(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
01 December 2022 (01.12.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/246641 A1

(51) International Patent Classification:
G06F 21/62 (2013.01)

(21) International Application Number:
PCT/CN2021/095746

(22) International Filing Date:
25 May 2021 (25.05.2021)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **MICROSOFT TECHNOLOGY LICENSING, LLC** [US/US]; One Microsoft Way, Redmond, Washington 98052 (US).

(72) Inventor; and

(71) Applicant *(for BZ only)*: **HOBDEN, Andrew James** [GB/CN]; One Microsoft Way, Redmond, Washington 98052 (US).

(74) Agent: **NTD PATENT & TRADEMARK AGENCY LTD.**; 10th Floor, Tower C, Beijing Global Trade Center, 36 North Third Ring Road East, Dongcheng District, Beijing 100013 (CN).

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

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

Declarations under Rule 4.17:
— *of inventorship (Rule 4.17(iv))*

Published:
— *with international search report (Art. 21(3))*

(54) **Title:** CONTENT MANAGEMENT OF DOCUMENTS

(57) **Abstract:** The present disclosure provides methods and apparatuses for content management of documents. A request for adding a restricted content to a document may be received from a first terminal device of a first user, the request including the restricted content and a corresponding access permission configuration. A restricted content layer containing the restricted content may be added into the document. A request for accessing the document may be received from a second terminal device of a second user. The document may be sent to the second terminal device. It may be determined whether the second user has an access permission to the restricted content based at least on the access permission configuration. The restricted content contained in the restricted content layer may be rendered on the second terminal device, in response to determining that the second user has the access permission.

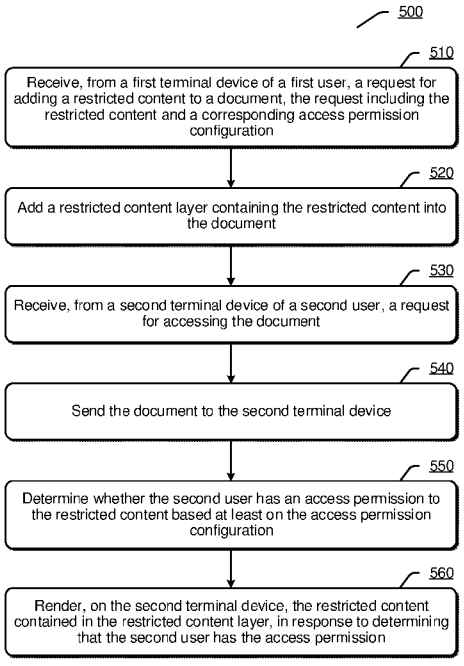

FIG 5

WO 2022/246641 A1

CONTENT MANAGEMENT OF DOCUMENTS

BACKGROUND

[0001] Document processing through computer techniques is common in people's work and life. Various document processing tools are proposed for processing various types of document. Herein, a document may refer to a file containing various types of digital content such as text, image, etc. Examples of document may include, e.g., word processing document, spreadsheet, presentation document, PDF document, etc. A document processing tool may refer to a document authoring or editing application. A user may create, view or edit a document through a corresponding document processing tool. In recent years, with the development of cloud techniques, document processing services that are based on cloud services are widely applied. Through these cloud-based document processing services, documents may be further shared, synchronized, collaborated, or protected among multiple users in a user group. Examples of cloud-based document processing service may include, e.g., productivity tools under cloud services, etc.

SUMMARY

[0002] This Summary is provided to introduce a selection of concepts that are further described below in the Detailed Description. It is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used to limit the scope of the claimed subject matter.

[0003] Embodiments of the present disclosure propose methods and apparatuses for content management of documents. A request for adding a restricted content to a document may be received from a first terminal device of a first user, the request including the restricted content and a corresponding access permission configuration. A restricted content layer containing the restricted content may be added into the document. A request for accessing the document may be received from a second terminal device of a second user. The document may be sent to the second terminal device. It may be determined whether the second user has an access permission to the restricted content based at least on the access permission configuration. The restricted content contained in the restricted content layer may be rendered on the second terminal device, in response to determining that the second user has the access

permission.

[0004] It should be noted that the above one or more aspects comprise the features hereinafter fully described and particularly pointed out in the claims. The following description and the drawings set forth in detail certain illustrative features of the one or more aspects. These features are only indicative of the various ways in which the principles of various aspects may be employed, and this disclosure is intended to include all such aspects and their equivalents.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] The disclosed aspects will hereinafter be described in connection with the appended drawings that are provided to illustrate and not to limit the disclosed aspects.

[0006] FIG.1 illustrates an exemplary architecture for implementing content management of documents according to an embodiment.

[0007] FIG.2 illustrates an exemplary process for content management of documents according to an embodiment.

[0008] FIG.3 illustrates an exemplary process for content management of documents according to an embodiment.

[0009] FIG.4 illustrates an exemplary process for content management of documents according to an embodiment.

[0010] FIG.5 illustrates a flowchart of an exemplary method for content management of documents according to an embodiment.

[0011] FIG.6 illustrates an exemplary apparatus for content management of documents according to an embodiment.

[0012] FIG.7 illustrates an exemplary apparatus for content management of documents according to an embodiment.

DETAILED DESCRIPTION

[0013] The present disclosure will now be discussed with reference to several example implementations. It is to be understood that these implementations are discussed only for enabling those skilled in the art to better understand and thus implement the embodiments of the present disclosure, rather than suggesting any limitations on the scope of the present disclosure.

[0014] For the cloud-based document processing services, access control or right

management for documents is important and necessary. For example, it may be desired that a certain document is accessible only by some specified users in a user group, but is not accessible by those users without permissions in or outside of the user group. Currently, access control or right management is typically performed on the whole document. For example, if a user has no access permission to a document, the user would be unable to see any content in the document.

[0015] Embodiments of the present disclosure propose content management of documents that directs to managing access permissions to a part of content in a document. Through setting respective layers for multiple parts of content in a document, access permission control may be applied to these parts of content respectively. Herein, a part of content in a document that is applied by access permission control may be referred to as a restricted content. A restricted content in a document may be widely interpreted as a content for which access restriction is applied according to specified access permissions. Access permissions to a restricted content may indicate which users in a user group are permitted to access the restricted content and what types of accessing operation are allowed. Herein, a user group may comprise a plurality of users that are associated with the document, e.g., users co-working on the document, users being as recipients of the document, etc. It should be understood that the embodiments of the present disclosure are not limited to the case that there is a user group, but can also be similarly applied for the case that no user group is defined. Examples of access permission to a restricted content may comprise, e.g., a permission to view the restricted content, a permission to edit the restricted content, etc. Multiple restricted contents may be defined in a document through setting multiple corresponding restricted content layers. Each restricted content layer may contain a corresponding restricted content, and an access permission configuration may be set for the restricted content, which contains access permissions to the restricted content specified for one or more users.

[0016] The content management of documents according to the embodiments of the present disclosure may be implemented in a document processing service. Hereinafter, a document processing service may widely refer to various document processing services or applications that are based on cloud services. The document processing service according to the embodiments of the present disclosure may enable a user who is creating or editing a document to add one or more restricted contents

into the document and set corresponding access permission configurations, and enable those users who requests to access the document to view or edit the restricted contents according to their respective access permissions.

[0017] In an implementation, restricted contents in a document may be annotations. Herein, annotations may widely refer to various contents that contain opinions or comments of creators, editors or viewers of the document, and are visually distinct from the text of the document. The annotations may take various forms, e.g., inline texts or images, sticky notes, signatures, comments, drawings, etc. In this scenario, restricted content layers may also be referred to as annotation layers. Multiple annotation layers may be set for multiple annotations respectively, and corresponding access permissions may be specified for these annotations respectively.

[0018] In an implementation, restricted contents in a document may be content sections in the document. Herein, content sections may widely refer to a group of words, sentences, paragraphs, etc. in the text of the document. In this scenario, restricted content layers may also be referred to as content section layers. Multiple content section layers may be set for multiple content sections respectively, and corresponding access permissions may be specified for these content sections respectively.

[0019] Through the content management of documents according to the embodiments of the present disclosure, more flexible and convenient access permission control to restricted contents in documents may be achieved, and thus user experience of document processing services may be significantly improved. Moreover, since restricted content layers are incorporated in a document, a single document could be sent to a terminal device and rendered on the terminal device according to a corresponding access permission, and thus the embodiments of the present disclosure could reduce processing burdens at the server or network side, and could avoid transmission delay of a restricted content in the case of sending the restricted content in a separate file from the document.

[0020] FIG.1 illustrates an exemplary architecture 100 for implementing content management of documents according to an embodiment.

[0021] In the architecture 100, a document processing service 110 is deployed for providing various types of document processing function for users, e.g., creating a document, viewing a document, editing a document, etc. The document processing

service 110 is based on cloud services, and documents may be shared, collaborated, etc. among multiple users.

[0022] The document processing service 110 may comprise a document processing unit 112. The document processing unit 112 is a core unit for document processing, and supports various traditional operations of creating, viewing, editing, etc. of documents.

[0023] The document processing service 110 may further comprise a restricted content processing unit 114. The restricted content processing unit 114 may provide various functions related to restricted content processing and access permission control. The restricted content processing unit 114 and the document processing unit 112 may communicate with each other, so as to transfer necessary information related to content management of documents between them.

[0024] It should be understood that the document processing unit 112 and the restricted content processing unit 114 in the document processing service 110 may be implemented through various approaches. For example, in a server-client implementation approach, a client application corresponding to the document processing unit 112 and/or the restricted content processing unit 114 may be installed in a terminal device, and the client may cooperate with a server corresponding to the document processing unit 112 and/or the restricted content processing unit 114 at the network or cloud side, so as to provide document processing service for users of the terminal device. For example, in a web-based implementation approach, the document processing unit 112 and/or the restricted content processing unit 114 may be hosted at the network or cloud side, and a user may utilize, e.g., a web browser in a terminal device to access the document processing unit 112 and/or the restricted content processing unit 114 so as to obtain document processing service. The embodiments of the present disclosure are not limited to any specific implementation approaches of the document processing unit 112 and/or the restricted content processing unit 114. Moreover, although the restricted content processing unit 114 is shown in FIG.1 as a separate unit from the document processing unit 112, the restricted content processing unit 114 may also be implemented as a component or an invoked function of the document processing unit 112.

[0025] As shown in FIG.1, a user 122 may utilize the document processing service 110 for creating or editing a document 102 on a terminal device 120. The

document processing service 110 may comprise various UIs for interacting with users. It is assumed that the user 122 has input a basic content into the document 102, wherein the basic content may refer to content in the text of the document 102 that is not applied by access permission control and thus accessible by all the users in a user group.

[0026] The user 122 may further identify or input restricted content 1 and restricted content 2, and set access permission configurations for the restricted content 1 and the restricted content 2 respectively. For example, the access permission configuration for the restricted content 1 may specify that a user 132 has an access permission to the restricted content 1, e.g., a permission to view the restricted content 1. For example, the access permission configuration for the restricted content 2 may specify that a user 142 has an access permission to the restricted content 2, e.g., a permission to view and edit the restricted content 2.

[0027] In an implementation, the user 122 may explicitly request in the UIs for establishing restricted content layers for the restricted contents 1 and 2 respectively, and the restricted content processing unit 114 would establish the restricted content layers accordingly. In another implementation, the establishing of restricted content layers may be transparent to the user 122, e.g., the user 122 may only identify or input the restricted contents 1 and 2, and the restricted content processing unit 114 would establish the restricted content layers on the backend.

[0028] The restricted content processing unit 114 may store access permission information contained in the access permission configurations in association with the restricted contents. The restricted content processing unit 114 may establish a restricted content layer 1 containing the restricted content 1 and a restricted content layer 2 containing the restricted content 2 respectively. The document processing unit 112 may add the restricted content layers 1 and 2 into the document 102. Thus, the document 102 would comprise both the basic content and the restricted content layers. In an implementation, the restricted content layers may be encrypted by the restricted content processing unit 114, and thus the document processing unit 112 would add the encrypted restricted content layers into the document 102. The encrypting operation of the restricted content layers would result in that the restricted contents could be rendered on a terminal device only after the encrypted restricted content layers are decrypted with a decryption key provided by the restricted content processing unit.

[0029] It is assumed that the user 132 requests to access the document 102 through the document processing service 110 on a terminal device 130. The document processing unit 112 may send the document 102 including the basic content and the restricted content layers 1 and 2 to the terminal device 130. The basic content may be further rendered on the terminal device 130. Meanwhile, since the user 132 is specified as having an access permission to the restricted content 1, e.g., to view the restricted content 1, but having no access permission to the restricted content 2, only the restricted content 1 would be rendered on the terminal device 130. Accordingly, the user 132 could view both the basic content and the restricted content 1 on the terminal device 130. The user 132 may further edit the basic content since no access permission control is applied to the basic content. However, the user 132 cannot edit the restricted content 1 since no access permission to edit the restricted content 1 is specified for the user 132. It should be understood that, if the restricted content layer 1 is encrypted, the rendering of the restricted content 1 may comprise: decrypting the encrypted restricted content layer 1 with, e.g., a decryption key provided by the restricted content processing unit 114; and rendering the restricted content 1 contained in the decrypted restricted content layer 1.

[0030] Similarly, when the user 142 requests to access the document 102 through the document processing service 110 on a terminal device 140, the basic content and the restricted content 2 could be rendered on the terminal device 140, wherein the restricted content 2 is rendered according to the access permission specified for the user 142. The user 142 may further view and edit the basic content. Moreover, the user 142 may also view and edit the restricted content 2 since the user 142 is specified as having an access permission to view and edit the restricted content 2.

[0031] As a further example, it is assumed that there is another user requesting to access the document 102, but this user is not listed in any access permission configuration, i.e., this user is not permitted to access anyone of the restricted contents 1 and 2. Accordingly, only the basic content would be rendered on a terminal device of this user.

[0032] It should be understood that the embodiments of the present disclosure are not limited to any specific approaches of specifying access permissions in access permission configurations. For example, instead of only specifying which users have access permissions to a restricted content in an access permission configuration, the

access permission configuration may also specify which users have no access permissions to the restricted content. Accordingly, when deciding whether to render the restricted content on a terminal device of a user, it may be checked whether the user is specified as having an access permission to the restricted content or is specified as having no access permission to the restricted content, based at least on the access permission configuration. For the sake of simplicity, the following discussions take the approach of only specifying which users have access permissions to a restricted content in an access permission configuration as an example.

[0033] FIG.2 illustrates an exemplary process 200 for content management of documents according to an embodiment. The process 200 may be implemented based on the architecture 100 in FIG.1, e.g., performed by the document processing service 110.

[0034] It is assumed that a first user is editing a document on a first terminal device as a creator or an editor of the document.

[0035] At 210, a request for adding a restricted content into the document may be received from the first terminal device of the first user. This request may indicate that the first user desires to add the restricted content to the document. The request may be made by the first user in the UIs of the document processing service in various approaches, and the present disclosure is not limited to any specific approach of inputting and sending the request by the first user. In an implementation, the request may include the restricted content and a corresponding access permission configuration. The access permission configuration specifies at least one access permission to the restricted content for at least one another user. For example, the access permission configuration may specify which users have access permissions to the restricted content and what types of access permission these users have. Users may be identified in the access permission configuration with corresponding user IDs, e.g., account numbers, user names, user emails, etc. The user IDs in the access permission configuration may be the same as those with which these users log in the document processing service. In another implementation, the request received at 210 is a logical concept which may be a combination of the restricted content and the access permission configuration, and accordingly the receiving of the request at 210 may comprise a step of receiving the restricted content and a step of receiving the access permission configuration respectively.

[0036] At 220, a restricted content layer containing the restricted content may be added into the document. For example, the restricted content layer may be inserted into the basic content of the document, attached at the side of the basic content, placed over the basic content, etc. Accordingly, the document would include both the restricted content layer and the basic content. In an implementation, the restricted content layer may be encrypted before being added into the document.

[0037] At 230, a request for accessing the document may be received from a second terminal device of a second user. The second user may have logged in the document processing service with a corresponding user ID, and thus can be identified by the document processing service. The request indicates that the second user desires to perform operations on the document, e.g., viewing, editing, etc. the document.

[0038] At 240, in response to the request for accessing the document from the second terminal device of the second user, the document may be sent to the second terminal device. This document includes both the basic content and the restricted content layer.

[0039] At 250, it is determined whether the second user has an access permission to the restricted content based at least on the access permission configuration. For example, the restricted content processing unit may check whether the second user is listed in the access permission configuration as having an access permission.

[0040] If it is determined at 250 that the second user has the access permission, the restricted content contained in the restricted content layer may be rendered on the second terminal device at 260. Moreover, the basic content may also be rendered on the second terminal device at 260. The basic content and the restricted content may be rendered independently or rendered together. If the restricted content layer has been encrypted, the rendering of the restricted content may comprise decrypting the encrypted restricted content layer first, and then rendering the restricted content contained in the decrypted restricted content layer.

[0041] If it is determined at 250 that the second user has no access permission, only the basic content would be rendered on the second terminal device at 270, while the restricted content would not be rendered.

[0042] Through the rendering at 260 or 270, the rendered basic content and possible restricted content would be displayed on the second terminal device, and thus the second user could view the rendered contents. It the second user further performs

operations on the rendered contents, the process 200 may respond to the user operations at 280. Here, only the user operations conforming to the access permission would be responded. For example, if the second user is only permitted to view the restricted content, only viewing-related operations, e.g., scrolling up/down, zooming in/out, etc. on the restricted content would be responded. While if the second user is permitted to edit the restricted content, editing-related operations, e.g., modifying, deleting, etc. on the restricted content would also be responded. Herein, the responding to user operations may refer to that the document processing service processes the restricted content according to intentions of the user operations. For example, if the user operation indicates that the user intends to modify a word in the restricted content to another word, the document processing service would replace the original word by said another word in the restricted content. It should be understood that, at 280, the process 200 may also respond to user operations on the basic content of the document.

[0043] It should be understood that all the steps and orders of these steps in the process 200 are exemplary, and the embodiments of the present disclosure may cover various changes to the process 200. In an implementation, the steps 210 to 220 may be performed repeatedly so as to add two or more restricted contents into the document. In an implementation, the second user may be the same as the first user, i.e., after the restricted content has been added into the document, the first user may return to the document processing service and request to access the document again. In this case, it may be predefined that the first user has all access permissions to the restricted content since the first user is the creator of the restricted content. In an implementation, although it is shown in the process 200 that the step 240 is performed before the step 250, the step 250 may also be performed before the step 240 or these two steps may be performed concurrently.

[0044] FIG.3 illustrates an exemplary process 300 for content management of documents according to an embodiment. The process 300 is a specific implementation of the process 200 in FIG.2, in which restricted contents are annotations, and restricted content layers are annotation layers.

[0045] At 310, it is assumed that a user 301 is currently editing a document on a terminal device 302. The editing of the document may be performed in UIs provided by a document processing service. Specifically, the editing of the document may be

supported by a document processing unit 304 in the document processing service. The document processing unit 304 may correspond to the document processing unit 112 in FIG.1.

[0046] When the user 301 desires to add a restricted content, e.g., an annotation, into the document, the user 301 may send the annotation to an annotation processing unit 306 in the document processing service at 312. For example, in the UIs of the document processing service, the user 301 may select or designate, in a basic content of the document, a position for adding the annotation, and input the annotation in an input box. The annotation processing unit 306 may receive the annotation from the terminal device 302 at 312. The annotation processing unit 306 may be a specific implementation of the restricted content processing unit 114 in FIG.1.

[0047] The user 301 may further specify access permissions to the annotation for other users. For example, at 314, the user 301 may input and send an access permission configuration to the annotation processing unit 306. The annotation processing unit 306 may receive the access permission configuration from the terminal device 302, wherein the access permission configuration specifies at least one access permission to the annotation for at least one another user.

[0048] It should be understood that, although the annotation and the access permission configuration are shown as being received by the annotation processing unit 306 at the step 312 and the step 314 respectively, the annotation and the access permission configuration may also be received in a single request sent from the terminal device, wherein this request may request to add the annotation into the document and may include both the annotation and the access permission configuration.

[0049] At 316, the annotation processing unit 306 may create a record which includes information in the access permission configuration.

[0050] At 318, the annotation processing unit 306 may establish an annotation layer containing the annotation and transfer the annotation layer to the document processing unit 304. In an implementation, the annotation layer may be encrypted, and the annotation processing unit 306 may further store a decryption key for decrypting the encrypted annotation layer in the record.

[0051] At 320, the document processing unit 304 may add the annotation layer into the document, so as to obtain a document including both the basic content and the

annotation layer.

[0052] At 322, the document processing unit 304 may receive a request for accessing the document from a terminal device 308 of a user 303. In an implementation, the user 303 may have logged in the document processing service with a corresponding user ID, and thus can be identified by the document processing service.

[0053] At 324, in response to the request received at 322, the document processing unit 304 may send the document to the terminal device 308.

[0054] At 326, the document processing unit 304 may forward the request received at 322 together with the user ID of the user 303 to the annotation processing unit 306.

[0055] At 328, the annotation processing unit 306 may determine whether the user 303 has an access permission to the annotation based at least on the access permission configuration. For example, the annotation processing unit 306 may check the record to see whether the user ID of the user 303 is listed in the access permission configuration as having an access permission. If it is determined that the user 303 has the access permission, the annotation processing unit 306 may further retrieve the decryption key from the record.

[0056] At 330, the document processing unit 304 may render the basic content in the document on the terminal device 308, such that the user 303 may view the basic content.

[0057] At 332, the annotation processing unit 306 may render the annotation on the terminal device 308. In an implementation, in the case that the annotation layer is encrypted and the decryption key is retrieved, the annotation may be rendered with the decryption key. For example, the encrypted annotation layer may be first decrypted with the decryption key, and then the annotation in the decrypted annotation layer may be rendered on the terminal device 308.

[0058] It should be understood that, if it is determined at 328 that the user 303 has no access permission to the annotation, the step of 332 would be omitted, i.e., the annotation would not be rendered, and thus the user 303 could only view or edit the rendered basic content.

[0059] In the process 300, the rendering of the basic content and the rendering of the annotation are independent from each other. That is, the document processing unit

304 would not recognize whether the annotation processing unit 306 has rendered the annotation and how the annotation is rendered. Such mechanism makes the annotation processing unit easy to be integrated into various types of document processing service.

[0060] It should be understood that although the basic content and the annotation are rendered independently, the basic content and the annotation may be presented on the terminal device 308 synchronously. Herein, synchronous presenting may refer to that the basic content and the annotation visually maintain fixed relative positions, fixed relative sizes, the same movement directions, etc., no matter how the user changes the displayed part of the document in a screen window on a terminal device. For example, the basic content and the annotation may be synchronously scrolled up/down, zoomed in/out, etc. in a screen window on the terminal device 308. In an implementation, the synchronous presenting of the basic content and the annotation may be achieved through transferring information of viewing-related operations between the document processing unit 304 and the annotation processing unit 306. For example, the document processing unit 304 may send information of viewing-related operations on the basic content to the annotation processing unit 306 in real time, and the annotation processing unit 306 may change the presenting of the annotation according to the viewing-related operations, such that both the presenting of the basic content and the presenting of the annotation would conform to the viewing-related operations, and thus are presented synchronously.

[0061] After the basic content and the annotation are rendered on the terminal device 308, the document processing service may respond to further operations performed by the user 303 on the terminal device 308. For example, the document processing unit 304 may respond to any user operations on the basic content, and the annotation processing unit 306 may respond to user operations on the annotation conforming to the access permission of the user 303.

[0062] It should be understood that all the steps and orders of these steps in the process 300 are exemplary, and the embodiments of the present disclosure may cover various changes to the process 300.

[0063] FIG.4 illustrates an exemplary process 400 for content management of documents according to an embodiment. The process 400 is a specific implementation of the process 200 in FIG.2, in which restricted contents are content sections, and

restricted content layers are content section layers.

[0064] At 410, it is assumed that a user 401 is currently editing a document on a terminal device 402. The editing of the document may be performed in UIs provided by a document processing service. Specifically, the editing of the document may be supported by a document processing unit 404 in the document processing service. The document processing unit 404 may correspond to the document processing unit 112 in FIG.1.

[0065] When the user 401 desires to add or identify a restricted content section in the document, the user 401 may send the content section to the document processing unit 404 at 412. For example, in one case, in the UIs of the document processing service, the user 401 may select a part of the document as the restricted content section. For example, in another case, the user 401 may establish a new region for inputting the content section in the document, and then input the content section into the region. The document processing unit 404 may receive the content section from the terminal device 402 at 412.

[0066] The user 401 may further specify access permissions to the content section for other users. For example, at 414, the user 401 may input and send an access permission configuration to the document processing unit 404. The document processing unit 404 may receive the access permission configuration from the terminal device 402 at 414, wherein the access permission configuration specifies at least one access permission to the content section for at least one another user.

[0067] It should be understood that, although the content section and the access permission configuration are shown as being received by the document processing unit 404 at the step 412 and the step 414 respectively, the content section and the access permission configuration may also be received in a single request sent from the terminal device, wherein this request may request to add the content section into the document and may include both the content section and the access permission configuration.

[0068] At 416, the document processing unit 404 may send the content section and the access permission configuration to a right management unit 406. The right management unit 406 may be a specific implementation of the restricted content processing unit 114 in FIG.1, and may adopt various right management techniques.

[0069] At 418, the right management unit 406 may create a record which includes

information in the access permission configuration.

[0070] At 420, the right management unit 406 may establish a content section layer containing the content section and transfer the content section layer to the document processing unit 404. In an implementation, the content section layer may be encrypted, and the right management unit 406 may further store a decryption key for decrypting the encrypted content section layer in the record.

[0071] At 422, the document processing unit 404 may add the content section layer into the document, so as to obtain a document including both a basic content and the content section layer.

[0072] At 424, the document processing unit 404 may receive a request for accessing the document from a terminal device 408 of a user 403. In an implementation, the user 403 may have logged in the document processing service with a corresponding user ID, and thus can be identified by the document processing service.

[0073] At 426, in response to the request received at 424, the document processing unit 404 may send the document to the terminal device 408.

[0074] At 428, the document processing unit 404 may forward the request received at 424 together with the user ID of the user 403 to the right management unit 406.

[0075] At 430, the right management unit 406 may determine whether the user 403 has an access permission to the content section based at least on the access permission configuration. For example, the right management unit 406 may check the record to see whether the user ID of the user 403 is listed in the access permission configuration as having an access permission. If it is determined that the user 403 has the access permission, the right management unit 406 may further retrieve the decryption key from the record.

[0076] At 432, the right management unit 406 may send the retrieved decryption key to the document processing unit 404.

[0077] At 434, the document processing unit 404 may render both the basic content and the restricted content section on the terminal device 408, such that the user 403 may view the basic content and the content section. In the case that the content section layer is encrypted and the decryption key is received, the document processing unit 404 may first decrypt the encrypted content section layer, and then

render the content section contained in the decrypted content section layer together with the basic content on the terminal device 408.

[0078] It should be understood that, if it is determined at 430 that the user 403 has no access permission to the content section, the document processing unit 404 would obtain no decryption key from the right management unit 406, and thus could not decrypt the encrypted content section layer and accordingly would not render the restricted content section on the terminal device 408.

[0079] In the process 400, the basic content and the content section are rendered together by the document processing unit 404. Accordingly, the right management unit 406 is not required to have the capability of rendering the content section on the terminal device.

[0080] After the basic content and the content section are rendered on the terminal device 408, the document processing service may respond to further operations performed by the user 403 on the terminal device 408. For example, the document processing unit 404 may respond to any user operations on the basic content, and respond to user operations on the content section conforming to the access permission of the user 403.

[0081] It should be understood that all the steps and orders of these steps in the process 400 are exemplary, and the embodiments of the present disclosure may cover various changes to the process 400.

[0082] FIG.5 illustrates a flowchart of an exemplary method 500 for content management of documents according to an embodiment.

[0083] At 510, a request for adding a restricted content to a document may be received from a first terminal device of a first user, the request including the restricted content and a corresponding access permission configuration.

[0084] At 520, a restricted content layer containing the restricted content may be added into the document.

[0085] At 530, a request for accessing the document may be received from a second terminal device of a second user.

[0086] At 540, the document may be sent to the second terminal device.

[0087] At 550, it may be determined whether the second user has an access permission to the restricted content based at least on the access permission configuration.

[0088] At 560, the restricted content contained in the restricted content layer may be rendered on the second terminal device, in response to determining that the second user has the access permission.

[0089] In an implementation, the adding a restricted content layer may comprise: encypting the restricted content layer; and adding the encrypted restricted content layer into the document.

[0090] The rendering the restricted content may comprise: decrypting the encrypted restricted content layer with a decryption key; and rendering the restricted content contained in the decrypted restricted content layer.

[0091] In an implementation, the restricted content may be an annotation.

[0092] The method 500 may further comprise: rendering, on the second terminal device, a basic content in the document independently from the rendering of the restricted content.

[0093] The method 500 may further comprise: presenting the basic content and the restricted content on the second terminal device synchronously.

[0094] In an implementation, the restricted content may be a content section in the document.

[0095] The method 500 may further comprise: rendering, on the second terminal device, a basic content in the document together with the rendering of the restricted content.

[0096] In an implementation, the access permission configuration may specify at least one access permission to the restricted content for at least one another user.

[0097] The determining whether the second user has an access permission may comprise: determining whether the second user is listed in the access permission configuration.

[0098] The at least one access permission may comprise: a permission to view the restricted content, and/or a permission to edit the restricted content.

[0099] In an implementation, the method 500 may further comprise: responding to operations performed on the second terminal device and conforming to the access permission.

[00100] It should be understood that the method 500 may further comprise any steps/processes for content management of documents according to the embodiments of the present disclosure as mentioned above.

[00101] FIG.6 illustrates an exemplary apparatus 600 for content management of documents according to an embodiment.

[00102] The apparatus 600 may comprise: an adding request receiving module 610, for receiving, from a first terminal device of a first user, a request for adding a restricted content to a document, the request including the restricted content and a corresponding access permission configuration; a restricted content layer adding module 620, for adding a restricted content layer containing the restricted content into the document; an accessing request receiving module 630, for receiving, from a second terminal device of a second user, a request for accessing the document; a document sending module 640, for sending the document to the second terminal device; an access permission determining module 650, for determining whether the second user has an access permission to the restricted content based at least on the access permission configuration; and a rendering module 660, for rendering, on the second terminal device, the restricted content contained in the restricted content layer, in response to determining that the second user has the access permission.

[00103] Moreover, the apparatus 600 may also comprise any other modules configured for content management of documents according to the embodiments of the present disclosure as mentioned above.

[00104] FIG.7 illustrates an exemplary apparatus 700 for content management of documents according to an embodiment.

[00105] The apparatus 700 may comprise: at least one processor 710; and a memory 720 storing computer-executable instructions. When executing the computer-executable instructions, the at least one processor 710 may: receive, from a first terminal device of a first user, a request for adding a restricted content to a document, the request including the restricted content and a corresponding access permission configuration; add a restricted content layer containing the restricted content into the document; receive, from a second terminal device of a second user, a request for accessing the document; send the document to the second terminal device; determine whether the second user has an access permission to the restricted content based at least on the access permission configuration; and render, on the second terminal device, the restricted content contained in the restricted content layer, in response to determining that the second user has the access permission.

[00106] In an implementation, the adding a restricted content layer may comprise:

encypting the restricted content layer; and adding the encrypted restricted content layer into the document.

[00107] The rendering the restricted content may comprise: decrypting the encrypted restricted content layer with a decryption key; and rendering the restricted content contained in the decrypted restricted content layer.

[00108] In an implementation, the restricted content may be an annotation.

[00109] The at least one processor 710 may be further for: rendering, on the second terminal device, a basic content in the document independently from the rendering of the restricted content.

[00110] In an implementation, the restricted content may be a content section in the document.

[00111] The at least one processor 710 may be further for: rendering, on the second terminal device, a basic content in the document together with the rendering of the restricted content.

[00112] Moreover, the at least one processor 710 may perform any other operations of the methods for content management of documents according to the embodiments of the present disclosure as mentioned above.

[00113] The embodiments of the present disclosure propose a computer program product for content management of documents. The computer program product may comprise a computer program that is executed by at least one processor for: receiving, from a first terminal device of a first user, a request for adding a restricted content to a document, the request including the restricted content and a corresponding access permission configuration; adding a restricted content layer containing the restricted content into the document; receiving, from a second terminal device of a second user, a request for accessing the document; sending the document to the second terminal device; determining whether the second user has an access permission to the restricted content based at least on the access permission configuration; and rendering, on the second terminal device, the restricted content contained in the restricted content layer, in response to determining that the second user has the access permission. Moreover, the computer program in the computer program product may be further executed by the at least one processor to perform any other operations of the methods for content management of documents according to the embodiments of the present disclosure as mentioned above.

[00114] The embodiments of the present disclosure may be embodied in a non-transitory computer-readable medium. The non-transitory computer-readable medium may comprise instructions that, when executed, cause one or more processors to perform any operations of the methods for content management of documents according to the embodiments of the present disclosure as mentioned above.

[00115] It should be appreciated that all the operations in the methods described above are merely exemplary, and the present disclosure is not limited to any operations in the methods or sequence orders of these operations, and should cover all other equivalents under the same or similar concepts.

[00116] It should also be appreciated that all the modules in the apparatuses described above may be implemented in various approaches. These modules may be implemented as hardware, software, or a combination thereof. Moreover, any of these modules may be further functionally divided into sub-modules or combined together.

[00117] Processors have been described in connection with various apparatuses and methods. These processors may be implemented using electronic hardware, computer software, or any combination thereof. Whether such processors are implemented as hardware or software will depend upon the particular application and overall design constraints imposed on the system. By way of example, a processor, any portion of a processor, or any combination of processors presented in the present disclosure may be implemented with a microprocessor, microcontroller, digital signal processor (DSP), a field-programmable gate array (FPGA), a programmable logic device (PLD), a state machine, gated logic, discrete hardware circuits, and other suitable processing components configured to perform the various functions described throughout the present disclosure. The functionality of a processor, any portion of a processor, or any combination of processors presented in the present disclosure may be implemented with software being executed by a microprocessor, microcontroller, DSP, or other suitable platform.

[00118] Software shall be construed broadly to mean instructions, instruction sets, code, code segments, program code, programs, subprograms, software modules, applications, software applications, software packages, routines, subroutines, objects, threads of execution, procedures, functions, etc. The software may reside on a computer-readable medium. A computer-readable medium may include, by way of example, memory such as a magnetic storage device (e.g., hard disk, floppy disk,

magnetic strip), an optical disk, a smart card, a flash memory device, random access memory (RAM), read only memory (ROM), programmable ROM (PROM), erasable PROM (EPROM), electrically erasable PROM (EEPROM), a register, or a removable disk. Although memory is shown separate from the processors in the various aspects presented throughout the present disclosure, the memory may be internal to the processors, e.g., cache or register.

[00119] Moreover, the articles "a" and "an" as used in this specification and the appended claims should generally be construed to mean "one" or "one or more" unless specified otherwise or clear from the context to be directed to a singular form.

[00120] The previous description is provided to enable any person skilled in the art to practice the various aspects described herein. Various modifications to these aspects will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other aspects. Thus, the claims are not intended to be limited to the aspects shown herein. All structural and functional equivalents to the elements of the various aspects described throughout the present disclosure that are known or later come to be known to those of ordinary skilled in the art are intended to be encompassed by the claims.

WHAT IS CLAIMED IS:

1. A method for content management of documents, comprising:

receiving, from a first terminal device of a first user, a request for adding a restricted content to a document, the request including the restricted content and a corresponding access permission configuration;

adding a restricted content layer containing the restricted content into the document;

receiving, from a second terminal device of a second user, a request for accessing the document;

sending the document to the second terminal device;

determining whether the second user has an access permission to the restricted content based at least on the access permission configuration; and

rendering, on the second terminal device, the restricted content contained in the restricted content layer, in response to determining that the second user has the access permission.

2. The method of claim 1, wherein the adding a restricted content layer comprises:

encypting the restricted content layer; and

adding the encrypted restricted content layer into the document.

3. The method of claim 2, wherein the rendering the restricted content comprises:

decrypting the encrypted restricted content layer with a decryption key; and

rendering the restricted content contained in the decrypted restricted content layer.

4. The method of claim 1, wherein

the restricted content is an annotation.

5. The method of claim 4, further comprising:

rendering, on the second terminal device, a basic content in the document

independently from the rendering of the restricted content.

6. The method of claim 5, further comprising:

presenting the basic content and the restricted content on the second terminal device synchronously.

7. The method of claim 1, wherein

the restricted content is a content section in the document.

8. The method of claim 7, further comprising:

rendering, on the second terminal device, a basic content in the document together with the rendering of the restricted content.

9. The method of claim 1, wherein

the access permission configuration specifies at least one access permission to the restricted content for at least one another user.

10. The method of claim 9, wherein the determining whether the second user has an access permission comprises:

determining whether the second user is listed in the access permission configuration.

11. The method of claim 9, wherein

the at least one access permission comprises: a permission to view the restricted content, and/or a permission to edit the restricted content.

12. The method of claim 1, further comprising:

responding to operations performed on the second terminal device and conforming to the access permission.

13. An apparatus for content management of documents, comprising:

at least one processor; and

a memory storing computer-executable instructions that, when executed, cause

the at least one processor to:

receive, from a first terminal device of a first user, a request for adding a restricted content to a document, the request including the restricted content and a corresponding access permission configuration,

add a restricted content layer containing the restricted content into the document,

receive, from a second terminal device of a second user, a request for accessing the document,

send the document to the second terminal device,

determine whether the second user has an access permission to the restricted content based at least on the access permission configuration, and

render, on the second terminal device, the restricted content contained in the restricted content layer, in response to determining that the second user has the access permission.

14. The apparatus of claim 13, wherein the adding a restricted content layer comprises:

encypting the restricted content layer; and

adding the encrypted restricted content layer into the document.

15. The apparatus of claim 14, wherein the rendering the restricted content comprises:

decrypting the encrypted restricted content layer with a decryption key; and

rendering the restricted content contained in the decrypted restricted content layer.

16. The apparatus of claim 13, wherein

the restricted content is an annotation.

17. The apparatus of claim 16, wherein the at least one processor is further for:

rendering, on the second terminal device, a basic content in the document independently from the rendering of the restricted content.

18. The apparatus of claim 13, wherein

the restricted content is a content section in the document.

19. The apparatus of claim 18, wherein the at least one processor is further for:

rendering, on the second terminal device, a basic content in the document together with the rendering of the restricted content.

20. A computer program product for content management of documents, the computer program product comprising a computer program that is executed by at least one processor for:

receiving, from a first terminal device of a first user, a request for adding a restricted content to a document, the request including the restricted content and a corresponding access permission configuration;

adding a restricted content layer containing the restricted content into the document;

receiving, from a second terminal device of a second user, a request for accessing the document;

sending the document to the second terminal device;

determining whether the second user has an access permission to the restricted content based at least on the access permission configuration; and

rendering, on the second terminal device, the restricted content contained in the restricted content layer, in response to determining that the second user has the access permission.

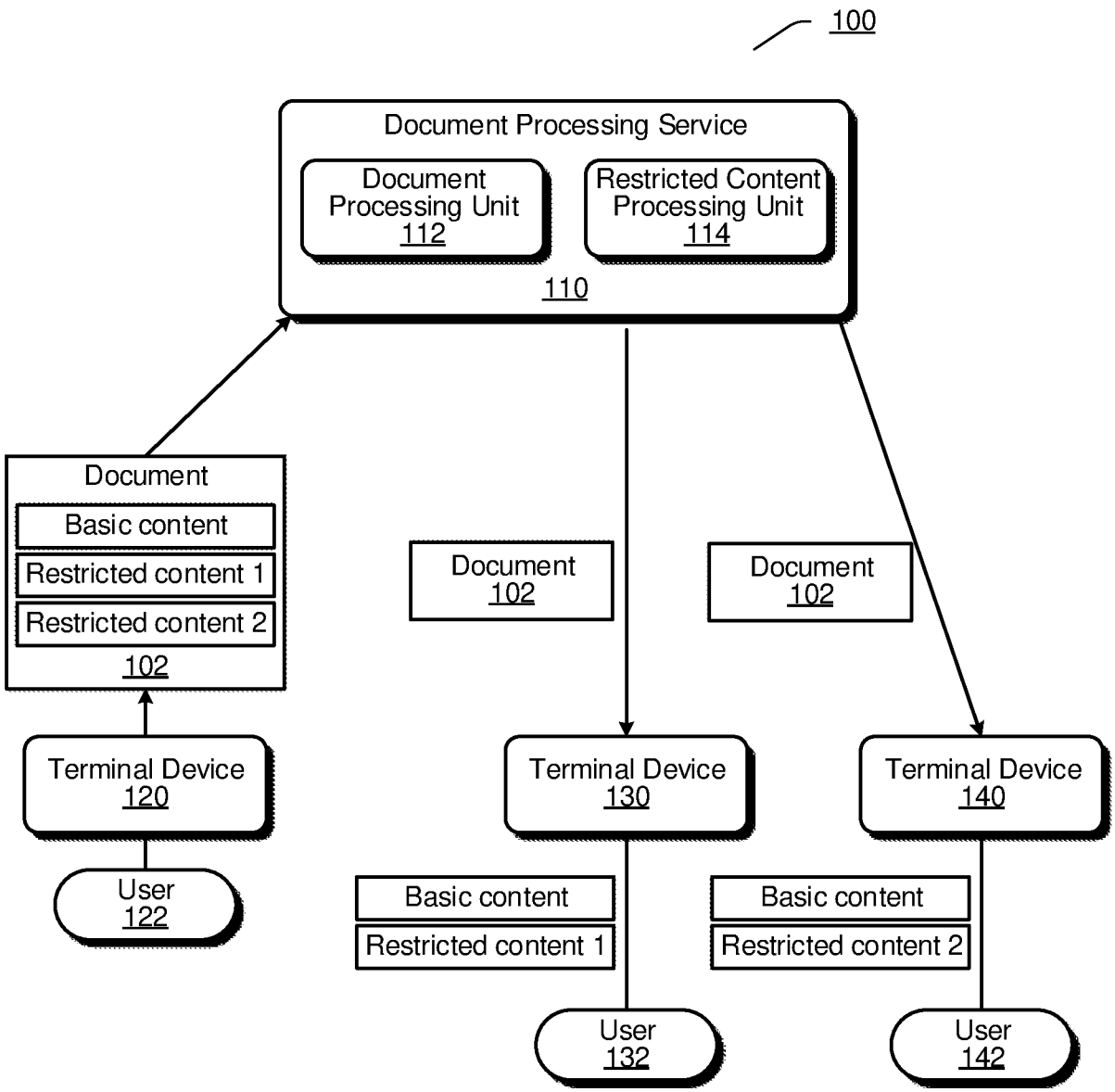
100
Document Processing Service
Document Processing Unit 112
Restricted Content Processing Unit 114
110
Document
Basic content
Restricted content 1
Restricted content 2
102
Document 102
Document 102
Terminal Device 120
Terminal Device 130
Terminal Device 140
User 122
Basic content
Restricted content 1
Basic content
Restricted content 2
User 132
User 142

FIG 1

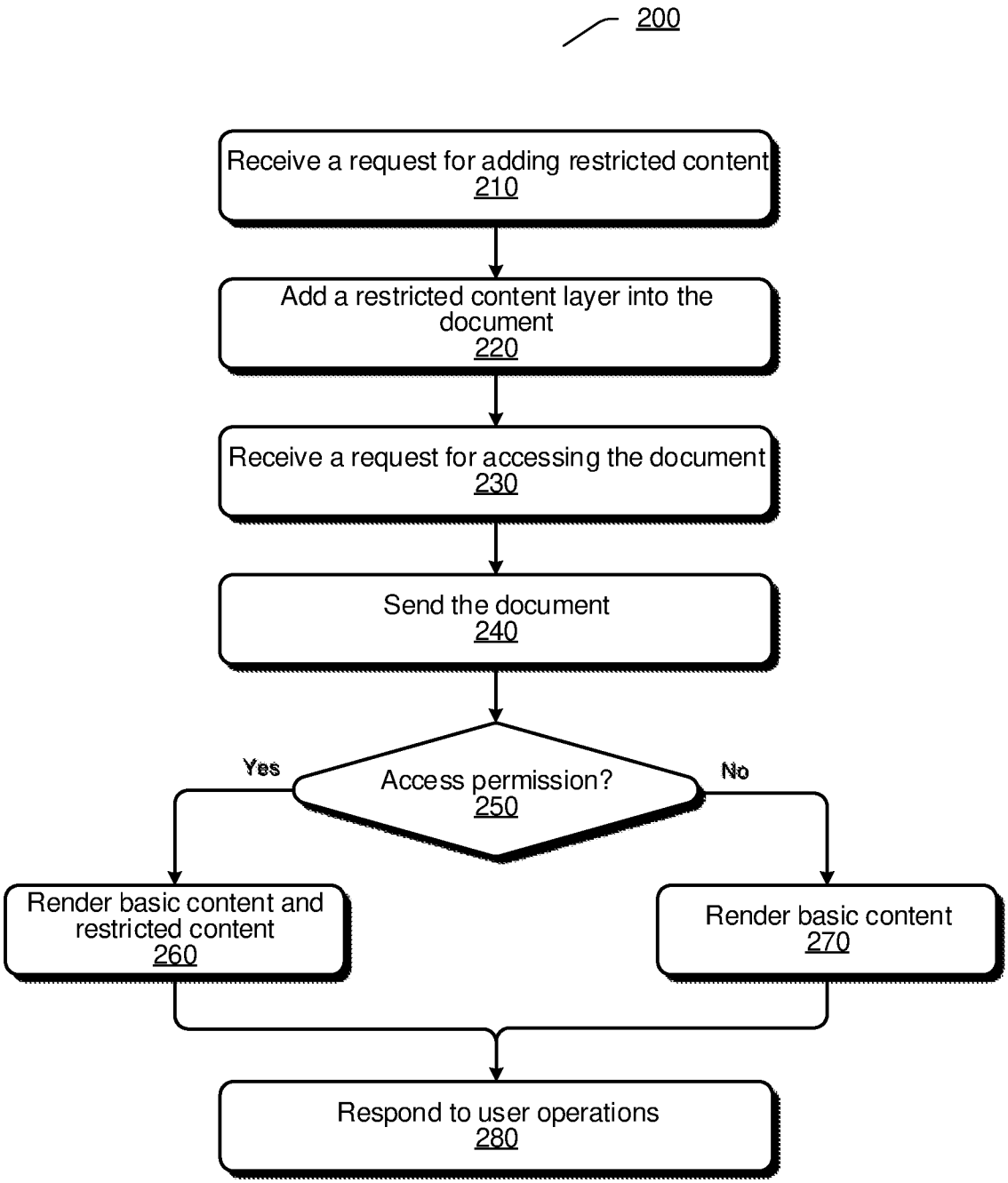
200
Receive a request for adding restricted content
210
Add a restricted content layer into the document
220
Receive a request for accessing the document
230
Send the document
240
Access permission?
250
Yes
No
Render basic content and restricted content
260
Render basic content
270
Respond to user operations
280

FIG 2

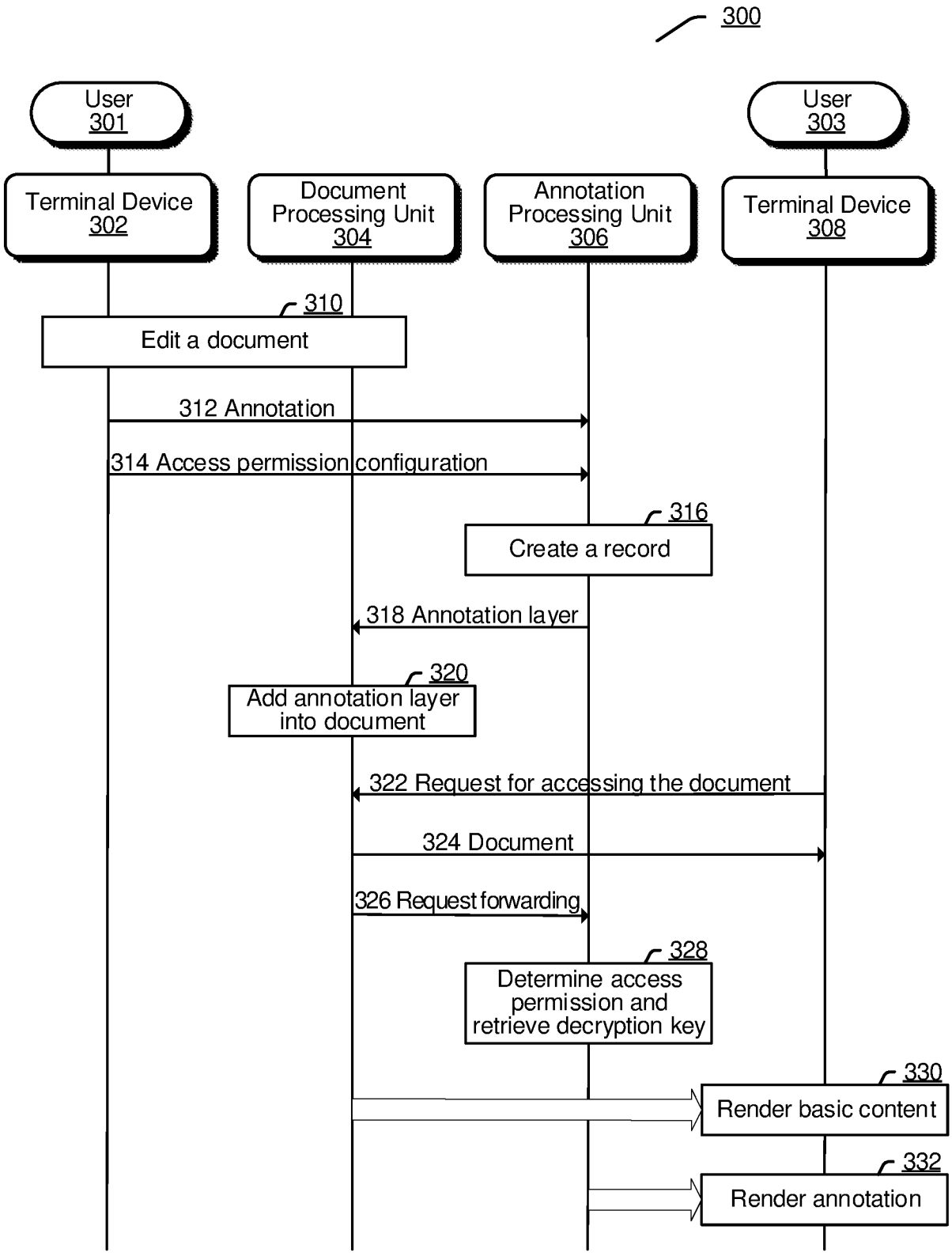
300
User 301
Terminal Device 302
Document Processing Unit 304
Annotation Processing Unit 306
User 303
Terminal Device 308
310
Edit a document
312 Annotation
314 Access permission configuration
316
Create a record
318 Annotation layer
320
Add annotation layer into document
322 Request for accessing the document
324 Document
326 Request forwarding
328
Determine access permission and retrieve decryption key
330
Render basic content
332
Render annotation

FIG 3

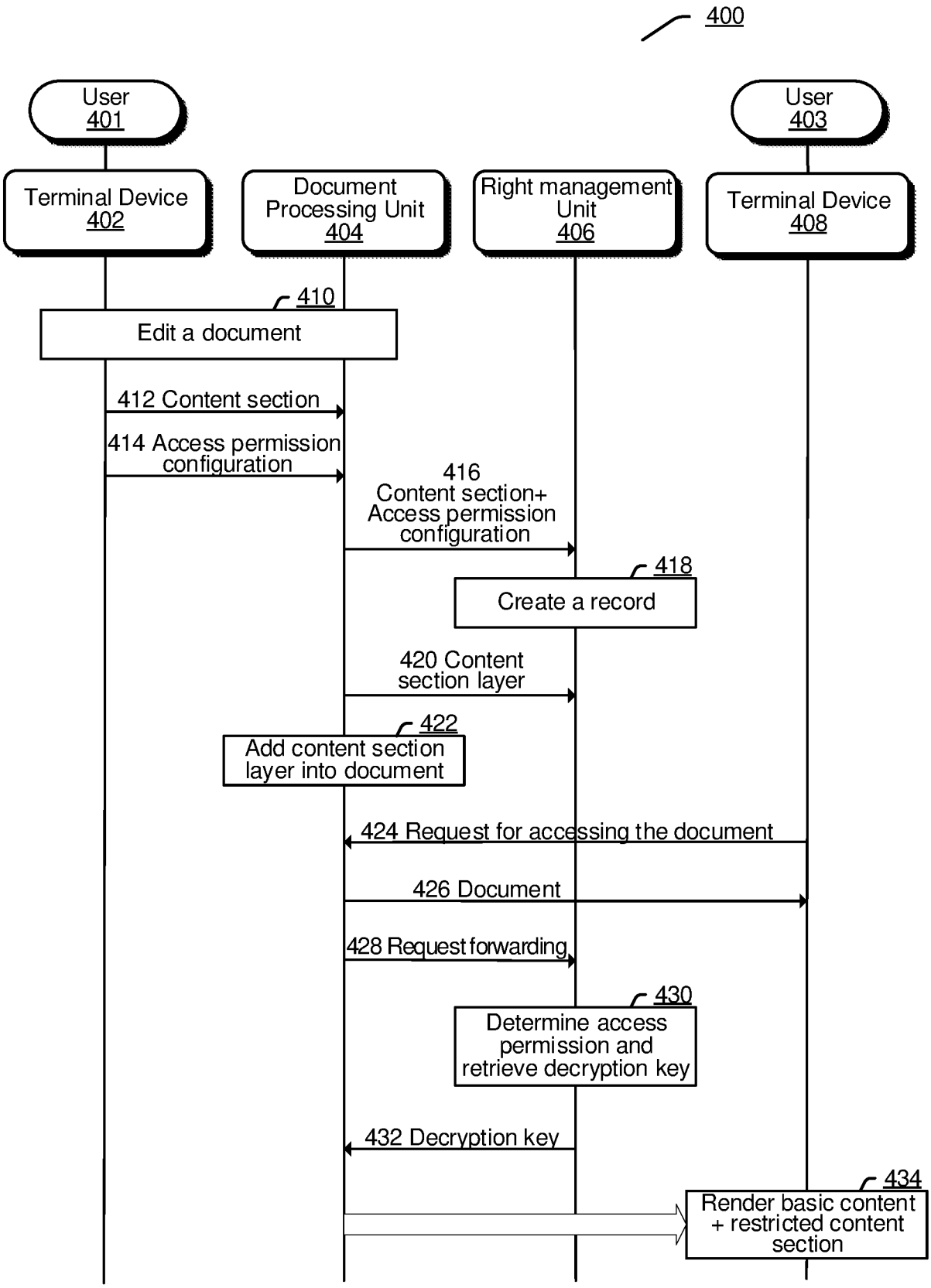
400
User 401
Terminal Device 402
Document Processing Unit 404
Right management Unit 406
User 403
Terminal Device 408
410
Edit a document
412 Content section
414 Access permission configuration
416 Content section+ Access permission configuration
418
Create a record
420 Content section layer
422
Add content section layer into document
424 Request for accessing the document
426 Document
428 Request forwarding
430
Determine access permission and retrieve decryption key
432 Decryption key
434
Render basic content + restricted content section

FIG 4

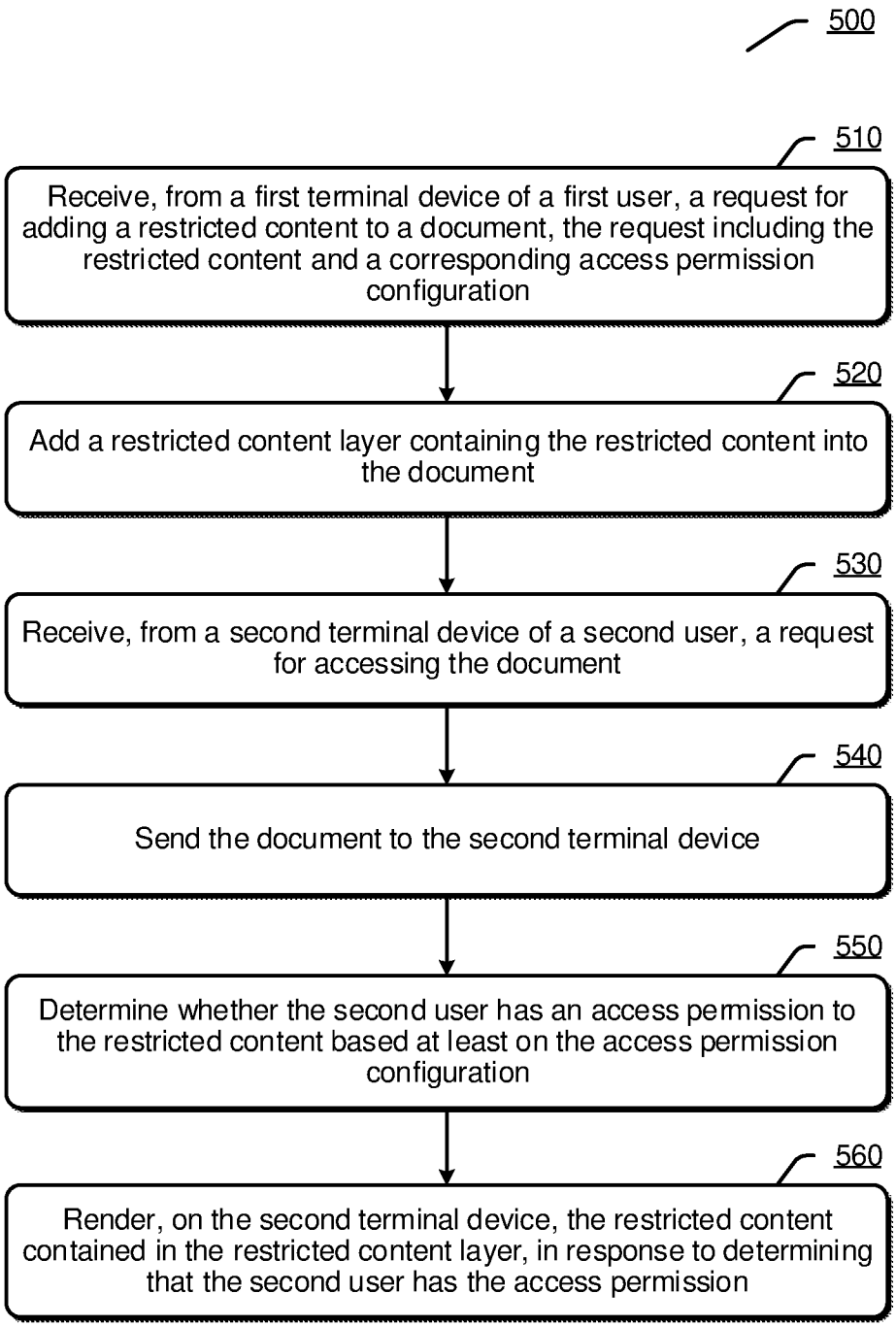
500
510
Receive, from a first terminal device of a first user, a request for adding a restricted content to a document, the request including the restricted content and a corresponding access permission configuration
520
Add a restricted content layer containing the restricted content into the document
530
Receive, from a second terminal device of a second user, a request for accessing the document
540
Send the document to the second terminal device
550
Determine whether the second user has an access permission to the restricted content based at least on the access permission configuration
560
Render, on the second terminal device, the restricted content contained in the restricted content layer, in response to determining that the second user has the access permission

FIG 5

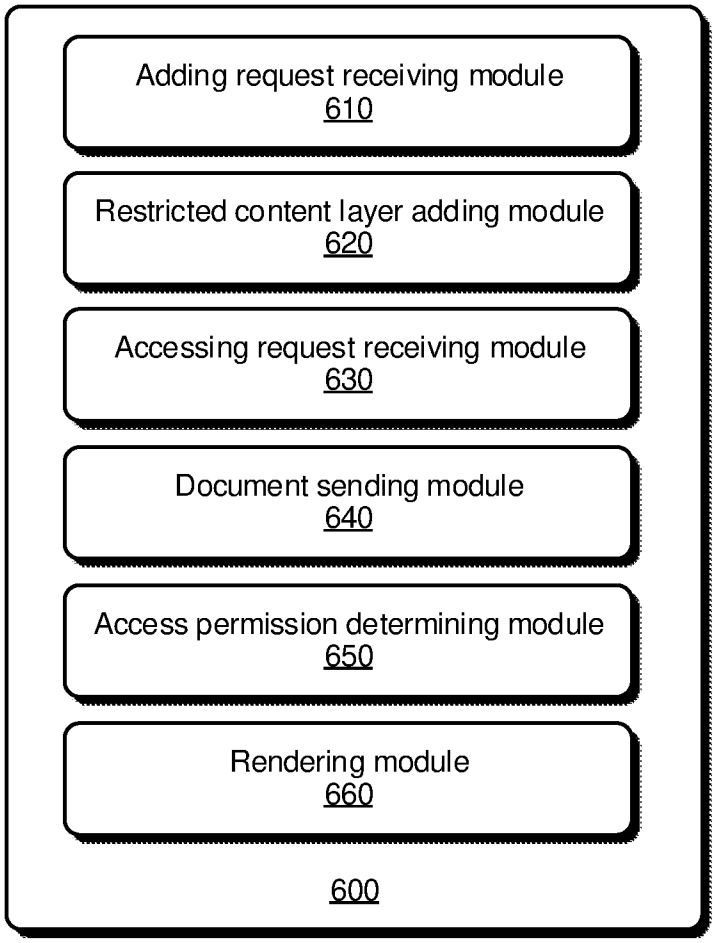
Adding request receiving module
610
Restricted content layer adding module
620
Accessing request receiving module
630
Document sending module
640
Access permission determining module
650
Rendering module
660
600

FIG 6

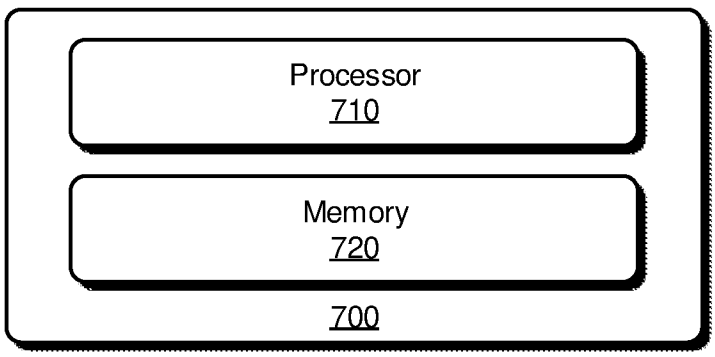
Processor
710
Memory
720
700

FIG 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/CN2021/095746

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/62
ADD.

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

B. FIELDS SEARCHED

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

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/099947 A1 (EVANS WILLIAM D [US]) 25 July 2002 (2002-07-25) paragraphs [0001], [0006] - [0008], [0014] - [0018], [0026], [0057], [0058], [0079] - [0080], [0096] - [0120] -----	1-20
X A	US 2020/265112 A1 (FOX SETH [US] ET AL) 20 August 2020 (2020-08-20) paragraphs [0001], [0002], [0028] - [0032], [0039] - [0057], [0064] - [0072]; claims 1-7, 10-14 -----	1,4-13, 16-20 2,3,14, 15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

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

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

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

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

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 November 2021	15/11/2021

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Winkelbauer, Andreas

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/CN2021/095746

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002099947 A1	25-07-2002	CA 2367778 A1	19-07-2002
		DE 60200616 T2	04-11-2004
		EP 1225500 A2	24-07-2002
		JP 4336078 B2	30-09-2009
		JP 2002278844 A	27-09-2002
		US 2002099947 A1	25-07-2002
US 2020265112 A1	20-08-2020	CN 113454633 A	28-09-2021
		EP 3908959 A1	17-11-2021
		US 2020265112 A1	20-08-2020
		WO 2020171960 A1	27-08-2020