, and/or the prior work and the content added based on the operation of the current user in the new work file are encrypted by using a private encryption key of the current user.

20 **[0041]** In an implementation, the new work file further includes a digital signature of the current user.

[0042] In the previous implementations, the digital signature of the current user can be a digital signature appended, by using a private signature key of the current user, to the content added based on the operation of the current user.

25 **[0043]** In the previous implementations, the digital signature of the current user can be a digital signature appended, by using a private signature key of the current user, to the prior work and the content added based on the operation of the current user.

[0044] Optionally, the new-work-file generation unit is configured to perform
30 signature verification on the prior work by using the digital signature of the prior author, and generate the new work file that includes the used prior work if the signature verification succeeds, otherwise, refuse to generate a new work file or generate a work with a signature verification failure mark.

[0045] Optionally, using the prior work includes: forwarding the prior work or

commenting on the prior work.

[0046] Optionally, the new work file further includes a publishing address of the prior work file in the network.

[0047] The previous descriptions are merely examples of implementations of the present application, but are not intended to limit the present application. Any modification, equivalent replacement, or improvement made without departing from the spirit and principle of the present application should fall within the protection scope of the present application.

[0048] In a typical configuration, a computing device includes one or more processors (CPU), one or more input/output interfaces, one or more network interfaces, and one or more memories.

[0049] The memory may include a non-persistent memory, a random access memory (RAM), and/or a nonvolatile memory in a computer readable medium, for example, a read-only memory (ROM) or a flash memory (flash RAM). The memory is an example of the computer readable medium.

[0050] The computer readable medium includes persistent, non-persistent, removable, and irremovable media that can store information by using any method or technology. The information can be a computer readable instruction, a data structure, a program module, or other data. Examples of the computer storage medium include but are not limited to a phase-change random access memory (PRAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), another type of random access memory (RAM), a read-only memory (ROM), an electrically erasable programmable read-only memory (EEPROM), a flash memory or another memory technology, a compact disc read-only memory (CD-ROM), a digital versatile disc (DVD) or another optical storage, a cassette magnetic tape, a magnetic tape/magnetic disk storage, another magnetic storage device, or any other non-transmission medium. The computer storage medium can be used to store information accessible by the computing device. As described in the present specification, the computer readable medium does not include computer-readable transitory media (transitory media) such as a modulated data signal and a carrier.

[0051] It is worthwhile to further note that the terms "include", "comprise", or their any other variants are intended to cover a non-exclusive inclusion, so that a process, a method, a product or a device that includes a list of elements not only includes those elements but also includes other elements which are not expressly

listed, or further includes elements inherent to such process, method, product or device. An element described by "includes a ..." further includes, without more constraints, another same or identical element in the process, method, article, or device that includes the element.

- 5 **[0052]** A person skilled in the art should understand that an implementation of the present application can be provided as a method, a system, or a computer program product. Therefore, the present application can use a form of hardware-only implementations, software-only implementations, or implementations with a combination of software and hardware. Moreover, the present application can use a
- 10 form of a computer program product that is implemented on one or more computer-usable storage media (including but not limited to a disk memory, a CD-ROM, an optical memory, etc.) that include computer-usable program code.

CLAIMS

What is claimed is:

1. A method for publishing a work in a network, comprising:
 - obtaining, by an end-user device, a prior work file that is not published by a current user in a network, wherein the prior work file comprises a digital signature of a prior author and a prior work;
 - generating, by the end-user device based on an operation of the current user, a new work file that comprises the used prior work, wherein the new work file comprises the digital signature of the prior author, the prior work, and content added based on the operation of the current user; and
 - publishing, by the end-user device, the new work file in the network.
2. The method according to claim 1, wherein the prior work in the prior work file is encrypted by using a private encryption key of the prior author, and/or the prior work and the content added based on the operation of the current user in the new work file are encrypted by using a private encryption key of the current user.
3. The method according to claim 1 or 2, wherein the new work file further comprises a digital signature of the current user.
4. The method according to claim 3, wherein the digital signature of the current user is a digital signature appended, by using a private signature key of the current user, to the content added based on the operation of the current user.
5. The method according to claim 3, wherein the digital signature of the current user is a digital signature appended, by using a private signature key of the current user, to the prior work and the content added based on the operation of the current user.
6. The method according to claim 1, wherein the generating, by the end-user device based on an operation of the current user, a new work file that comprises the used prior work comprises: performing signature verification on the prior work by using the digital signature of the prior author, and generating the new work file that comprises the used prior work if the signature verification succeeds, otherwise, refusing to generate a new work file or generating a work with a signature verification failure mark.

7. The method according to claim 1, wherein using the prior work comprises: forwarding the prior work or commenting on the prior work.

8. The method according to claim 1, wherein the new work file further comprises a publishing address of the prior work file in the network.

9. An apparatus for publishing a work in a network, comprising:

a prior-work-file acquisition unit, configured to obtain a prior work file that is not published by a current user in a network, wherein the prior work file comprises a digital signature of a prior author and a prior work;

a new-work-file generation unit, configured to generate, based on an operation of the current user, a new work file that comprises the used prior work, wherein the new work file comprises the digital signature of the prior author, the prior work, and content added based on the operation of the current user; and

a new-work-file publishing unit, configured to publish the new work file in the network.

10. The apparatus according to claim 9, wherein the prior work in the prior work file is encrypted by using a private encryption key of the prior author, and/or the prior work and the content added based on the operation of the current user in the new work file are encrypted by using a private encryption key of the current user.

11. The apparatus according to claim 9 or 10, wherein the new work file further comprises a digital signature of the current user.

12. The apparatus according to claim 11, wherein the digital signature of the current user is a digital signature appended, by using a private signature key of the current user, to the content added based on the operation of the current user.

13. The apparatus according to claim 11, wherein the digital signature of the current user is a digital signature appended, by using a private signature key of the current user, to the prior work and the content added based on the operation of the current user.

14. The apparatus according to claim 9, wherein the new-work-file generation unit is configured to perform signature verification on the prior work by using the digital signature of the prior author, and generate the new work file that comprises the used prior work if the signature verification succeeds, otherwise, refuse to generate a new work file or generate a work with a signature verification failure mark.

15. The apparatus according to claim 9, wherein using the prior work comprises: forwarding the prior work or commenting on the prior work.

16. The apparatus according to claim 9, wherein the new work file further comprises a publishing address of the prior work file in the network.