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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
06 January 2022 (06.01.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/005609 A1

(51) International Patent Classification:
G06F 21/16 (2013.01) *G06Q 30/00* (2012.01)

(21) International Application Number:
PCT/US2021/031464

(22) International Filing Date:
10 May 2021 (10.05.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
202010611319.3 29 June 2020 (29.06.2020) CN

(71) Applicant: **MICROSOFT TECHNOLOGY LICENSING, LLC** [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(72) Inventors: **ZHANG, Xian**; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). **GUO, Xiaobing**; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). **CHEN, Yang**; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). **CHEN, Shuo**; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). **GUO, Zhongxin**; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). **YIN, Qiufeng**; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). **YANG, Mao**; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). **ZHOU, Lidong**;

(54) **Title:** THIRD PARTY BASED PIRATED COPY TRACING

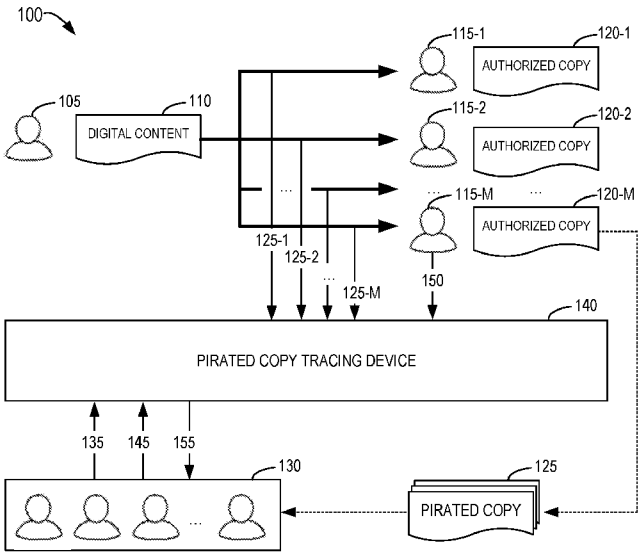

FIG. 1

(57) **Abstract:** According to implementations of the subject matter described herein, a solution is provided for pirated copy tracing based on a third party. In the solution, a report on a pirated copy of a digital content is received from a third party, wherein the report comprises first secret information for characterizing a first identification, time information and tracing information of the pirated copy. Subsequently, a request for verifying the report is received to determine whether the report is valid. When the report is determined as valid, a licensee associated with the report is marked as a first status to indicate that the pirated copy might be leaked by the licensee. Therefore, the pirated copy may be effectively traced based on third parties. The tracing information in the report can be hidden, and other third parties can therefore be prevented from using the tracing information for duplicate reports.

WO 2022/005609 A1

[Continued on next page]

MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US).

(74) **Agent: SWAIN, Cassandra T.** et al.; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US).

(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:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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

THIRD PARTY BASED PIRATED COPY TRACING

BACKGROUND

[0001] The rapid development of the network has provided tremendous convenience for information exchange, and has also brought severe challenges to the protection of digital content (also referred to as "digital assets"). Piracy and illegal use of digital content have caused huge economic losses to content owners of digital content.

[0002] With the development of computer technology, watermarking technology has been gradually applied so as to protect the copyright of digital content. By identifying watermark information carried in digital content, it is possible to distinguish illegally copied and/or pirated digital content. However, due to characteristics of Internet dissemination, it is difficult for content owners to fully monitor whether their owned digital content are illegally pirated. Therefore, how to effectively trace pirated copies of digital content has become a focus.

SUMMARY

[0003] According to implementations of the subject matter described herein, a solution is provided for third party based pirated copy tracing. In the solution, a report on a pirated copy of a digital content is received from a third party, wherein the report comprises first secret information for characterizing a first identification, time information and tracing information of the pirated copy. Subsequently, a request for verifying the report is received for determining whether the report is valid. When the report is determined as valid, a licensee associated with the report is marked as a first status for indicating that the pirated copy might be leaked by the licensee. Therefore, the pirated copy may be effectively traced with the third parties. Besides, the tracing information in the report can be hidden, and other third parties can therefore be prevented from using the tracing information for duplicate reports.

[0004] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary 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.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] Fig. 1 illustrates a block diagram of a computing environment which can implement a plurality of implementations of the subject matter described herein;

[0006] Fig. 2 illustrates a flowchart of an example process of tracing a pirated copy

according to some implementations of the subject matter described herein;

[0007] Fig. 3 illustrates a flowchart of an example procedure of offering an incentive to a third party according to some implementations of the subject matter described herein;

[0008] Fig. 4 illustrates a flowchart of an example process of a licensee making an appeal according to some implementations of the subject matter described herein; and

[0009] Fig. 5 illustrates a block diagram of an example computing device according to some implementations of the subject matter described herein.

[0010] Throughout the drawings, the same or similar reference signs refer to the same or similar elements.

DETAILED DESCRIPTION

[0011] The subject matter described herein will now be discussed with reference to several example implementations. It is to be understood these implementations are discussed only for the purpose of enabling persons skilled in the art to better understand and thus implement the subject matter described herein, rather than suggesting any limitations on the scope of the subject matter.

[0012] As used herein, the term "includes" and its variants are to be read as open terms that mean "includes, but is not limited to." The term "based on" is to be read as "based at least in part on." The term "one implementation" and "an implementation" are to be read as "at least one implementation." The term "another implementation" is to be read as "at least one other implementation." The terms "first," "second," and the like may refer to different or same objects. Other definitions, explicit and implicit, may be included below.

[0013] As discussed above, how to effectively trace pirated copies is one of core issues in copyright protection of digital content. Some traditional solutions require a content owner to detect copies on the network for determining whether there is illegal piracy of digital content. However, such an approach requires a large computation cost for the content owner, and the detection might not be thorough.

[0014] Other traditional solutions trace pirated copies of digital content by collecting third-party reports. However, on the one hand, such reports might not be transparent, and third parties might therefore not trust such a reporting mechanism and further lack motivation to report pirated copies. On the other hand, some content owners encourage third parties to report pirated copies by offering incentives to third parties. However, if such reports are transparent, then obviously other third parties may obtain details of reports. Some other third parties might use revealed reports to resubmit reports of pirated copies for obtaining inappropriate incentives. This will cause an unnecessary loss to content owners.

[0015] According to implementations of the subject matter described herein, a solution is provided for third party based pirated copy tracing. In the solution, a report on a pirated copy of a digital content is received from a third party, wherein the report comprises first secret information for characterizing a first identification, time information and tracing information (e.g., watermark information) of a pirated copy. For example, the first secret information may be determined through irreversible hash operations so that other third party cannot directly obtain the tracing information.

[0016] Subsequently, a request for verifying the report is received, so as to determine whether the report is valid. The request comprises second secret information and a second identification of the third party, wherein the second secret information is used to characterize the tracing information and the time information. It may be determined based on the received report and the request whether the report is valid, so that it may prevent other third parties from using the disclosed first secret information for a duplicate report. When it is determined that the report is valid, a licensee associated with the report is marked as a first status, so as to indicate that the pirated copy might be leaked by the licensee. Thus, the pirated copy may be effectively traced based on third parties. Further, the tracking information in the report can be hidden, and other third parties can be prevented from using the tracing information for a duplicate report.

[0017] Illustration is presented below to basic principles and several example implementations of the subject matter described herein with reference to the drawings.

Example Environment

[0018] Fig. 1 illustrates a block diagram of an environment 100 in which a plurality of implementations of the subject matter described herein can be implemented. It should be understood that the environment 100 shown in Fig. 1 is only exemplary and shall not constitute any limitation on the functions and scope of the implementations described by the subject matter described herein.

[0019] As shown in Fig. 1, the computing environment 100 includes a content owner 105, which is an owner of a digital content 110. The content owner 105 may be any individual, organization or institution, etc. The digital content 110 is any type of digital asset owned by the content owner 105, such as an image, a video, an audio, a document, a model, a software, etc. The subject matter described herein is not intended to limit the form of the digital content 110.

[0020] As shown in Fig. 1, the digital content 110 is shared to a plurality of licensees 115-1, 115-2 ... 115-M (individually or collectively referred to as licensee 115). In order

to facilitate tracing of a pirated copy, different tracing information (e.g., watermark) is added to the digital content 110 to thereby form a plurality of authorized copies 120-1, 120-2 ... 120-M (individually or collectively referred to as authorized copy 120). As shown in Fig. 1, each licensee 115 will own a corresponding authorized copy 120.

[0021] In some implementations, to subsequently determine which licensee leaks the pirated copy, transmission evidences 125-1, 125-2 ... 125-M (individually or collectively referred to as transmission evidence 125) characterizing that the authorized copy 120 is shared to the corresponding licensee 115 may be stored to a pirated copy tracing device 140.

[0022] In some implementations, to prevent the content owner 105 from maliciously framing a certain licensee 115 for leaking the corresponding authorized copy 120, the authorized copy 120 may be shared based on an oblivious transfer (OT) protocol. Accordingly, the corresponding transmission evidence 125 may comprise an OT evidence generated by the OT protocol.

[0023] During transmission based on the OT protocol, each licensee 115 will be provided with a plurality of candidate copies, and one candidate copy will be randomly selected by the licensee 115 as the authorized copy 120. In this way, the content owner 105 will be unable to know which copy is selected by the licensee 115.

[0024] As discussed above, without knowledge of the content owner 105, some licensees 115 might intentionally or unintentionally leak the authorized copy 120, thereby forming a spreading pirated copy 125. For example, without authorization, a certain authorized copy 120-M might be leaked and appear on a certain unauthorized forum for users to download. A copy on the forum for users to download will be referred to as the pirated copy 125.

[0025] As shown in Fig. 1, one or more third parties 130 might obtain the pirated copy 125. For some consideration, some third parties 130 may provide reports on the pirated copy 125 to the pirated copy tracing device 140. In some implementations, the content owner 105 may, for example, offer an incentive to a third party 130 who provides a valid report on the pirated copy 125, thereby encouraging the third parties 130 to report the obtained pirated copy 125 to the pirated copy tracing device 140.

[0026] According to implementations of the subject matter described herein, the third party 130 may first provide a report 135 on the pirated copy 125 to the pirated copy tracing device 140, and then in a subsequent appropriate time period submit a request 145 for verifying the report 135. After the report 135 is determined as valid by the pirated copy tracing device 140, the licensee 115 associated with the report 135 may be marked as possibly leaking the corresponding pirated copy 125. In some implementations, to

motivate more third parties to proactively report pirated copies, the content owner 105 may offer to the third party 130 an incentive 155 corresponding to the report 135 through the pirated copy tracing device 140.

[0027] In some implementations, the pirated copy tracing device 140 may further receive an appeal request 150 from a doubted licensee 115. For example, the pirated copy tracing device 140 may use the maintained transmission evidence 125 to prove the authorized copy 120 actually obtained by the licensee 115, and then determine whether the licensee 115 is a leaker of the pirated copy 125 based on a comparison between the authorized copy 120 and the pirated copy 125.

[0028] It should be understood although the pirated copy tracing device 140 is shown as a separate box in Fig. 1, the pirated copy tracing device 140 may comprise an independent device or a group of devices connected via a network. In one example implementation of the subject matter described herein, the pirated copy tracing device 140 may comprise one or more nodes deployed on a blockchain (e.g., a public blockchain or a consortium blockchain).

[0029] A detailed discussion is presented below of example implementations of pirated copy tracing.

Tracing of Pirated Copy

[0030] Fig. 2 shows a flowchart of a process 200 of tracing a pirated copy according to some implementations of the subject matter described herein. The process 200 may be implemented by, for example, the pirated copy tracing device 140 in Fig. 1.

[0031] At 202, the pirated copy tracing device 140 receives, from a third party 130, a report 135 on a pirated copy 125 of a digital content 110, wherein the report 135 comprises first secret information, and the first secret information is for characterizing a first identification, time information and tracing information of the pirated copy 125. The time information indicates a creation time of the first secret information. The pirated copy 125 is a leaked copy of an authorized copy 120 of the digital content which is authorized to a licensee 115 by a content owner 105.

[0032] As discussed above, a third party 130 may obtain the pirated copy 125 in some cases. In some implementations, the third party 130 may extract the tracing information in the pirated copy 125 and may then generate the first secret information based on the tracing information. As an example, the tracing information may comprise watermark information included in the pirated copy 125, wherein the watermark information was added when the digital content 110 was shared by the content owner 105 to the licensee 115.

[0033] In some implementations, to prevent the tracing information from being leaked, during generating the report 135, the third party 130 may combine the tracing information and the time information and then perform a hash operation on the combined data to obtain a first hash value. Further, the third party 130 may combine the first hash value and identification of the third party and then perform a hash operation on the combined data to obtain a second hash value. The second hash value may be used as the first secret information.

[0034] In one example, the first secret information may be formulated as Formula (1):

$$\mathcal{H}(\mathcal{H}(id_{xy}||T)||pk_i^I) \quad (1)$$

wherein cm_1 denotes the first secret information, $\mathcal{H}$ denotes a hash operation, $||$ denotes linking two data, id_{xy} denotes the tracing information, T denotes the time information, and pk_i^I denotes the identification of the third party.

[0035] In some implementations, the time information T may be represented as a time period when the first secret information is created. Specifically, after the digital content 110 is shared, the content owner 105 may, for example, set a specific time window to allow for receiving reports from the third party 130 on the pirated copy 125 of the digital content 110.

[0036] In some implementations, the time window may further be divided into a plurality of time periods, and the time information T may represent a serial number of the time period during which the first secret information is created. For example, if the first secret information is created within the second time period, then the time information T may be determined as a value "2."

[0037] In some implementations, when generating the report 135, the third party 130 may further obtain a first index indicating the licensee 115 associated with the pirated copy 125 and a second index indicating the authorized copy 120 corresponding to the licensee 115 among a plurality of versions provided to the licensee 115. Specifically, the third party 130 may, for example, send the hash value of the tracing information to the content owner 105 so as to query the first index and the second index according to the tracing information.

[0038] In some implementations, the content owner 105 may maintain a hash table so as to indicate mapping relations among hash values of tracing information of different authorized copies 120, index values of corresponding licensees 115 and index values of authorized copies 120. By querying the hash table, the content owner 105 may return the first index and the second index corresponding to the tracing information in the pirated copy

125. As an example, the first index and the second index may be, for example, be included in the report 135 in plain text.

[0039] As an example, the report 135 may be formulated as Formula (2):

$$cm = (cm_1, cm_2, cm_3) = (\mathcal{H}(\mathcal{H}(id_{xy}||T)||pk_i^I), x, y) \quad (2)$$

wherein cm denotes a report, which comprises a tuple (cm_1, cm_2, cm_3), and x and y denote the first index and the second index, respectively.

[0040] In some implementations, the pirated copy tracing device 140 may store the report 135 in a report list (e.g., represented as CMList_T) associated with a time period when the report 135 is received. In some implementations, to guarantee the transparency of the report, the pirated copy tracing device 140 may be a node deployed on a blockchain (e.g., a public blockchain or a consortium blockchain). The pirated copy tracing device 140 may maintain relevant information of the report 135 on the blockchain, so as to make the first secret information, the first index and the second index included in the report be available from the blockchain.

[0041] By storing the report 135 on the blockchain, the implementations of the subject matter described herein may reduce the risk that the report 135 sent by the third party 130 will be maliciously modified, thereby increasing the accuracy of pirated copy tracing. In addition, by using the tracing information, the time information and the identification to generate the first secret information, the implementations of the subject matter described herein may prevent the tracing information or the hash value thereof from being directly exposed to other third parties, thereby further preventing other third parties from maliciously generating a fake report by using the tracing information included in the report.

[0042] At 204, the pirated copy tracing device 140 receives a request 145 for verifying the report 135, wherein the request 145 comprises second secret information and a second identification of the third party 130, and the second secret information is for characterizing the tracing information and the time information.

[0043] In some implementations, the third party may submit the request 145 for verifying the report 135 to the pirated copy tracing device 140 in a predetermined time after sending the report 135. Specifically, as discussed above, the time window allowing for receiving the report from the third party 130 on the pirated copy 125 of the digital content 110 may be divided into a plurality of time periods. In some implementations, the third party 130 may send the request 145 in a time period after sending the report 135. Unlike the traditional approach of verifying the report after the expiration of the time window, by

verifying the report 135 in time, the implementations of the subject matter described herein may provide a verification result of the report 135 to the third party in time. In addition, this can facilitate offering a timely incentive to the third party 130, so as to encourage the third party 13 to proactively report a pirated copy of the digital content.

[0044] In some implementations, to prevent other third parties from maliciously generating a fake report by using the disclosed report 135, the third party 130 may include the second secret information and the identification of the third party 130 in the request 145. As an example, the second secret information may be a hash value resulting from a hash operation on the combination of the tracing information and the time information. For example, the second secret information rv_1 may be formulated as Formula (3):

$$rv_1=\mathcal{H}(id_{xy}||T) \tag{3}$$

Definitions of respective elements in Formula (3) may refer to Formulas (1) and (2).

[0045] In some implementations, the request 145 may further comprise path information, which indicates corresponding paths of the above first index, second index and event information in a Merk tree maintained by the content owner 105.

[0046] Specifically, in the data sharing phase, the content owner 105 may construct a Merk tree, wherein each licensee 115 comprises a plurality of nodes as shown by Formula (4).

$$\mathcal{H}(\mathcal{H}(id_{ij}||1)||i||j),\ldots,\mathcal{H}(\mathcal{H}(id_{ij}||K)||i||j) \tag{4}$$

wherein K denotes the number of time periods included in the time window, i denotes the index information of the licensee 115, j denotes the index information of the corresponding authorized copy 120 among N copies provided to the licensee 115.

[0047] In some implementations, when generating the report 135, the content owner 105 may further use the first index x, the second index y and the time information T to query the Merk tree so as to determine a path Path_{xyT} corresponding to x, y and T and then send the path to the third party 130. Accordingly, the path may be included in the request 145. As an example, the request 145 may be formulated as Formula (5):

$$rv=(rv_1,rv_2,rv_3)=(\mathcal{H}(id_{xy}||T),\text{Path}_{xyT},pk_i^I) \tag{5}$$

wherein rv denotes the request 145, which comprises a tuple (rv_1,rv_2,rv_3), id_{xy} denotes the tracing information, and pk_i^I denotes the identification of the third party.

[0048] At 206, the pirated copy tracing device 140 determines whether report is valid according to the first secret information, the second secret information and the second identification.

[0049] In some implementations, the pirated copy tracing device 140 may determine whether the second identification included in the request 145 matches the identification of the third party who sends the request 145.

[0050] As discussed above, the pirated copy tracing device may be a node deployed on a blockchain. Therefore, the reports and requests sent by other third parties are transparent and available to all nodes and users on the blockchain.

[0051] On the one hand, some malicious third parties might directly copy content of a disclosed report and request which are verified from another third party and then submit the content as a new report and request. Accordingly, the pirated copy tracing device 140 may determine that plaintext identification included in the request fails to match the identification of the third party 130 sending the request, and further identify the report as invalid.

[0052] On the other hand, since the identification included in the request is plaintext information, some malicious third parties might replace identification in a previous request with their own identification. That is, a malicious third party might construct a new report 135 by copying the contents of a previous report and construct a new request 145 by replacing the identification in the corresponding request.

[0053] In some implementations, the pirated copy tracing device 140 may determine whether the second secret information and the second identification included in the request 145 match the first secret information included in the report 135, so as to determine whether the report 135 is valid.

[0054] Specifically, the pirated copy tracing device 140 may generate third secret information according to the second secret information and the identification. For example, the third secret information may be represented as $\mathcal{H}(rv_1||rv_3)$, wherein definitions of rv_1 and rv_3 may refer to Formula (5).

[0055] Subsequently, if the first secret information matches the third secret information, then the pirated copy tracing device 140 may determine the report 135 as valid. On the contrary, the pirated copy tracing device 140 may determine the report 135 as invalid.

[0056] In some implementations, the pirated copy tracing device 140 may compare, based on a time period (e.g., T+1) when the request 145 is received, the third secret information with a first element in a tuple in a report list (e.g., CMList_T) associated with a previous time period (e.g., T), so as to determine whether there is the first secret information matching the third secret information. As an example, if the report list includes the first secret information which match the third secret information, the pirated copy tracing device 140 may determine the report 135 as valid. On the contrary, the first secret information

which match the third secret information are not present in the list, then the pirated copy tracing device 140 may determine the report 135 as invalid.

[0057] Regarding the above cases where identification is replaced to construct the new malicious request 145, the pirated copy tracing device 140 may determine that the third secret information constructed based on the request 145 fail to match the first secret information included in the report 135, thereby identifying the report 135 as invalid.

[0058] Based on such an approach, the implementations of the subject matter described herein, under the premise that the report and request are transparent to the blockchain, can effectively identify a request and report faked by other third parties using a published request and report and further protect rights and interests of the content owner and licensee.

[0059] In some implementations, if the request 145 further comprises the path $Path_{xyT}$, then the pirated copy tracing device 140 may further query whether the path $Path_{xyT}$ indicates a valid path in the Merk tree maintained by the content owner 105. If the path $Path_{xyT}$ fails to indicate a valid path, then the pirated copy tracing device 140 may determine the report 135 as invalid. As an example, the Merk tree may be stored on the blockchain.

[0060] Further, if the path $Path_{xyT}$ indicates a valid path in the Merk tree, then the pirated copy tracing device 140 may, for example, further determine whether $\mathcal{H}(\mathcal{H}(rv_1)||x||y)$ is included in the corresponding path, wherein rv_1, x and y are information included in the report 135. If it is determined that $\mathcal{H}(\mathcal{H}(rv_1)||x||y)$ is not included in the corresponding path, then the pirated copy tracing device 140 may determine the report 135 as invalid. By using the Merk tree to maintain hash values corresponding to the tracing information, the first index, the second index and the time information, the embodiments of the subject matter described herein may further improve the security of the verification procedure of the report 135.

[0061] At 208, if the report 135 is determined as valid, the pirated copy tracing device 140 will mark the licensee 115 associated with the report 135 as a first status, which indicates the pirated copy might be leaked by the licensee.

[0062] For example, regarding the example in Fig. 1, the pirated copy 125 is associated with the licensee 115-M. If the report 135 is determined as valid, then the pirated copy tracing device 140 may, for example, mark the licensee 115-M as the first status.

[0063] With the above discussed method, the embodiments of the subject matter described herein achieve effective tracing of a pirated copy based on third parties. In addition, with the method of verification using a report and request, the embodiments of the subject matter described herein can further prevent fake reports being constructed using

disclosed reports and requests by malicious third parties.

Incentive for Third Parties

[0064] The example procedure of pirated copy tracing according to the implementations of the subject matter described herein has been described above. In some implementations, if the report 135 is determined as valid, the pirated copy tracing device 140 may offer an incentive 155 corresponding to the report 135 to the third party 130. It should be understood that the incentive 155 may comprise any appropriate type of incentive, and the subject matter described herein is not intended to be limiting in this regard.

[0065] Some existing solutions offer equal incentives to reports 135 on the same pirated copy 125. As a result, the same third party will use the same pirated copy 125 to submit duplicate reports in multiple time periods by changing its identity, for obtaining multiple incentives. This will damage interests of the content owner and make it impossible to accurately estimate the number of pirated copies leaked by licensees.

[0066] In order to prevent the same third party from submitting duplicate reports on the same pirated copy 125 by modifying its identity, the pirated copy tracing device 140 may dynamically adjust an incentive available to the same pirated copy 125.

[0067] Specifically, an incentive for the third party 130 whose report 135 is verified as valid may be formulated as:

$$B(I_i, n) = -\xi_i + \sum_{j=i+1}^{n} \xi_j + c * 2^{-n+1} \tag{6}$$

wherein $B(I_i, n)$ denotes an incentive for the *i*-th third party to submit a report among *n* third parties who successfully submit reports, wherein $\{\xi_i\} \in \mathbb{R}^*_{\geq 0}$, $0 \leq \xi_i \leq 2 * \xi_{i+1} \leq c * 2^{-i+1}$, and $\xi_1 = 0$.

[0068] Based on such an approach, the incentive determined by the subject matter described herein may ensure that a total incentive obtained through repetitively submitting a report is less than an incentive obtained by submitting a report only once. In this way, it could effectively prevent a third party from repetitively reporting a duplicate report by modifying its identity.

[0069] Unlike the traditional approach of making statistics and offering incentives after the time window, to encourage the third party to submit a report, the implementations of the subject matter described herein may divide the incentive into two portions, wherein a first portion may be offered in a time period when the report is determined as valid, and a second portion may be offered after the time window expires.

[0070] Description is presented below to a detailed process of providing an incentive with reference to Fig. 3. Figure 3 shows a flowchart of an example process 300 of offering an incentive to a third party according to implementations of the subject matter described herein.

[0071] As shown in Fig. 3, at 302, if the report 135 is determined as valid, the pirated copy tracing device 140 may offer a first incentive corresponding to the report to the third party in a second time period, wherein the first incentive is determined based on the number of third parties who have submitted valid reports on the pirated copy before the report. The first incentive may be formulated as:

$$B_1(i) = 2 * \sum_{j=i}^{\infty} \Delta_j \tag{7}$$

wherein $\{\Delta_i\} \in \mathbb{R}^*_{\geq 0}$, and $\xi_{i+1} = \frac{1}{2}\xi_i + \Delta_i$. For the definition of ξ_i, reference may be made to Formula (6).

[0072] At 304, after the time window expires, the pirated copy tracing device 140 may offer a second incentive corresponding to the report to the third party, wherein the second incentive is determined based on the number of third parties who have submitted valid reports on the pirated copy within the time window.

[0073] Accordingly, according to Formula (6), the pirated copy tracing device 140 may determine a total incentive which the third party is supposed to get, according to the number *n* of third parties who have submitted valid reports on the pirated copy within the time window and an order *i* in which the third party 130 submits the report. Subsequently, the pirated copy tracing device 140 may determine the second incentive to be offered, according to the total incentive and the first incentive determined by Formula (7).

[0074] In this way, the embodiments of the subject matter described herein may ensure that: (1) a report submitted earlier may be offered a larger incentive; (2) an incentive may be offered to the third party in time; (3) and an incentive for a repetitively submitted report will reduce.

Appeal of Licensee

[0075] In some implementations, after the licensee 115 is marked as a first status, the pirated copy tracing device 140 may further receive an appeal request 150 from the licensee 115.

[0076] In some implementations, the licensee 115 may submit the appeal request 150 to the pirated copy tracing device 140 within a predetermined time. If no appeal request 150

on the report 135 is received from the licensee 115 within the predetermined time after receipt of the report 135, the pirated copy tracing device 140 may mark the licensee 115 as a second status, which indicates that the pirated copy 125 is leaked by the licensee 115.

[0077] As discussed above, the authorized copy 120 is sent by the content owner 105 to the licensee 115 through an oblivious transfer OT protocol. In some implementations, the OT evidence 125 corresponding to the transfer may be maintained at the pirated copy tracing device 140. Specifically, the OT evidence 125 may be maintained on the blockchain to prevent it from being illegally tampered with by the third parties and thereby guarantee the accuracy of pirated copy tracing.

[0078] A flowchart of an example process 400 of appealing by the licensee according to some implementations of the subject matter described herein will be described in conjunction with Fig. 4.

[0079] As shown in Fig. 4, at 402, the pirated copy tracing device 140 may receive the appeal request 150 on the report 135 from the licensee 115, wherein the appeal request 150 comprises the OT evidence jointly signed by the content owner 105 and the licensee 115, a local random number for determining the OT evidence as maintained by the licensee 115, and a local index of the authorized copy as maintained by the licensee 115.

[0080] Specifically, the OT evidence may be formulated as:

$$R = P_l - r \cdot G \tag{8}$$

wherein, R denotes the OT evidence, $\{P_1, \ldots, P_N\} \in \mathbb{G}^N$, r is a random number determined by the licensee 115, l indicates an index of the authorized copy among N candidate copies provided to the licensee 115, $l \in [N]$, and N denotes the number of copies provided to the licensee 115. It should be understood that the OT evidence is generated based on OT protocol transfer data. Details about the OT protocol will not be detailed here.

[0081] Accordingly, the appeal request 150 may be represented as a tuple $((\mathrm{Sig}_*(R), r, l))$, wherein $\mathrm{Sig}_*(R)$ denotes the OT evidence signed with private keys of the content owner 105 and the licensee 115, respectively.

[0082] At 404, if the OT evidence matches the random number and the local index and that local index is different from an index indicated by the tracing information in the report, then the pirated copy tracing device 140 may mark the licensee 115 as a third status, wherein the third status indicates that the licensee is irrelevant to the pirated copy 125.

[0083] Specifically, the pirated copy tracing device 140 may determine whether Formula

(9) is satisfied or not:

$$P_l - r \cdot G = R \tag{9}$$

If Formula (9) is satisfied, then the pirated copy tracing device 140 may further compare l with l_x, wherein l_x indicates the index indicated by the tracing information. If $l \neq l_x$, then the pirated copy tracing device 140 may determine that the appeal of the licensee 115 succeeds, and further mark the licensee 115 as irrelevant to the pirated copy 125.

[0084] On the contrary, if Formula (9) is not satisfied, or $l = l_x$, then the pirated copy tracing device 140 may determine that the appeal of the licensee 115 fails.

[0085] In some implementations, if the licensee 115 is marked as the first status within a predetermined time after the report 135 is received, then the pirated copy tracing device 140 may mark the licensee 115 as a second status, wherein the second status indicates that the pirated copy 125 is leaked by the licensee 115.

[0086] Unlike the traditional OT-based appeal process, the implementations of the subject matter described herein do not need to re-transmit transfer vectors (e.g., $\{E_1, \ldots, E_N\}$) associated with N candidate copies provided to the licensee. Only the above mentioned tuple is needed to be provided during the appeal procedure. Therefore, the complexity of the appeal may be reduced from O(N) to O(1), thereby greatly reducing network overheads and computation overheads required for the appeal.

Example Device

[0087] Fig. 5 shows a schematic block diagram of an example device 500 which is applicable to implement the embodiments of the subject matter described herein. The device 500 may be used to implement the pirated copy tracing device 140 of Fig. 1. It should be understood that the device 500 shown in Fig. 5 is merely exemplary and should not form any limitation on the functions and scope of the implementations of the subject matter described herein. As shown in Fig. 1, components of the device 500 may include, without limitation to, one or more processors or processing units 510, a memory 520, a storage device 530, one or more communication units 540, one or more input devices 550, and one or more output devices 560.

[0088] In some implementations, the device 500 may be implemented as various user terminals or service terminals. The service terminals may be servers, large-scale computing devices, and the like provided by a variety of service providers. The user terminal, for example, is a mobile terminal, a fixed terminal or a portable terminal of any type, including a mobile phone, a multimedia computer, a multimedia tablet, Internet nodes,

a communicator, a desktop computer, a laptop computer, a notebook computer, a netbook computer, a tablet computer, a Personal Communication System (PCS) device, a personal navigation device, a Personal Digital Assistant (PDA), an audio/video player, a digital camera/video, a positioning device, a television receiver, a radio broadcast receiver, an electronic book device, a gaming device or any other combination thereof consisting of accessories and peripherals of these devices or any other combination thereof. It may also be predicted that the device 500 can support any type of user-specific interface (such as a "wearable" circuit, and the like).

[0089] The processing unit 510 may be a physical or virtual processor and may execute various processing based on the programs stored in the memory 520. In a multi-processor system, a plurality of processing units executes computer-executable instructions in parallel to enhance parallel processing capability of the device 500. The processing unit 510 can also be known as a central processing unit (CPU), microprocessor, controller and microcontroller.

[0090] The device 500 usually includes a plurality of computer storage mediums. Such mediums may be any attainable medium accessible by the computing device 102, including but not limited to, a volatile and non-volatile medium, a removable and non-removable medium. The memory 520 may be a volatile memory (e.g., a register, a cache, a Random Access Memory (RAM)), a non-volatile memory (such as, a Read-Only Memory (ROM), an Electrically Erasable Programmable Read-Only Memory (EEPROM), flash), or any combination thereof. The memory 520 may include one or more pirated copy tracing modules 522, which are configured to perform various functions described herein. The pirated copy tracing module 522 may be accessed and operated by the processing unit 510 to realize corresponding functions. The storage device 530 may be a removable or non-removable medium, and may include a machine-readable medium (e.g., a memory, a flash drive, a magnetic disk) or any other medium, which may be used for storing information and/or data and be accessed within the device 500.

[0091] Functions of components of the device 500 may be realized by a single computing cluster or a plurality of computing machines, and these computing machines may communicate through communication connections. Therefore, the device 500 may operate in a networked environment using a logic connection to one or more other servers, a Personal Computer (PC) or a further general network node. The device 500 may also communicate through the communication unit 540 with one or more external devices (not shown) as required, where the external device, e.g., a data base 570, a further storage device,

a server, a display device, and so on, communicates with one or more devices that enable users to interact with the device 500, or with any device (such as a network card, a modem, and the like) that enable the device 500 to communicate with one or more other computing devices. Such communication may be executed via an Input/Output (I/O) interface (not shown).

[0092] The input device 550 may be one or more various input devices, such as a mouse, a keyboard, a trackball, a voice-input device, and the like. The output device 560 may be one or more output devices, e.g., a display, a loudspeaker, a printer, and so on.

[0093] The device 500 may include a pirated copy tracing module 522 configured to: receive a report on a pirated copy of a digital content from a third party, the report comprising first secret information, the first secret information being used for characterizing first identification, time information and tracing information of the pirated copy, the time information indicating a creation time of the first secret information, the pirated copy being a leaked version of an authorized copy of the digital content which is authorized by a content owner to a licensee; receive a request for verifying the report, the request comprising second secret information and second identification of the third party, the second secret information being used for characterizing the tracing information and the time information; determine whether the report is valid according to the first secret information, the second secret information and the second identification; and if the report is determined as valid, mark a licensee associated with the report as first status, the first status indicating that the pirated copy might be leaked by the licensee.

Example Implementations

[0094] Some example implementations of the subject matter described herein are listed below.

[0095] In a first aspect, the subject matter described herein provides a computer-implemented method. The method comprises: receiving, from a third party, a report on a pirated copy of a digital content, the report comprising first secret information for characterizing a first identification, time information and tracing information of the pirated copy, the time information indicating a creation time of the first secret information, the pirated copy being a leaked version of an authorized copy of the digital content which is authorized by a content owner to a licensee; receiving a request for verifying the report, the request comprising second secret information and a second identification of the third party, the second secret characterizing the tracing information and the time information; determining whether the report is valid according to the first secret information, the second

secret information and the second identification; and if the report is determined as valid, marking a licensee associated with the report as a first status, the first status indicating that the pirated copy might be leaked by the licensee.

[0096] In some implementations, the first secret information is a second hash value determined based on the first identification and a first hash value, the first hash value being determined based on the tracing information and the time information.

[0097] In some implementations, determining whether the report is valid according to the first secret information, the second secret information and the second identification comprises: generating third secret information according to the second secret information and the second identification; and if the first secret information matches the third secret information, determining that the report is valid.

[0098] In some implementations, the method further comprises: if an appeal request on the report fails to be received from the licensee within a predetermined time after receipt of the report, marking the licensee as a second status, the second status indicating that the pirated copy is leaked by the licensee.

[0099] In some implementations, the authorized copy is sent by the content owner to the licensee through an oblivious transfer OT protocol, the method further comprising: receiving an appeal request on the report from the licensee, the appeal request comprising an OT evidence jointly signed by the content owner and the licensee, a local random number for determining the OT evidence as maintained by the licensee, and a local index of the authorized copy as maintained by the licensee; and if the OT evidence fails to match the random number and the local index and the local index is different from an index indicated by the tracing information in the report, marking the licensee as a third status, the third status indicating that the licensee has nothing to do with the pirated copy.

[00100] In some implementations, the method further comprises: maintaining the first secret information and the OT evidence on a blockchain, so as to make the first secret information and the OT evidence be available from the blockchain.

[00101] In some implementations, a time window for receiving a report on a pirated copy is divided into a plurality of time periods, and receiving a request for verifying the report comprises: receiving a request for verifying the report in a second time period of the plurality of time periods neighboring a first time period for receiving the report.

[00102] In some implementations, the method further comprises: if the report is determined as valid, offering to the third party a first incentive corresponding to the report in the second time period, the first incentive being determined based on a number of third

parties who have submitted valid reports on the pirated copy before the report; and after the time window expires, offering to the third party a second incentive corresponding to the report, the second incentive being determined based on a number of third parties who have submitted valid reports on the pirated copy within the time window.

[00103] In a second aspect, a device is provided. The device comprises: a processing unit; and a memory, coupled to the processing unit and having instruction stored thereon, the instructions, when executed by the processing unit, causing the device to perform acts, comprising: receiving, from a third party, a report on a pirated copy of a digital content, the report comprising first secret information for characterizing a first identification, time information and tracing information of the pirated copy, the time information indicating a creation time of the first secret information, the pirated copy being a leaked version of an authorized copy of the digital content which is authorized by a content owner to a licensee; receiving a request for verifying the report, the request comprising second secret information and a second identification of the third party, the second secret characterizing the tracing information and the time information; determining whether the report is valid according to the first secret information, the second secret information and the second identification; and if the report is determined as valid, marking a licensee associated with the report as a first status, the first status indicating that the pirated copy might be leaked by the licensee.

[00104] In some implementations, the first secret information is a second hash value determined based on the first identification and a first hash value, the first hash value being determined based on the tracing information and the time information.

[00105] In some implementations, determining whether the report is valid according to the first secret information, the second secret information and the second identification comprises: generating third secret information according to the second secret information and the second identification; and if the first secret information matches the third secret information, determining that the report is valid.

[00106] In some implementations, the acts further comprise: if an appeal request on the report fails to be received from the licensee within a predetermined time after receipt of the report, marking the licensee as a second status, the second status indicating that the pirated copy is leaked by the licensee.

[00107] In some implementations, the authorized copy is sent by the content owner to the licensee through an oblivious transfer OT protocol, the acts further comprising: receiving an appeal request on the report from the licensee, the appeal request comprising an OT

evidence jointly signed by the content owner and the licensee, a local random number for determining the OT evidence as maintained by the licensee, and a local index of the authorized copy as maintained by the licensee; and if the OT evidence fails to match the random number and the local index and the local index is different from an index indicated by the tracing information in the report, marking the licensee as a third status, the third status indicating that the licensee has nothing to do with the pirated copy.

[00108] In some implementations, the acts further comprise: maintaining the first secret information and the OT evidence on a blockchain, so as to make the first secret information and the OT evidence be available from the blockchain.

[00109] In some implementations, a time window for receiving a report on a pirated copy is divided into a plurality of time periods, and receiving a request for verifying the report comprises: receiving a request for verifying the report in a second time period of the plurality of time periods neighboring a first time period for receiving the report.

[00110] In some implementations, the acts further comprise: if the report is determined as valid, offering to the third party a first incentive corresponding to the report in the second time period, the first incentive being determined based on a number of third parties who have submitted valid reports on the pirated copy before the report; and after the time window expires, offering to the third party a second incentive corresponding to the report, the second incentive being determined based on a number of third parties who have submitted valid reports on the pirated copy within the time window.

[00111] In a third aspect, a computer program product is provided. The computer program product is tangibly stored in a non-transitory computer storage medium and comprises machine-executable instructions which, when executed by a device, cause the device to perform acts, comprising: receiving, from a third party, a report on a pirated copy of a digital content, the report comprising first secret information for characterizing a first identification, time information and tracing information of the pirated copy, the time information indicating a creation time of the first secret information, the pirated copy being a leaked version of an authorized copy of the digital content which is authorized by a content owner to a licensee; receiving a request for verifying the report, the request comprising second secret information and a second identification of the third party, the second secret characterizing the tracing information and the time information; determining whether the report is valid according to the first secret information, the second secret information and the second identification; and if the report is determined as valid, marking a licensee associated with the report as a first status, the first status indicating that the pirated copy

might be leaked by the licensee.

[00112] In some implementations, the first secret information is a second hash value determined based on the first identification and a first hash value, the first hash value being determined based on the tracing information and the time information.

[00113] In some implementations, determining whether the report is valid according to the first secret information, the second secret information and the second identification comprises: generating third secret information according to the second secret information and the second identification; and if the first secret information matches the third secret information, determining that the report is valid.

[00114] In some implementations, the acts further comprise: if an appeal request on the report fails to be received from the licensee within a predetermined time after receipt of the report, marking the licensee as a second status, the second status indicating that the pirated copy is leaked by the licensee.

[00115] In some implementations, the authorized copy is sent by the content owner to the licensee through an oblivious transfer OT protocol, the acts further comprising: receiving an appeal request on the report from the licensee, the appeal request comprising an OT evidence jointly signed by the content owner and the licensee, a local random number for determining the OT evidence as maintained by the licensee, and a local index of the authorized copy as maintained by the licensee; and if the OT evidence fails to match the random number and the local index and the local index is different from an index indicated by the tracing information in the report, marking the licensee as a third status, the third status indicating that the licensee has nothing to do with the pirated copy

[00116] In some implementations, the acts further comprise: maintaining the first secret information and the OT evidence on a blockchain, so as to make the first secret information and the OT evidence be available from the blockchain.

[00117] In some implementations, a time window for receiving a report on a pirated copy is divided into a plurality of time periods, and receiving a request for verifying the report comprises: receiving a request for verifying the report in a second time period of the plurality of time periods neighboring a first time period for receiving the report.

[00118] In some implementations, the acts further comprise: if the report is determined as valid, offering to the third party a first incentive corresponding to the report in the second time period, the first incentive being determined based on a number of third parties who have submitted valid reports on the pirated copy before the report; and after the time window expires, offering to the third party a second incentive corresponding to the report, the second

incentive being determined based on a number of third parties who have submitted valid reports on the pirated copy within the time window.

[00119] The functionality described herein can be performed, at least in part, by one or more hardware logic components. For example, and without limitation, illustrative types of hardware logic components that can be used include Field-Programmable Gate Arrays (FPGAs), Application-specific Integrated Circuits (ASICs), Application-specific Standard Products (ASSPs), System-on-a-chip systems (SOCs), Complex Programmable Logic Devices (CPLDs), and the like.

[00120] Program code for carrying out methods of the subject matter described herein may be written in any combination of one or more programming languages. These program codes may be provided to a processor or controller of a general purpose computer, a special purpose computer, or other programmable data processing apparatuses, such that the program codes, when executed by the processor or controller, cause the functions/operations specified in the flowcharts and/or block diagrams to be implemented. The program code may execute entirely on a machine, partly on the machine, as a stand-alone software package, partly on the machine and partly on a remote machine or entirely on the remote machine or a server.

[00121] In the context of this subject matter described herein, a machine-readable medium may be any tangible medium that may contain, or store a program for use by or in connection with an instruction execution system, apparatus, or device. The machine-readable medium may be a machine-readable signal medium or a machine-readable storage medium. A machine-readable medium may include, but is not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples of the machine-readable storage medium would include an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of the foregoing.

[00122] Further, although operations are depicted in a particular order, it should be understood that the operations are required to be executed in the particular order shown or in a sequential order, or all operations shown are required to be executed to achieve the expected results. In certain circumstances, multitasking and parallel processing may be advantageous. Likewise, while several specific implementation details are contained in

the above discussions, these should not be construed as limitations on the scope of the subject matter described herein. Certain features that are described in the context of separate implementations may also be implemented in combination in a single implementation. Conversely, various features that are described in the context of a single implementation may also be implemented in multiple implementations separately or in any suitable sub-combination.

[00123] Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter specified in the appended claims is not necessarily limited to the specific features or acts described above. Rather, the specific features and acts described above are disclosed as example forms of implementing the claims.

CLAIMS

1. A computer-implemented method, comprising:

receiving, from a third party, a report on a pirated copy of a digital content, the report comprising first secret information for characterizing a first identification, time information and tracing information of the pirated copy, the time information indicating a creation time of the first secret information, the pirated copy being a leaked version of an authorized copy of the digital content which is authorized by a content owner to a licensee;

receiving a request for verifying the report, the request comprising second secret information and a second identification of the third party, the second secret information characterizing the tracing information and the time information;

determining whether the report is valid according to the first secret information, the second secret information and the second identification; and

if the report is determined as valid, marking a licensee associated with the report as a first status, the first status indicating that the pirated copy might be leaked by the licensee.

2. The method of claim 1, wherein the first secret information is a second hash value determined based on the first identification and a first hash value, the first hash value being determined based on the tracing information and the time information.

3. The method of claim 1, wherein determining whether the report is valid according to the first secret information, the second secret information and the second identification comprises:

generating third secret information according to the second secret information and the second identification; and

if the first secret information matches the third secret information, determining that the report is valid.

4. The method of claim 1, further comprising:

if an appeal request on the report fails to be received from the licensee within a predetermined time after receipt of the report, marking the licensee as a second status, the second status indicating that the pirated copy is leaked by the licensee.

5. The method of claim 1, wherein the authorized copy is sent by the content owner to the licensee through an oblivious transfer OT protocol, the method further comprising:

receiving an appeal request on the report from the licensee, the appeal request comprising an OT evidence jointly signed by the content owner and the licensee, a local random number for determining the OT evidence as maintained by the licensee, and a local

index of the authorized copy as maintained by the licensee; and

if the OT evidence fails to match the random number and the local index and the local index is different from an index indicated by the tracing information in the report, marking the licensee as a third status, the third status indicating that the licensee has nothing to do with the pirated copy.

6. The method of claim 3, further comprising:

maintaining the first secret information and the OT evidence on a blockchain, so as to make the first secret information and the OT evidence be available from the blockchain.

7. The method of claim 1, wherein a time window for receiving a report on a pirated copy is divided into a plurality of time periods, and wherein receiving a request for verifying the report comprises:

receiving a request for verifying the report in a second time period of the plurality of time periods neighboring a first time period for receiving the report.

8. The method of claim 7, further comprising:

if the report is determined as valid, offering to the third party a first incentive corresponding to the report in the second time period, the first incentive being determined based on a number of third parties who have submitted valid reports on the pirated copy before the report; and

after the time window expires, offering to the third party a second incentive corresponding to the report, the second incentive being determined based on a number of third parties who have submitted valid reports on the pirated copy within the time window.

9. A device, comprising:

a processing unit; and

a memory coupled to the processing unit and having instructions stored thereon which, when executed by the processing unit, cause the device to perform acts comprising:

receiving, from a third party, a report on a pirated copy of a digital content, the report comprising first secret information for characterizing a first identification, time information and tracing information of the pirated copy, the time information indicating a creation time of the first secret information, the pirated copy being a leaked version of an authorized copy of the digital content which is authorized by a content owner to a licensee;

receiving a request for verifying the report, the request comprising second secret information and a second identification of the third party, the second secret information characterizing the tracing information and the time information;

determining whether the report is valid according to the first secret information,

the second secret information and the second identification; and

if the report is determined as valid, marking a licensee associated with the report as a first status, the first status indicating that the pirated copy might be leaked by the licensee.

10. The device of claim 9, wherein the first secret information is a second hash value determined based on the first identification and a first hash value, the first hash value being determined based on the tracing information and the time information.

11. The device of claim 9, wherein determining whether the report is valid according to the first secret information, the second secret information and the second identification comprises:

generating third secret information according to the second secret information and the second identification; and

if the first secret information matches the third secret information, determining that the report is valid.

12. The device of claim 9, the acts further comprising:

if an appeal request on the report fails to be received from the licensee within a predetermined time after receipt of the report, marking the licensee as a second status, the second status indicating that the pirated copy is leaked by the licensee.

13. The device of claim 9, wherein the authorized copy is sent by the content owner to the licensee through an oblivious transfer OT protocol, the acts further comprising:

receiving an appeal request on the report from the licensee, the appeal request comprising an OT evidence jointly signed by the content owner and the licensee, a local random number for determining the OT evidence as maintained by the licensee, and a local index of the authorized copy as maintained by the licensee; and

if the OT evidence fails to match the random number and the local index and the local index is different from an index indicated by the tracing information in the report, marking the licensee as a third status, the third status indicating that the licensee has nothing to do with the pirated copy.

14. The device of claim 13, the acts further comprising:

maintaining the first secret information and the OT evidence on a blockchain, so as to make the first secret information and the OT evidence be available from the blockchain.

15. A computer program product being tangibly stored in a computer storage medium and comprising machine-executable instructions which, when executed by a device, cause the device to perform acts comprising:

receiving, from a third party, a report on a pirated copy of a digital content, the report comprising first secret information for characterizing a first identification, time information and tracing information of the pirated copy, the time information indicating a creation time of the first secret information, the pirated copy being a leaked version of an authorized copy of the digital content which is authorized by a content owner to a licensee;

receiving a request for verifying the report, the request comprising second secret information and a second identification of the third party, the second secret information characterizing the tracing information and the time information;

determining whether the report is valid according to the first secret information, the second secret information and the second identification; and

if the report is determined as valid, marking a licensee associated with the report as a first status, the first status indicating that the pirated copy might be leaked by the licensee.

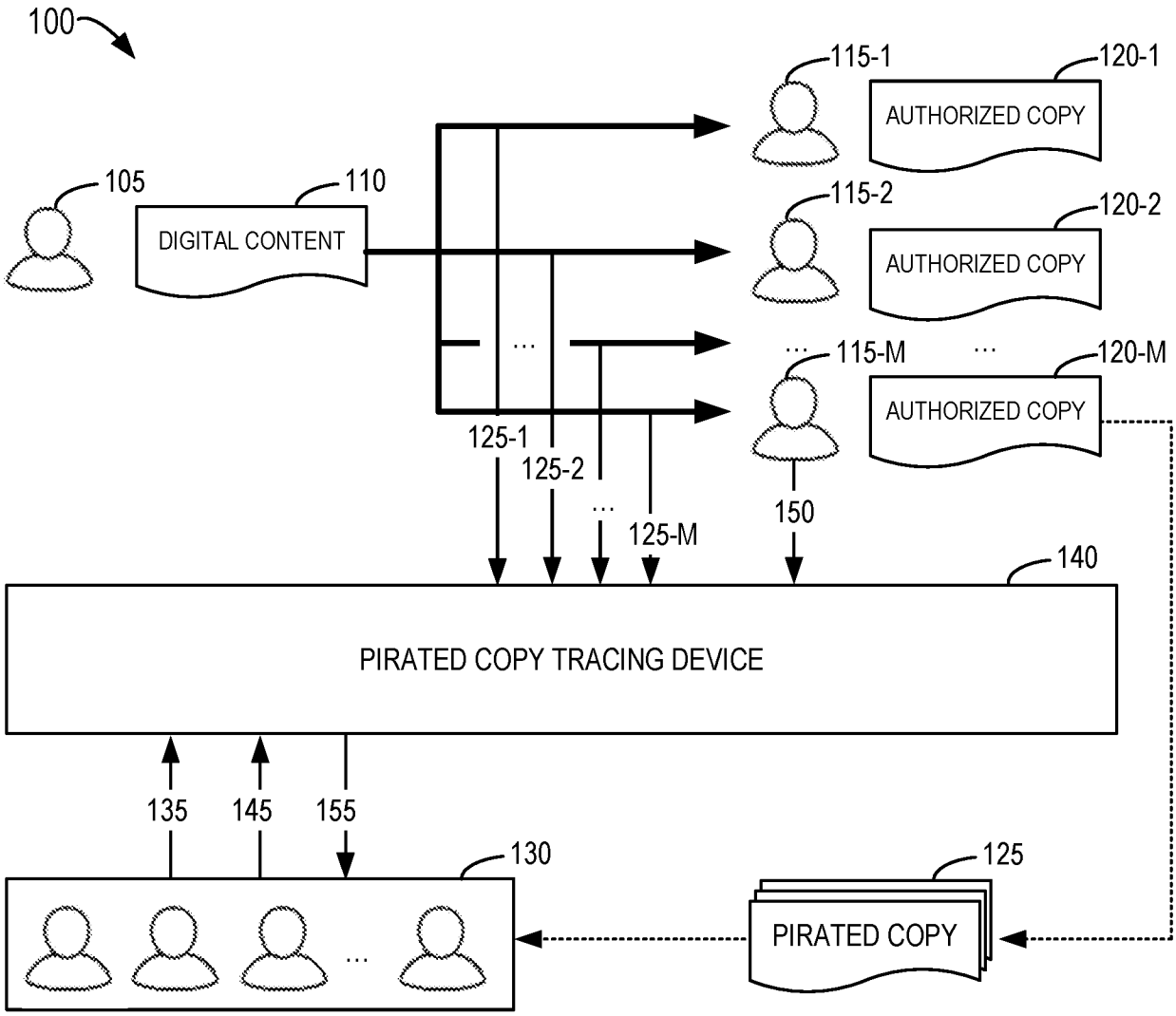
100
105
110
DIGITAL CONTENT
115-1
120-1
AUTHORIZED COPY
115-2
120-2
AUTHORIZED COPY
115-M
120-M
AUTHORIZED COPY
125-1
125-2
125-M
150
140
PIRATED COPY TRACING DEVICE
135
145
155
130
125
PIRATED COPY

FIG. 1

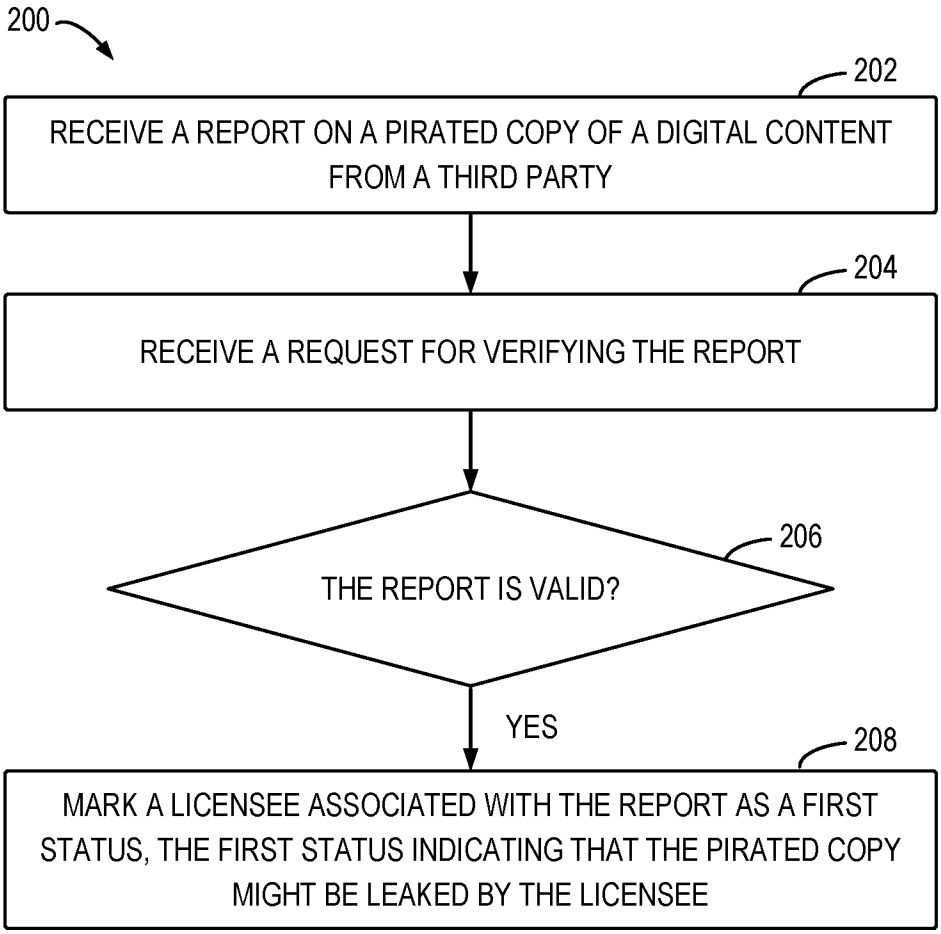
200
202
RECEIVE A REPORT ON A PIRATED COPY OF A DIGITAL CONTENT FROM A THIRD PARTY
204
RECEIVE A REQUEST FOR VERIFYING THE REPORT
206
THE REPORT IS VALID?
YES
208
MARK A LICENSEE ASSOCIATED WITH THE REPORT AS A FIRST STATUS, THE FIRST STATUS INDICATING THAT THE PIRATED COPY MIGHT BE LEAKED BY THE LICENSEE

FIG. 2

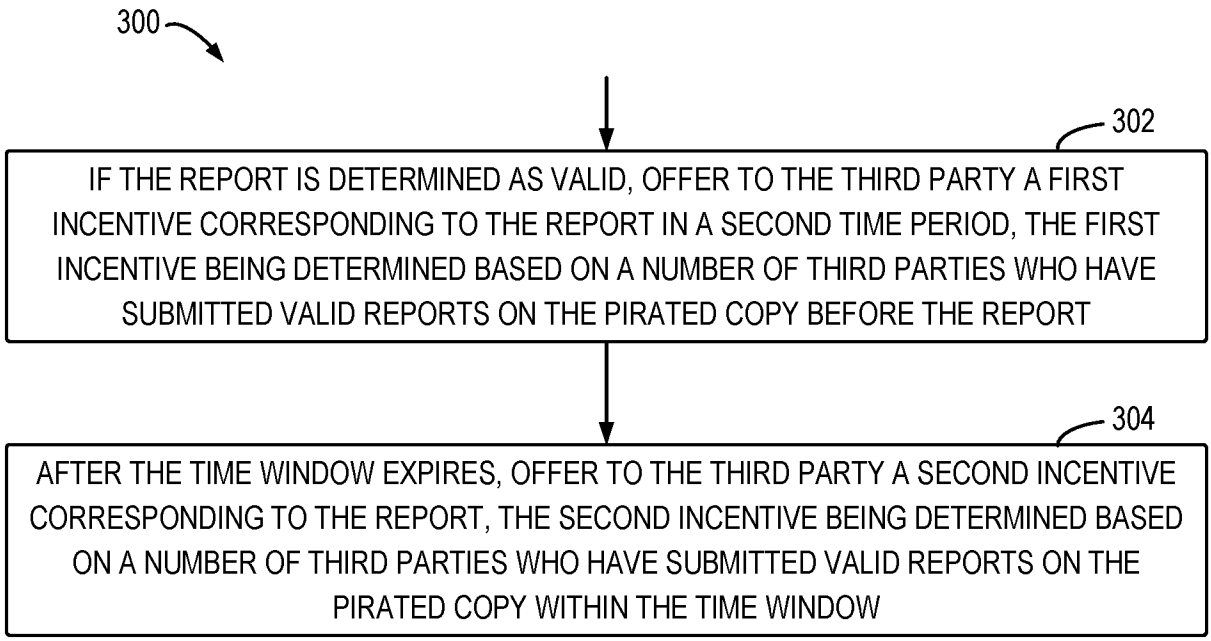
300
302
IF THE REPORT IS DETERMINED AS VALID, OFFER TO THE THIRD PARTY A FIRST INCENTIVE CORRESPONDING TO THE REPORT IN A SECOND TIME PERIOD, THE FIRST INCENTIVE BEING DETERMINED BASED ON A NUMBER OF THIRD PARTIES WHO HAVE SUBMITTED VALID REPORTS ON THE PIRATED COPY BEFORE THE REPORT
304
AFTER THE TIME WINDOW EXPIRES, OFFER TO THE THIRD PARTY A SECOND INCENTIVE CORRESPONDING TO THE REPORT, THE SECOND INCENTIVE BEING DETERMINED BASED ON A NUMBER OF THIRD PARTIES WHO HAVE SUBMITTED VALID REPORTS ON THE PIRATED COPY WITHIN THE TIME WINDOW

FIG. 3

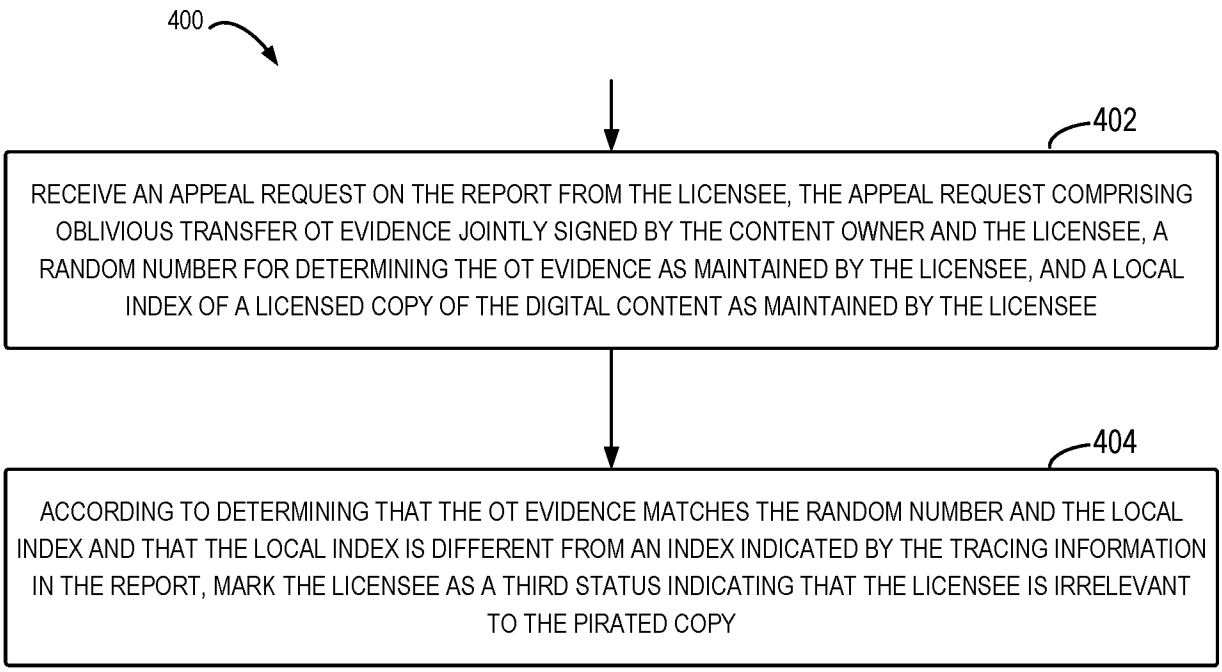
400
402
RECEIVE AN APPEAL REQUEST ON THE REPORT FROM THE LICENSEE, THE APPEAL REQUEST COMPRISING OBLIVIOUS TRANSFER OT EVIDENCE JOINTLY SIGNED BY THE CONTENT OWNER AND THE LICENSEE, A RANDOM NUMBER FOR DETERMINING THE OT EVIDENCE AS MAINTAINED BY THE LICENSEE, AND A LOCAL INDEX OF A LICENSED COPY OF THE DIGITAL CONTENT AS MAINTAINED BY THE LICENSEE
404
ACCORDING TO DETERMINING THAT THE OT EVIDENCE MATCHES THE RANDOM NUMBER AND THE LOCAL INDEX AND THAT THE LOCAL INDEX IS DIFFERENT FROM AN INDEX INDICATED BY THE TRACING INFORMATION IN THE REPORT, MARK THE LICENSEE AS A THIRD STATUS INDICATING THAT THE LICENSEE IS IRRELEVANT TO THE PIRATED COPY

FIG. 4

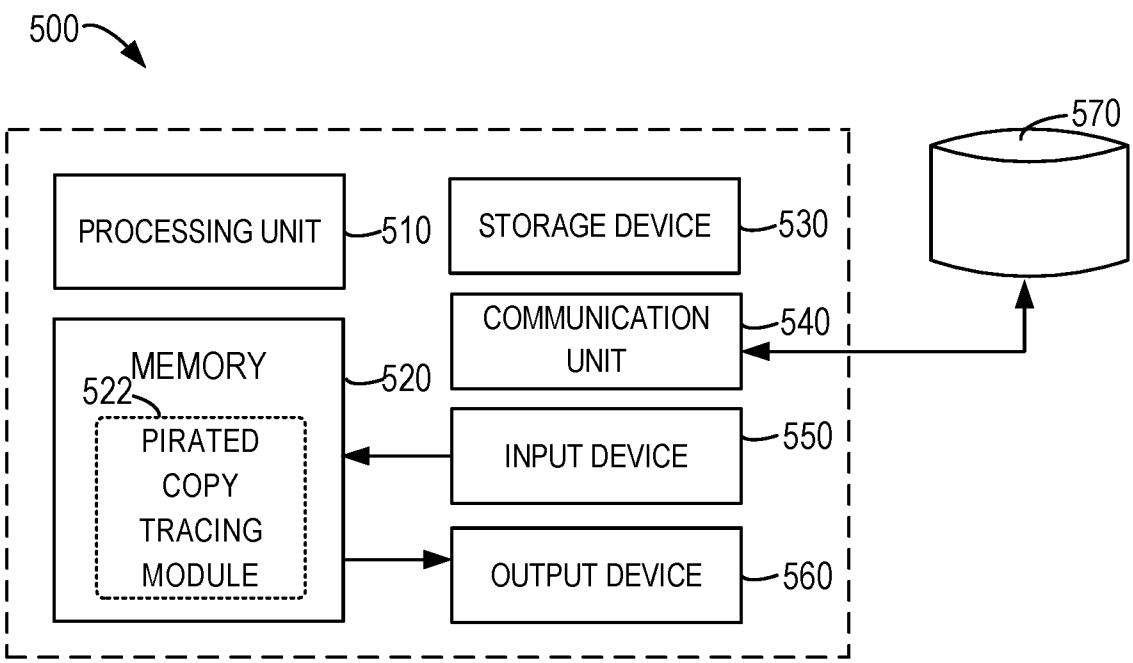
500
570
PROCESSING UNIT
510
STORAGE DEVICE
530
COMMUNICATION UNIT
540
MEMORY
522
520
PIRATED COPY TRACING MODULE
INPUT DEVICE
550
OUTPUT DEVICE
560

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2021/031464

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/16 G06Q30/00
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 G06Q H04L

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 2014/283123 A1 (LONSTEIN WAYNE D [US] ET AL) 18 September 2014 (2014-09-18) abstract paragraph [0020]; figures 1-9 paragraph [0033] paragraph [0041] - paragraph [0048] -----	1-15
X	US 2016/034914 A1 (GONEN DAVID [US] ET AL) 4 February 2016 (2016-02-04) abstract paragraph [0060] - paragraph [0074] -----	1-15

☐ 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
12 August 2021	23/08/2021

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	Savvides, George

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2021/031464

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014283123 A1	18-09-2014	US 2014283123 A1	18-09-2014
		US 2017279809 A1	28-09-2017
US 2016034914 A1	04-02-2016	NONE	