

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
18 December 2008 (18.12.2008)

PCT

(10) International Publication Number
WO 2008/153473 A1

(51) International Patent Classification:
G06F 21/24 (2006.01) **H04L 9/32** (2006.01)

(21) International Application Number:
PCT/SE2008/000396

(22) International Filing Date: 13 June 2008 (13.06.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0701443-4 13 June 2007 (13.06.2007) SE

(71) Applicant (for all designated States except US): **HEAD-
WEB AB** [SE/SE]; Tomtebgatan 35, SE-113 38 Stock-
holm (SE).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **ALVARSSON, Peter**
[SE/SE]; Larsbergsvägen 9, SE-181 38 Lidingö (SE).

(74) Agent: **STRÖM & GULLIKSSON AB**; P.O. Box 5275,
SE-102 46 Stockholm (SE).

(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, BR, BW, BY, BZ, CA,
CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE,
EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID,
IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC,
LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN,
MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH,
PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV,
SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN,
ZA, ZM, ZW.

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

Published:
— with international search report

(54) Title: METHOD AND SYSTEM FOR LEGALLY SHARING FILES

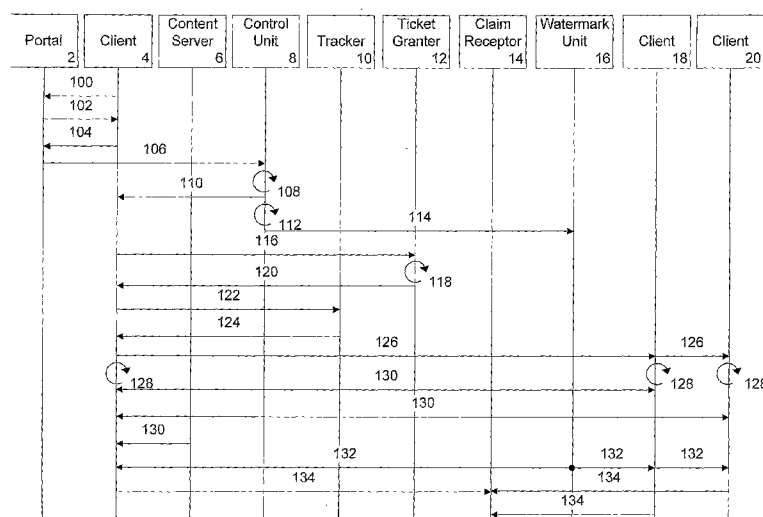


FIG. 3

(57) **Abstract:** The invention relates to a method and a system for distributing a content item, which has been divided into a plurality of blocks of data. A control unit (8) creates at least one watermark block. This watermark block is unique for the client (4) and the content item to be distributed and is stored in a watermark unit (16). Before the content item is distributed to the client (4) the client will need a ticket in order to verify himself when connecting to other clients (18, 20). The clients (4, 18, 20) can, if they have valid tickets, connect to each other and transfer the blocks of data to and from each other. In order for a client to receive a complete content item it also needs to connect to the watermark unit (16) in order to obtain the at least one watermark block that makes the content item complete.

METHOD AND SYSTEM FOR LEGALLY SHARING FILES

Technical Field of the Invention

5 The present invention relates to a method and a system for distribution of content over a peer-to-peer network to authorized nodes only.

Description of Related Art

10 Today more and more people use the Internet to distribute or download files. The most common method by which files are transferred on the Internet is the client-server model. A central server sends the entire file to each client that requests it. The clients only speak to the server, and never to each other, i.e. it is a point-to-point connection. The main advantages of this method are that it is simple to set up, and the
15 files are usually always available since the servers tend to be dedicated to the task of serving, and are always on and connected to the Internet. However, this model has a significant problem with files that are large or very popular, or both. It takes a great amount of bandwidth and server resources to distribute such a file, since the server must transmit the entire file to each client.

20 Another method of transferring files that have become popular is the use of a peer-to-peer network, with techniques such as Kazaa, eDonkey, Gnutella, Direct Connect, etc. In most of these networks, ordinary Internet users trade files by directly connecting one-to-one. The advantage here is that files can be shared without having
25 access to a proper server, and because of this there is little accountability for the contents of the files. Hence, these networks tend to be very popular for illegal files such as music, movies, pirated software, etc.

 A widely spread content distribution system is a technique called BitTorrent.
30 BitTorrent is a file sharing protocol for efficient distribution of large files over the Internet. It is peer-to-peer in nature, as users connect to each other directly to send and receive portions of the file. However, there is a central server called a tracker, which coordinates the action of all such peers. The tracker only manages connections, it does not have any knowledge of the contents of the files being distributed, and therefore a
35 large number of users can be supported with relatively limited tracker bandwidth. The key philosophy of BitTorrent is that users should upload (transmit outbound) at the same time they are downloading (receiving inbound.) In this manner, network

bandwidth is utilized as efficiently as possible. BitTorrent is designed to work better as the number of people interested in a certain file increases, in contrast to other file transfer protocols.

5 In order for BitTorrent to work and coordinate the downloading and uploading each peer or client needs to download a torrent, which is a metadata file containing information about all the files that it makes downloadable, including their names and sizes and checksums of all pieces in the torrent. It also contains the address of a tracker that coordinates the communication.

10

US Patent application no. 2006/0206486 describes a method and a system for legally sharing files in a peer-to-peer network on the Internet. The method is focused on incentive programs, which allow users to earn credits for later use. This invention is also concerned with verifying that the files that are shared are authorized files.

15 However, how the verification of clients that are connected to the peer-to-peer network is done is not clear.

European patent application no. 05105865.9 describes a content distribution method with the aim to maximize the delivery throughput in a peer-to-peer network.

20 This is done by assigning content to the nodes based on the capacity of each node.

WO 2005/112334 describes a method and a system for secure distribution of content over a communications network. The content owner distributes the content broken down into blocks to one or more content sources, which serve as distribution
25 points for a subscriber. A subscriber requesting a content item from a content owner receives a list of content sources with available blocks of the content item. In addition, a subscriber may determine if any peers on a peer-to-peer network to which the subscriber belongs also has any of the blocks of the content item available.

30 Thus, today there are several efficient methods for distribution content items over the Internet. However, the major problem is that these methods almost solely are used illegally, i.e. the legitimate owner of the original content item has not given his or her consent to download it. There are some legal file sharing sites today, but they have the drawback of distributing copy-protected content, which restricts the way a client can
35 use the file.

Thus, there is a need for a system and a method that uses these efficient methods for distributing content on a legal basis. In order to do so it is important that peers in a peer-to-peer network can verify that they have the right to download content from each other. Furthermore, it is important that a downloaded file is traceable. If a downloaded file is unique for the client who has downloaded it, it will probably prevent the client from distributing illegal copies thereof.

Summary of Invention

It is an object of the present invention to provide a method and a system for facilitating legal distribution of content items, which have been divided into a plurality of blocks of data, to at least one client using a peer-to-peer network. It is also an object of the invention to improve the security and the traceability during and after a content item is distributed to a client in a peer-to-peer network.

According to one aspect of the present invention there is provided a method for distributing a content item, in which at least one watermark block is created that is unique for the client and the content item to be distributed. The method further comprises issuing a ticket to the client, which ticket makes it possible for the client to verify himself when connecting to selected clients identified on a list that has been sent to the client. When connected, blocks of data are transferred from the selected clients to the client. The watermark block is also transferred to the client from a dedicated storage unit.

According to a second aspect of the present invention the step of creating at least one watermark block comprises assigning at least one of the blocks of data to be a watermark, dividing the at least one watermark block into a plurality of watermark pieces, and adding a unique watermark to each watermark piece.

According to a third aspect of the present invention there is provided a system for distributing a content item, which has been divided into a plurality of blocks of data, to at least one client connected to a peer-to-peer network. The system comprises a control unit for creating the at least one watermark block that is unique for the client and the content item, a dedicated storage unit for storing the watermark block, a ticket granter for issuing a ticket to the client, a tracker for identifying other clients that also are interested in receiving the content item.

Brief Description of the Drawings

Further objects, features, and advantages of the invention will appear from the following description of several embodiments of the invention, wherein various aspects
5 of the invention will be described in more detail with reference to the accompanying drawings, in which:

Figure 1, shows a system for distributing a content item according to the present invention,

10 Figure 2, shows how a content item is divided into a plurality of data blocks and watermark blocks and how each watermark block is divided into a plurality of watermark pieces, and

Figure 3 shows a communication table explaining the basic method according to the present invention.

Detailed description of the invention

Figure 1 illustrates a system for distribution of content over a peer-to-peer network to authorized nodes only. The system comprises a portal 2, usually a website,
20 to which a client 4 may connect. Furthermore, the system comprises a content server 6, a control unit 8, a tracker 10, a ticket granter 12, a claim receptor 14, a watermark unit 16 and further clients 18 and 20.

The portal 2 can be set up as a member site requiring a login in order for a
25 client 4 to get access to the content of the site or it may be available to anyone. The portal is the user interface for a client 4 wanting to purchase a content item. In context of the present invention it should be understood that a content item might include any type of digital content such as, movies, videos, music, e-books, games etc. Furthermore, a content item may be stored in one single file or in multiple files. The portal 2 shows
30 the contents available for a client 4 to purchase. Once the client 4 has decided what to purchase, he clicks a "buy button". The portal 2 will then ask the client 4 to enter information about how he will pay. The portal 2 sends this information to the control unit 8 that processes this information in order to approve or disapprove this transaction.

35 If the control unit 8 approves the transaction, it will send an approval back to the portal 2 and the client 4 will be provided with a so-called "info-hash". The info-hash

is a unique ID containing the name of the file (content) to be downloaded in form of a checksum.

In order to know where to start downloading the client 4 connects to the tracker 10 and communicates the info-hash to the tracker 10 that corresponds to the purchase made by the client. The tracker 10 responds thereto by sending a list identifying other clients 18, 20 that have purchased the same content item and that are connected to the peer-to-peer network. It should be noted that even if this example and figure 1 only mention and show two other clients the number of clients could be any number. The more clients connected to the peer-to-peer network the faster the downloading time usually is. The identifying list also identifies a content server 6, acting as a client, having a complete copy of the content item, or almost the complete copy, as will be described further below. The content server 6 is usually provided by the service provider who set up the portal 2. This is done in order to always have an available copy for downloading in the peer-to-peer network, regardless if there are any other clients connected to the network at the time.

When the content item first is uploaded on the content server 6 it is divided into a plurality of content blocks of data as can be seen in figure 2. Each block typically has a size of 1-2 MB. The size of a typical movie is 1-4,5 GB, which gives a total of 1000-2000 data blocks for one movie. At least one of these blocks of data is assigned to be a watermark block. A watermark block is in turn divided into a plurality of watermark pieces. A unique watermark will be added to each watermark piece. This addition of unique watermarks will be made individually for the client 4 each time he purchases a new content item.

When a purchase has been made and the control unit 8 has approved this transaction, as mentioned above, the control unit 8 will create the unique watermark for each watermark piece and save it on the watermark unit 16 for later retrieval of the client 4. Thus, as mentioned above almost the complete file is stored on the content server 6, the exception being the at least one watermark block. In a preferred embodiment of the invention a new watermark block is created for each 10 minutes of a movie. Thus, for a normal full-length movie of around 100 minutes there will be 10 different watermark blocks. Preferably, each watermark block comprises 10 to 30 different watermark pieces. In a preferred embodiment of the invention each watermark piece can be set either to a logical "0" or a logical "1". In a preferred embodiment of the invention, in which 20 watermark pieces are used, this will give over 1 million

combinations for a watermark block if logical “1” and “0” are used. For a full-length movie having around 10 watermark blocks the combinations are almost unlimited. As mentioned above it is the control unit 8 that is responsible for the creation and the setting of the watermark block, which is stored on the watermark unit 16.

5

The creation of the watermark block could in alternative embodiment of the invention be made in another way. Thus, in this embodiment a set of watermark pieces are already set and stored on the watermark unit 16. The creation process performed by the control unit 8 then comprises the selection of a combination of watermark pieces that make up the watermark block, connected to a specific client 4 and purchase. The use of watermarks will secure that each individual purchase that is made through the portal 2 can be traced through its unique ID.

Thus, at least one watermark block has now been created and stored on the watermark unit 16 and the client 4 has now also received a list identifying other clients 18, 20 that have purchased the same content item. But, before the client 4 can start downloading from other clients 18, 20 the client 4 will need a ticket in order to be verified by other clients 18,20. The client 4 will need to contact the ticket granter 12 and request a ticket. The client 4 sends the above mentioned info-hash to the ticket granter 12. The ticket granter 12 will in turn contact the control unit 8 in order to check that the client 4 has made a legal purchase according to what is specified in the info-hash.

If the client is approved by the control unit 8, the ticket granter 12 will receive this information and the ticket granter 12 will in turn send a receipt, including a valid ticket, to the client 4. At first this ticket will be valid both for downloading and uploading. But, as soon as the client 4 has downloaded the complete content item, the client 4 contacts the ticket granter 12 once again, and the ticket granter 12 will issue a new ticket for the client 4, which is valid only for uploading. The ticket granter 12 will, of course, first make a check with the control unit 8 if it is allowed to issue a new ticket.

30

In context of the present application it should be noted that a ticket could be anything that can identify a client in a secure and safe way. For example a ticket can be an encrypted key or the like. There, are many authorization techniques available for a person skilled in the art and it is therefore not described in detail here.

35

Once the client 4 has obtained a valid ticket he is free to contact other clients 18, 20, which are identified on the list previously obtained by the tracker 10. A contact

between two clients always starts with the exchange of tickets in order to verify each other. It is first after this verification of each other that the downloading and uploading between clients can take place. This is of course an important feature in order to secure that no illegal file sharing is taking place. Only clients that have made a legitimate
5 purchase are able to share files with each other.

The client 4 can download the content item from all clients 18, 20 on the identifying list and also from the content server 6, which also is on the identifying list. However, the client cannot download the complete content item from other clients 18,
10 20 or the content server 6, since it also needs the at least one watermark block that is stored on the watermark unit 16. The client 4 will request the at least one watermark block from the watermark unit 16. When the watermark unit 16 receives the request it first checks if the client 4 has a valid ticket. In order to do so the watermark unit 16 contacts the control unit 8, which verifies the ticket and if it is valid returns information
15 to the watermark unit 16 about which unique watermark block this individual client 4 shall download. The watermark unit 16 then uploads this watermark block to the client 4. This is a very important feature, which makes it possible to trace the origin of the file. If for example the client 4 decides to share his legally obtained file in an illegal file sharing network it will be easy to check that it was just this individual client 4 that
20 started to share the file illegally.

Different peer-to-peer techniques can be used in order to download and upload the content item. In one preferred embodiment of the invention a variation of BitTorrent is used. The BitTorrent protocol has according to the preferred embodiment been
25 provided with extra functionality, which is to be described below.

In one preferred embodiment of the present invention clients 4, 18, 20 that upload data to other clients 4, 18, 20 will earn credits. This is a way for a service provider to encourage clients to upload data and thereby increase the availability of the files to be downloaded. Thus, when a client 4 has downloaded a complete content item,
30 the clients 18, 20 that have uploaded the data blocks to the client 4, will contact the claim receptor 14 and claim credits for the uploaded data. Also, the client 4 will contact the claim receptor 14 and report how much and from which clients 18, 20 he has been downloading. The claim receptor 14 will keep track of all claims and also check if they are valid claims, by comparing uploading and downloading information from the
35 clients. It should be noted that each time a client contacts the claim receptor 14 it has to show a valid ticket in order to start communication there in between. This is also true

for all communication between clients and all units included in the system according to the present invention, such as the watermark unit 16, the content server 6 etc.

5 In another embodiment of the invention the claiming of credits are performed before the client 4 has downloaded the complete file. Thus, preferably the clients 4, 18, 20 contact the claim receptor 14 every 5 minutes to make a claim. The advantage with making these claims more often is that it gives a faster detection of fraudulently behaviour.

10 As mentioned above, the workflow of downloading and uploading between the clients is coordinated by using a torrent. Compared to BitTorrent, the torrent used in preferred embodiments of the present invention comprises added functionality in regard of coordinating the downloading of watermark blocks and also in regard of the claiming of credits and the use of tickets to verify that clients are legitimate.

15 Furthermore, it should be understood that the system described above has been described according to preferred embodiments. Even if figure 1 shows for example the ticket granter 12 and the claim receptor 14 in separate boxes it does not mean that the software thereof is stored physically on separate units. Figure 1 only shows that these are two different applications, which may or may not run on the same computer.
20 However, the clients 4, 18 and 20 depicted in figure 1 are separate physical units.

Figure 3 shows a table with the applications and units depicted in Figure 1. In the table an arrow shows that communication takes place between two or more units or
25 applications. A circular arrow shows that there is an ongoing process run by the unit or by the application. The table also shows a time dimension by that the further down you go in the table the more time has elapsed. For example, the communication for the arrow in step 102 occurs prior to that of the arrow in step 122.

30 As described above it all starts at step 100, with the client 4 connecting to a portal 2 and making a purchase. The portal 2 responds by sending a request for payment information in step 102. The client 4 responds thereto and sends the payment details to the portal 2 in step 104. The portal 2 in turn, connects to the control unit 8 and forwards the payment information to the control unit 8 in step 106. In step 108, the control unit 4
35 processes this information (purchase request) and approves or disapproves the purchase. If the purchase is disapproved the process will come to an end. However, if the purchase request is approved the control unit 8 will send the info-hash to the client 4 in step 110.

Thereafter in step 112, the control unit 8 will start creating 112 the watermark, which is unique for the client in combination with the purchase in question. After this process is ready the control unit will, in step 114, send the watermark to the watermark
5 unit 16 for storage.

The client 4 will use the info-hash received from the control unit 8 to get a ticket that will allow him to start downloading. Thus, the client 4 sends, in step 116, the info- hash to the ticket granter 12. In step 118, the ticket granter 14 processes the
10 request for a ticket and approves or disapproves the request. This step 118 may involve, even if it is not explicitly shown in the table, that the ticket granter 12 connects to the control unit 8 in order to verify that the client 4 has made a valid purchase. Disapproval will end the process and an approval will, in step 120, trigger the sending of a ticket to the client 4.

15 The client 4 will also send the info-hash to the tracker 10, in step 122. This step does not have to be performed after the above described steps 116-120 for requesting a ticket. It could be done in parallel or even prior to the ticket request. In step 124, the tracker 10 will after receiving the info-hash send a list back to the client 4 identifying
20 other clients 18, 20 in the peer-to-peer network that also purchased the same content item. The client 4, now having the list, can in step 126 connect to other clients 18, 20. Before downloading and uploading can be performed the client 4, in step 128, needs to verify 128 the other clients 18, 20 and the other clients 18, 20 need to verify 128 the client 4. If the clients 4, 18, 20 verify each other the process continues and the clients 4,
25 18, 20 start uploading and downloading to and from each other, in step 130. As can be seen in figure 3 the client 4 can also download from the content server 6, which has a complete file of the content item, except for the watermark pieces as discussed above. The watermarks are downloaded from the watermark unit 16 in step 132. It should be understood that the downloading of watermarks not necessarily must occur after the
30 downloading of the content item. In reality the downloading of watermarks and content would be done in parallel.

When the complete content item, including watermarks, has been downloaded it is time for the clients 4, 18, 20 to make their claims for the amount of data that they
35 have uploaded in order to earn credits. This is done in step 134. As mentioned above this claiming can also be done every 5 minutes and thus in parallel with many of the steps described above.

It shall be understood that even if the invention has been described with reference to preferred embodiments the invention is not limited thereto. There are many other embodiments and variations that are likewise within the scope of the invention,
5 which is best defined by the accompanying claims.

0

CLAIMS

1. A method for distributing a content item, which has been divided into a plurality of blocks of data, to at least one client (4) connected to a peer-to-peer network,
5 comprising the steps of,
creating at least one watermark block that is unique for the client (4) and the content item to be distributed and storing it in a dedicated storing unit (16),
issuing a ticket to the client (4),
sending a list to the client (4) identifying other clients (18, 20) that also are
10 interested in receiving the content item,
connecting to selected clients (18, 20) identified on the list,
transferring the plurality of blocks of data from the selected clients (18, 20) to the client (4) and
transferring the at least one watermark block from the dedicated storing unit
15 (16) to the client (4).

2. Method according to claim 1, wherein the step of creating at least one watermark block further comprises the steps of,
assigning at least one of the blocks of data to be a watermark,
20 dividing the at least one watermark block into a plurality of watermark pieces,
and
adding a unique watermark to each watermark piece.

3. Method according to claim 2, wherein the step of dividing the watermark
25 block comprises the step of dividing the watermark block into 10-30 watermark pieces, preferably 20 watermark pieces.

4. Method according to claim 1, wherein the step of issuing a ticket to the client (4) further comprises the steps of
30 receiving a request from the client (4) for the content item,
verifying and authorizing the request from the client (4), and
sending a ticket to the client (4).

5. Method according to claim 1, wherein the step of connecting to selected
35 clients (18, 20) identified on the list further comprises the step of verifying that the selected clients have a valid ticket.

6. Method according to any of the preceding claims, further comprising the step of requesting credits for data blocks that the client (4) has uploaded.

5 7. A system for distributing a content item, which has been divided into a plurality of blocks of data, to at least one client (4) connected to a peer-to-peer network, comprising, a control unit (8) for creating at least one watermark block that is unique for the client (4) and the content item, a dedicated storage unit (16) for storing the watermark block, a ticket granter (12) for issuing a ticket to the client (4) and a tracker (10) for identifying other clients (18, 20) that also are interested in receiving the content item.

8. A system according to claim 7, further comprising a portal (2) configured to display downloadable content items.

15 9. A system according to claim 7 or 8, further comprising a content server (6) for storing content items.

20 10. A system according to any of claims 7-9, further comprising a claim receptor (14) for managing credits for data blocks that the client (4) has uploaded.

11. A computer program comprising code means for performing the steps of any one of the claims 1-6, when the program is run on a computer.

25 12. A computer program product comprising program code means stored on a computer readable medium for performing the method of any of the claims 1-6, when said product is run on a computer.

30

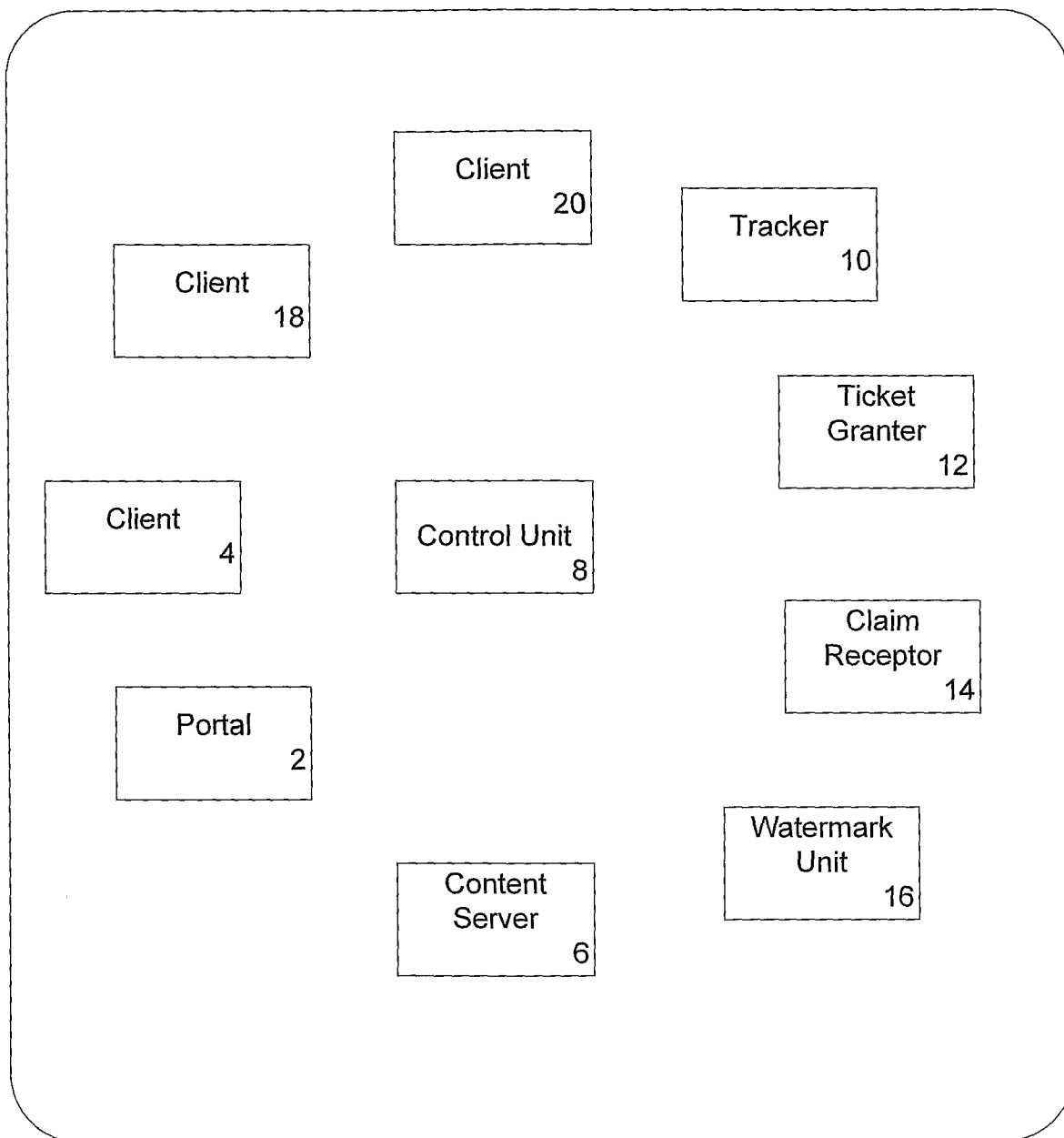


FIG. 1

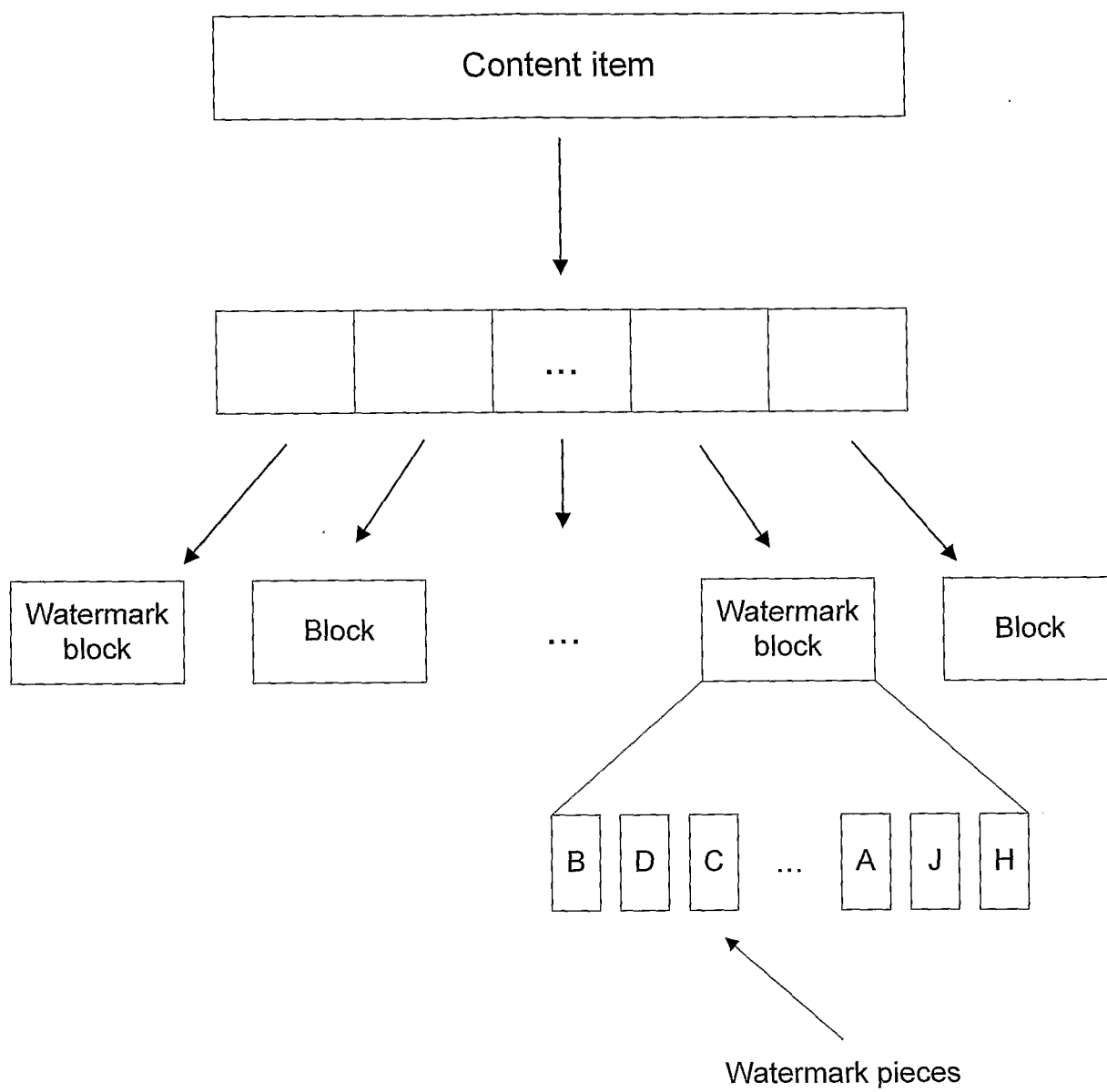


FIG. 2

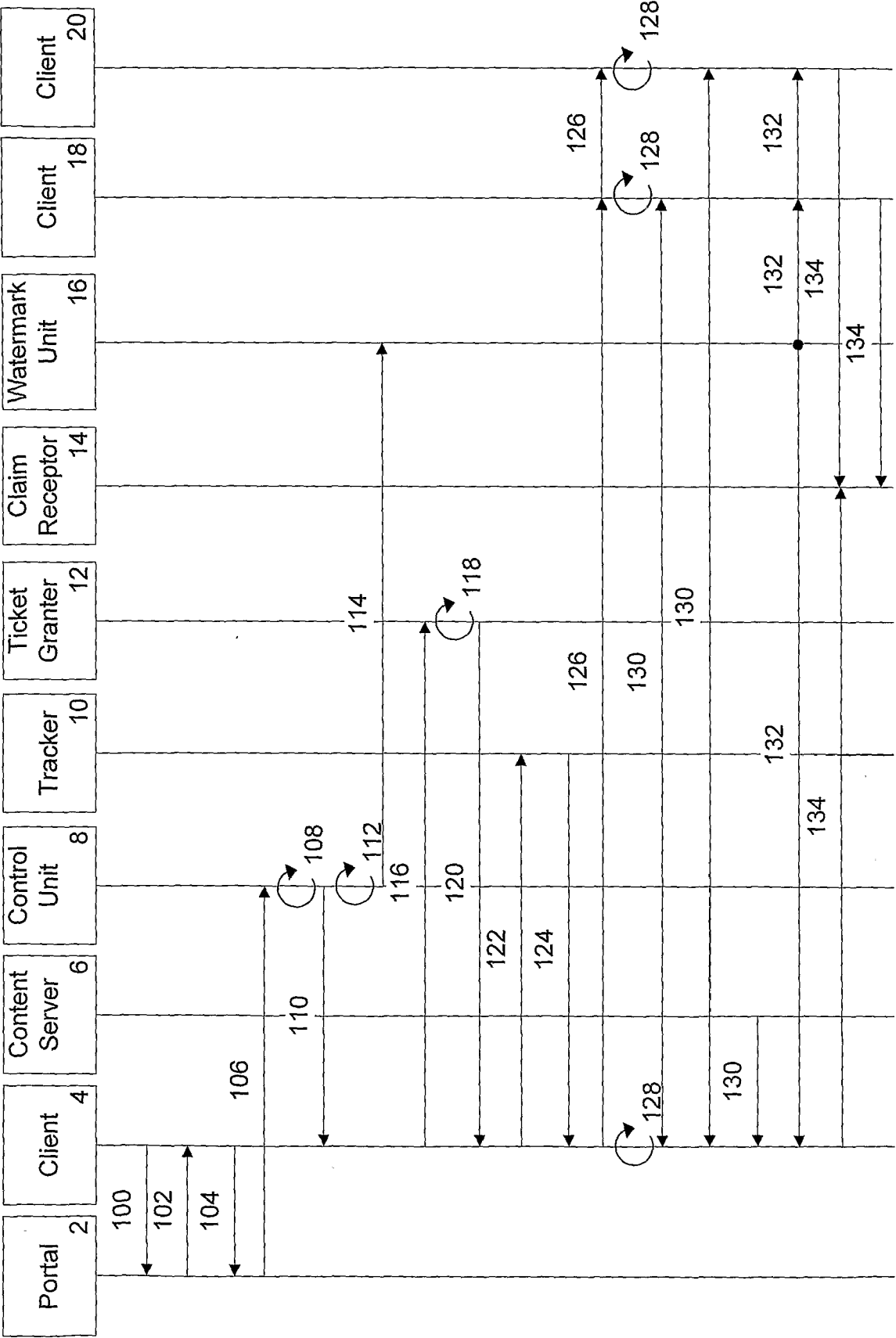


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE2008/000396

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet

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)

IPC: G06F, H04L

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

SE,DK,FI,NO classes as above

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

EPO-INTERNAL, WPI DATA, PAJ, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 20070047442 A1 (SNYDER, A M), 1 March 2007 (01.03.2007), abstract, paragraph [0007]; [0015]; [0028]; [0029]; [0037]; [0039]; [0040]; [0054]-[0058] --	1-12
Y	WO 2007053454 A1 (MICROSOFT CORP), 10 May 2007 (10.05.2007), figure 6, abstract, paragraphs [0013]-[0015]; [0029] --	1-12
A	WO 0208945 A1 (DIGIMARC CORP), 31 January 2002 (31.01.2002), page 5, line 28 - page 6, line 16; page 7, line 5 - line 9; page 10, line 23 - line 24, page 17, line 28 - line 30 --	1-12

☒ 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

25 Sept 2008

Date of mailing of the international search report

29-09-2008

Name and mailing address of the ISA/

Swedish Patent Office

Box 5055, S-102 42 STOCKHOLM

Facsimile No. +46 8 666 02 86

Authorized officer

Heidi Hjelmstedt /LR

Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE2008/000396

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 20050268102 A1 (DOWNEY, K F), 1 December 2005 (01.12.2005), abstract, paragraphs [0009], [0025]-[0028]; [0031]-[0038] --	1-12
A	US 20060242405 A1 (GUPTA, R ET AL), 26 October 2006 (26.10.2006), figure 3, abstract, paragraphs [0005]; [0009] -- -----	1-12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2008/000396

International patent classification (IPC)

G06F 21/24 (2006.01)

H04L 9/32 (2006.01)

Download your patent documents at www.prv.se

The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument (service in Swedish).

Use the application number as username.

The password is **DVUAHPHBOZ**.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

INTERNATIONAL SEARCH REPORT

International application No.

28/06/2008

PCT/SE2008/000396

US	20070047442	A1	01/03/2007	EP	1935123 A	25/06/2008
				WO	2007024994 A	01/03/2007
WO	2007053454	A1	10/05/2007	US	20070113096 A	17/05/2007
WO	0208945	A1	31/01/2002	AT	358850 T	15/04/2007
				AU	3281702 A	01/07/2002
				AU	4745701 A	03/10/2001
				AU	7704701 A	05/02/2002
				AU	2001277047 B	06/09/2007
				CA	2416530 A	31/01/2002
				DE	60127689 D,T	06/09/2007
				EP	1266475 A	18/12/2002
				EP	1311973 A,B	21/05/2003
				EP	1785890 A	16/05/2007
				JP	2003528538 T	24/09/2003
				JP	2004505349 T	19/02/2004
				US	6965683 B	15/11/2005
				US	7111168 B	19/09/2006
				US	7123740 B	17/10/2006
				US	7142691 B	28/11/2006
				US	7289643 B	30/10/2007
				US	7369676 B	06/05/2008
				US	7372976 B	13/05/2008
				US	20010037313 A	01/11/2001
				US	20010054150 A	20/12/2001
				US	20020052885 A	02/05/2002
				US	20020118394 A	29/08/2002
				US	20020120839 A	29/08/2002
				US	20020126872 A	12/09/2002
				US	20030012548 A	16/01/2003
				US	20050056700 A	17/03/2005
				US	20050111723 A	26/05/2005
				US	20060274915 A	07/12/2006
				US	20070027818 A	01/02/2007
				US	20070033409 A	08/02/2007
				US	20070055689 A	08/03/2007
				US	20070101147 A	03/05/2007
				US	20070174059 A	26/07/2007
				US	20080052783 A	28/02/2008
				WO	0171960 A	27/09/2001
				WO	0251063 A	27/06/2002
				US	20020033844 A	21/03/2002
US	20050268102	A1	01/12/2005	CA	2564959 A	24/11/2005
				EP	1747636 A	31/01/2007
				JP	2007538315 T	27/12/2007
				WO	2005112334 A	24/11/2005
US	20060242405	A1	26/10/2006	CN	101171782 A	30/04/2008
				EP	1872502 A	02/01/2008
				WO	2006115522 A	02/11/2006