

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
17 November 2005 (17.11.2005)

PCT

(10) International Publication Number
WO 2005/109337 A1

(51) International Patent Classification⁷: **G06T 1/00**

(21) International Application Number:
PCT/EP2005/052037

(22) International Filing Date: 4 May 2005 (04.05.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
04291192.5 7 May 2004 (07.05.2004) EP

(71) Applicant (for all designated States except US): **ALCATEL** [FR/FR]; 54, rue La Boetie, F-75008 Paris (FR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **TOMSU, Marco** [DE/DE]; Adalbert-Stifter-Strasse 12, 71254 Ditzingen (DE). **KESSLER, Markus** [DE/DE]; Mörgelenstrasse 3, 70329 Stuttgart (DE). **DOMSCHITZ, Peter** [DE/DE]; Stresemannstrasse 94, 70191 Stuttgart (DE).

(74) Agent: **RAUSCH, Gabriele**; Alcatel SEL AG, IPG, Lorenzstr. 10, 70430 Stuttgart (DE).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

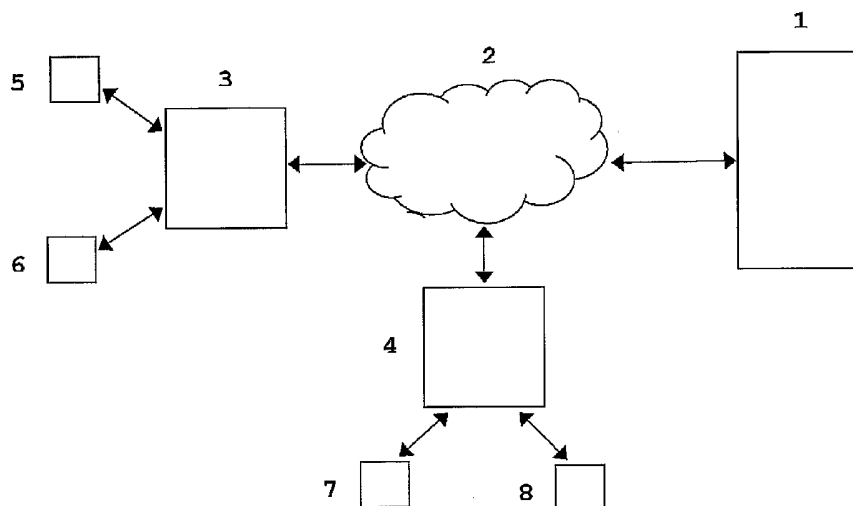
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

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

[Continued on next page]

(54) Title: METHOD FOR SENDING DIGITAL COPIES OF PROTECTED MEDIA AND NETWORK ACCESS DEVICE



(57) Abstract: Method for sending digital copies of protected media and network access device Method for sending digital copies of protected media, using receiver-individual digital watermarks, from a media server (1) via a telecommunications network (2) and a network access device (3, 4) with connecting devices to an end user terminal (5 - 8), in which a digital copy which is to be sent to a specific end user terminal (5 - 8) of the telecommunications network (2) is made available in the network access device (3, 4) from which the end user terminal (5 - 8) is connected to the telecommunications network (2) in which the digital copy provided with the digital watermark is sent to the end user terminal (5 - 8) via the connecting device of the network access device (3, 4) via which this end user terminal (5 - 8) is connected, the digital watermark being imprinted into the digital copy to be sent in this network access device (3, 4), wherein the digital watermark contains at least data acting as identification of the end user to whom the digital copy is to be sent.



Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Description

- [001] Method for sending digital copies of protected media and network access device
- [002] The invention relates to a method for sending digital copies of protected media with receiver-individual watermarks according to the preamble of claim 1 and a network access device according to the preamble of claim 4.
- [003] The rapidly growing number of broadband connections, such as ADSL, for example, for private customers has also caused a sharp increase in the demand for high-quality multimedia services requiring a large bandwidth, such as video-on-demand, for example, or downloading music from the internet. These data are transmitted in digital form and are of a quality comparable to a DVD or CD. Data properties of this kind in turn enable the production of a large number of copies of the data without loss of quality and thereby of course also the production and distribution of illegal copies.
- [004] In order to master this problem, the concept of the electronic watermark, in which the data are electronically marked, has been introduced in the transmission of media. This marking is here imprinted by only small changes in the signals to be transmitted and is therefore not perceptible to human senses. By a suitable choice of encrypting for the watermark it is additionally achieved that the watermark is inseparably linked to the data to be transmitted. Based on the information on the sender and the receiver of the data contained in the watermark of the copy, it can clearly be concluded from the copies whether the owner has obtained them legally, in other words is identical to the receiver, or whether they are pirated copies.
- [005] WO patent 01/67667 describes how receiver-specific watermarks are used in combination with encrypting techniques in order thereby to be able both to determine the origin of unauthorised copies and also to increase the probability that only the rightful receiver can reproduce the media contents by means of a key.
- [006] Currently the only possibility is to attach the watermark in a media server, which in the case of transmission of the same data to many or even all end users based on the receiver-individual watermark means that for every receiver a separate marked data stream has to be sent from the server via the network and the network access device to the end user. As this leads to extraordinarily high server and network utilisation, receiver-individual marking of the data in this way is impracticable. Additionally, there is no guarantee that the receiver of the data has actually ordered them and is therefore the rightful owner, as the data can be intercepted on the way from the server to the network access device, even if the data are being transmitted encrypted. Watermarks imprinted into the data stream in the server are therefore suitable only for identifying the sender, i.e. the holder of the copyright, but not for identification of the receiver

beyond reasonable doubt. Watermarks of this kind are useful for producers of CDs and DVDs and for the police to identify forgeries in which the copyright marking is missing or is incorrect, but this hardly discourages software pirates from making forgeries or pirated copies.

[007] An alternative possibility of preventing pirated copies is to incorporate copy protection, such as TCPA (trusted computing platform architecture), for example, in the terminals of the end users. These kinds of copy protection enable the media data to be reproduced only with specific reproduction equipment and thus prevent the reproduction of pirated copies on reproduction equipment other than that originally provided. However, this also stops the legal reproduction of private copies on other reproduction equipment, representing a curtailment of the rights obtained with the purchase of the media.

[008] The object of the invention is to create a way of alleviating the above-described situation.

[009] This object is achieved according to the invention by a method according to the doctrine of claim 1 and by a network access device according to the doctrine of claim 4.

[010] Any kind of marking, for individualising multimedia contents, for example, is performed by a network access device assigned to the respective end user and located in the path between the media server and the end user terminal. As this path is represented either by a separate line or a virtual connection, it can very reliably be guaranteed that the individualised media contents can really be received only by the rightful owner. Therefore in turn the origin of illegal copies can also be very reliably discovered.

[011] Each end user, as mentioned, is connected by a special virtual or physical connection to a special network access device. This puts the provider of the network access (network access provider or abbreviated NAP), as owner of the bit transmission layer (physical layer), in a position to identify the end user requesting a service. Provided that there is a contract between the provider of services and the provider of the network access, the latter can institute a service object based on software or hardware in the network access device assigned to the end user. The functionality of this service object is similar to code conversion in media. The end user identity in conjunction with other transaction data, such as the identity of the owner of the copyright or the date of the download, for example, is attached to the multimedia contents being transmitted via the network access device in the form of a watermark. In this way a clear link between the service provider, the service itself and the end user is produced and enables the prosecution of pirate copiers. Removal of the watermark is possible only by accepting great losses in quality. As the watermark is attached to the

data stream in the network access element assigned to the end user, this method is suitable not only for individual downloads or streaming, but also for transmitting multimedia contents to several end users simultaneously or even for broadcast messages. The method is further also suitable for providing multimedia contents if these multimedia contents are stored in a cache, wherein in this case the watermark is not attached until after the data have been fetched from the cache.

- [012] Instituting service objects of this kind with which watermarks can be attached to multimedia contents in the network access devices can take place for each end user individually, without there being unacceptably strong demands on the network capacity, as would be the case if the individual markings were to be attached in the media server. This also enables individual marking by means of watermarks in the case of transmission of the same data to many or even all the end users.
- [013] Attaching these individual, non-removable watermarks does not require any kind of expensive changes or extensions of the devices on the part of the end user or service provider and can therefore be executed flexibly and at a reasonable price.
- [014] Attaching the watermark in a network access device assigned to the end user additionally reduces the risk of incorrect assignment of watermarks and content.
- [015] The method is above all tailored to telecommunications companies acting as network access providers, as they hold exclusive control over the network access device and therefore can take on the attachment of the watermarks.
- [016] Based on the network access provider's control over the network access device and the technical implementation of the path between the network access device and the end user terminal by a separate line or a virtual connection, this connection between the network access device and the end user terminal is relatively secure and the danger of data manipulation and pirated copying is thereby minimised. It is quite possible for transmission of the multimedia contents also to be encrypted on the network path between the media server and the network access device, in order thereby to obtain additional security against pirated copying.
- [017] By the method described end users retain the facility, which is also theirs by right, of making security copies.
- [018] The contractual cooperation between the service provider and the network access provider opens up for the service provider potential access to the large pool of customers of the network access provider and therefore the prospect of additional commissions. Additionally, multimedia services can thereby be combined with additional services, such as payment services and the like, for example, likewise offered by the network access providers.
- [019] Further configurations of the invention are to be found in the subordinate claims and the following description.

- [020] The invention is explained in greater detail below with the aid of the attached drawing.
- [021] Fig. 1 shows as an example a network environment in which the invention can be implemented.
- [022] The network environment from Fig. 1 contains a media server (1), a telecommunications network (2), network access devices (3, 4) according to the invention and end user terminals (5 – 8). The media server (1) can communicate with a plurality of end user terminals (5 – 8) via the telecommunications network (2) and the network access terminals (3, 4).
- [023] The telecommunications network (2) may in this case be the internet, but also any other network, such as a so-called Local Area Network (LAN) or a Wide Area Network (WAN), for example. This telecommunications network (2) can in this case be implemented both in a fixed network and in a mobile radio environment.
- [024] The media server (1) is a network terminal for communicating via the telecommunications network (2). This media server (1) can in this case either simply be a computer which acts, e.g., as a web server, or also include special network functions, such as those of a router, switch or gateway, for example. The media server (1) additionally has means for storing media, such as hard disks, compact disks (CDs), digital versatile disks (DVDs) or similar, for example. The media may consist of video and/or audio data, such as MPEG data (MPEG = moving picture experts group), for example, or similar data. For communication via the telecommunications network (2) the media server (1) has means both for processing and for receiving and/or sending media.
- [025] The network access devices (3, 4) according to the invention have means for receiving, sending, storing and processing data, such as digital copies of media, for example. The means for processing data enable digital watermarks, which contain at least data acting as identification of the end user to whom the digital copies are to be sent, to be imprinted into the digital copies to be sent. The network access device (3, 4) is connected to the telecommunications network (2), such as the internet, for example, via one or more connecting devices. Via further connecting devices of the network access devices (3, 4) there is the possibility of data exchange with end user terminals (5 – 8) connected by means of virtual connections.
- [026] In a further embodiment the network access devices (3, 4) have means which enable the decoding of encrypted digital copies which the network access devices (3, 4) have received via the connecting devices to the telecommunications network (2). Encrypting the data on the path between the media server (1) and the network access devices (3, 4) acts in this case as additional security against illegal copying.
- [027] In a further embodiment the network access devices (3, 4) have means which enable

the encrypting of digital copies into which digital watermarks have previously been imprinted and which after encrypting are sent via the connecting devices to the appropriate end user terminals (5 – 8). Encrypting the data on the path between the network access devices (3, 4) and the end user terminals (5 – 8) in this case acts as additional security against illegal copying.

[028] The end user terminals (5 – 8) can receive the digital copies which are sent to them via a special physical or virtual connection by one of the network access devices (3, 4). The end user terminals (5 – 8) can be implemented as computers, such as personal computers (PC) or laptop computers, for example, but also again represent a media server. Additionally, the end user terminals (5 – 8) may also stand for portable electronic equipment, such as the personal data assistant (PDA) or mobile telephones, for example. Applications such as Windows Media Player™ or Real Player™, for example, can run on the end user terminals (5 – 8) to illustrate the received digital copies of the media.

[029] In the method according to the invention digital copies of media are sent by the media server (1) via the telecommunications network (2) and a network access device (3, 4) to one of the end user terminals (5 – 8), a digital watermark being imprinted into the digital copy in the network access device (3,4). This digital watermark contains at least information acting as identification of the end user for whom the digital copy is intended, but can additionally also contain, for example, information on the data source or the date of sending. The digital copy provided with the digital watermark is then sent via the connecting device of the network access device (3, 4) via which the respective end user for whom the digital copy is intended is connected.

[030] In a further embodiment the digital copies of the media in the media server (1) are first encrypted before they are sent by the media server (1) via the telecommunications network (2) to the network access device (3, 4). In the network access device (3, 4) the digital copies are decoded again before the digital watermarks are imprinted into the digital copies and they are then sent to the end user terminals (5 – 8).

[031] In a further embodiment the digital copies of the media in the network access device (3, 4) are encrypted after the digital watermarks have been imprinted into the digital copies and then the digital copies are sent encrypted to the end user terminals (5 – 8).

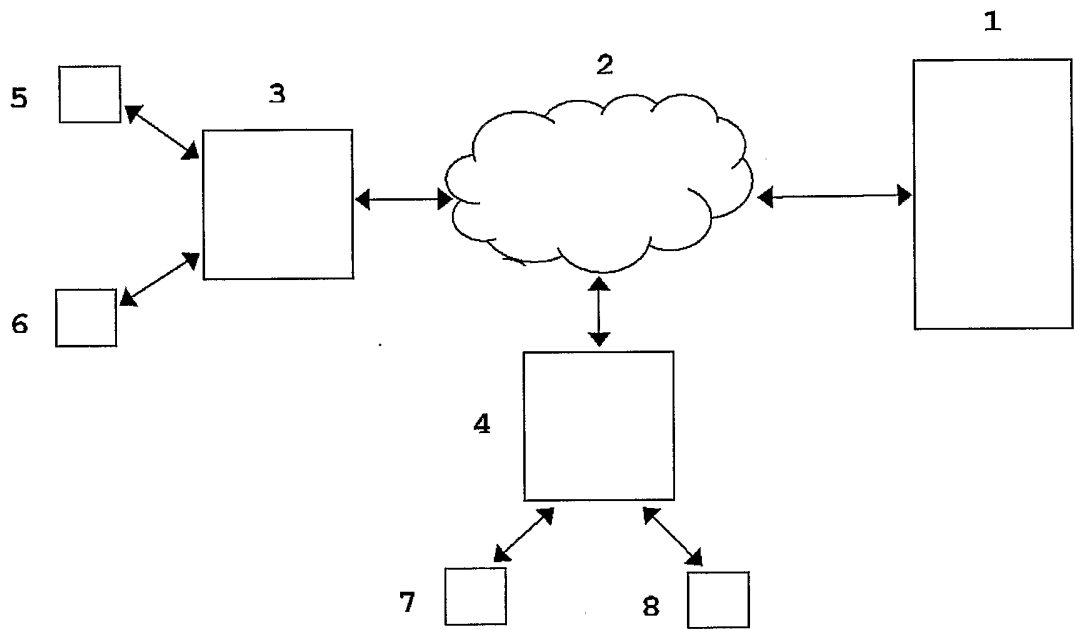
Claims

- [001] Method for sending digital copies of protected media, using receiver-individual digital watermarks, from a media server (1) via a telecommunications network (2) and a network access device (3, 4) with connecting devices to an end user terminal (5 - 8), in which a digital copy which is to be sent to a specific end user terminal (5 - 8) of the telecommunications network (2) is made available in the network access device (3, 4) from which the end user terminal (5 - 8) is connected to the telecommunications network (2) in which the digital copy provided with the digital watermark is sent to the end user terminal (5 - 8) via the connecting device of the network access device (3, 4) via which this end user terminal (5 - 8) is connected, characterised in that the digital watermark in this network access device (3, 4) is imprinted into the digital copy to be sent, the digital watermark containing at least data acting as identification of the end user to whom the digital copy is being sent.
- [002] Method according to claim 1, characterised in that the digital copy is sent encrypted between the media server (1) via the telecommunications network (2) to the network access device (3, 4) and in the network access device (3, 4) is decoded before the digital watermark is imprinted into the digital copy and it is sent to the end user terminal (5 - 8).
- [003] Method according to claim 1, characterised in that the digital copy is encrypted after imprinting of the digital watermark and before sending to the end user terminal (5 - 8).
- [004] Network access device (3, 4) with connecting devices for connecting end user terminals (5 - 8) of a telecommunications network (2) to this telecommunications network (2) by means of user-individually safeguarded connection channels, in particular for connecting to the internet, characterised in that the network access device (3, 4) has means for making available a digital copy which is to be sent to a specific end user terminal (5 - 8) of a telecommunications network (2), for imprinting a digital watermark into the digital copy to be sent, the digital watermark containing at least data acting as identification of the end user to whom the digital copy is to be sent, and for sending the digital copy provided with the digital watermark to the end user terminal (5 - 8) via the connecting device of the network access device (3, 4) via which this end user terminal (5 - 8) is connected.
- [005] Network access device (3, 4) according to claim 4, characterised in that the network access device (3, 4) has means for decoding an encrypted digital copy which the network access device (3, 4) has received via a connecting device to

the telecommunications network (2).

- [006] Network access device (3, 4) according to claim 4, characterised in that the network access device (3, 4) has means for encrypting the digital copy after imprinting of the digital watermark and before sending to the end user terminal (5 – 8).

[Fig. 001]



INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP2005/052037

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06T1/00

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 7 G06T H04N G06F

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

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

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JUDGE P ET AL: "WHIM: watermarking multicast video with a hierarchy of intermediaries" COMPUTER NETWORKS, ELSEVIER SCIENCE PUBLISHERS B.V., AMSTERDAM, NL, vol. 39, no. 6, 21 August 2002 (2002-08-21), pages 699-712, XP004371479 ISSN: 1389-1286 paragraph '0001! paragraph '2.1.1! paragraph '0003! paragraph '04.1! paragraph '0005! paragraph '05.1! figure 4 figure 5 ----- -/--	1-6

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in 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 document 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

19 August 2005

Date of mailing of the international search report

01/09/2005

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Fantini, F

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP2005/052037

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	PIVA A ET AL: "Managing copyright in open networks" IEEE INTERNET COMPUTING, IEEE SERVICE CENTER, PISCATAWAY, NJ, US, vol. 6, no. 3, June 2002 (2002-06), pages 18-26, XP002255464 ISSN: 1089-7801 figure 1	1,4
A	figure 2	2,3,5,6
A	US 2002/144116 A1 (GIOBBI JOHN J) 3 October 2002 (2002-10-03) figure 10	1-6

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP2005/052037

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002144116 A1	03-10-2002	US 2002080969 A1	27-06-2002
		US 2003115351 A1	19-06-2003
		US 2004098597 A1	20-05-2004
		US 2004255139 A1	16-12-2004
		WO 02052853 A1	04-07-2002