BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

Internal distribution code:
(A) [ ] Publication in OJ
(B) [ ] To Chairmen and Members
(C) [ ] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 18 April 2013

Case Number: T 1288/09 - 3.5.06

Application Number: 02725522.3

Publication Number: 1490767

IPC: G06F 1/00

Language of the proceedings: EN

Title of invention:
Copyright detection and protection system and method

Applicant:
Audible Magic Corporation

Headword:
Detecting unauthorized transmission/AUDIBLE MAGIC

Relevant legal provisions (EPC 1973):
EPC Art. 56

Keyword:
"Inventive step - yes (after amendment)"

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 1288/09 - 3.5.06

D E C I S I O N
of the Technical Board of Appeal 3.5.06
of 18 April 2013

Appellant: (Applicant)
Audible Magic Corporation
985 University Avenue
Suite 35
Los Gatos, CA 95032 (US)

Representative:
Bartle, Robin Jonathan
WP Thompson
Coopers Building
Church Street
Liverpool L1 3AB (GB)

Decision under appeal:
Decision of the Examining Division of the European Patent Office posted 20 January 2009 refusing European patent application No. 02725522.3 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman: W. Sekretaruk
Members: Martin Müller
A. Teale

Summary of Facts and Submissions

I. The appeal lies against the decision of the examining division, dispatched on 20 January 2009, to refuse European patent application no. 02725522.3 in view of, in particular, the following document:

D2: WO 96/36163 A2

The decision concluded that the then main and first auxiliary requests did not comply with Article 123 (2) EPC and that the then second and third auxiliary requests lacked an inventive step, Article 56 EPC 1973, over D2 in view of common knowledge in the art. To establish the common knowledge, reference was made to the following excerpt from a standard reference book:

D4: B. Schneier, "Applied Cryptography", pp. 30-31, Wiley, 2nd ed., 1995.

It is noted that the label "D4", used to refer to this document, was not used in the decision but has been introduced by the board.

II. A notice of appeal against this decision was received on 25 March 2009, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 27 May 2009. The appellant requested that the decision be set aside and that a patent be granted based on a main or one of two auxiliary requests filed with the grounds of appeal. It also criticized as an abuse of procedure that the examining division had only introduced D4 during the oral proceedings and without any forewarning.

III. In an annex to a summons to oral proceedings the board raised objections under Articles 84 EPC 1973 and 123 (2) EPC against all requests and under Article 56 EPC 1973 against the main request.

IV. In response to the summons, on 12 April 2013, the appellant filed an amended set of claims to replace all three previously pending sets of claims and a new description page 4 and requested the grant of a patent based on the following documents.

claims, no.	
1-19	received on 12 April 2013
description, pages	
2, 3, 5-38, 40-47	as published
1, 4a, 39	received on 4 July 2007
4	received on 12 April 2013
drawings, sheets	
1/22-22/22	as published

At the same time, the appellant informed the board of its intention not to appear at the oral proceedings.

V. Claim 1 reads as follows.

"A method of identifying transmissions of digital works to detect unauthorized transmissions of the digital works, the method comprising:

maintaining (702) a registry (244) of information identifying registered works including at least one content based fingerprint for each of the registered works, wherein each of the at least one content based fingerprints has a corresponding feature sequence;

monitoring (706) a network for transmission of at least one packet-based digital signal, wherein the transmission comprises a source IP (internet protocol) address, a recipient IP address, and a digital work;

extracting a plurality of features from the at least one packet-based digital signal, wherein the at least one packet-based digital signal comprises audio data, and wherein each feature is a plurality of characteristics of the at least one packet-based digital signal;

generating (732) a content based fingerprint for the at least one packet-based digital signal from the plurality of features, wherein the content based fingerprint of the at least one packet-based digital signal has a corresponding feature sequence;

performing a probabilistic identification comparison between the feature sequence of the content based fingerprint of the at least one packet-based digital signal and the feature sequence of a content based fingerprint of one of the registered works to determine a probability that the digital work in the transmission of the [at] least one packet-based digital signal is a match to one of the registered works;

determining whether the transmission is an authorized transmission, based on at least one of the source IP address or the recipient IP address, if the transmission of the at least one packet-based digital signal includes at least one portion of one of the registered digital works; and

taking action (720, 722, 726) based on the determination."

Claim 11 sets out a "digital works identification system" which is defined in terms which closely correspond to the wording of claim 1.

VI. The oral proceedings were held on 18 April 2013 as scheduled in the absence of the appellant. At the end of the oral proceedings, the chairman announced the board's decision.

Reasons for the Decision

The introduction of D4 during the oral proceedings - no deficiency in the first instance proceedings (Art. 11 RPBA)

1. The appellant considers it an "abuse of procedure by the examining division" to have only introduced D4 during the oral proceedings and without any forewarning (see grounds of appeal, point 16). The board notes that the examining division did not introduce D4 to support a new argument but merely to support an allegation about common knowledge in the art that had been made before (see decision under appeal, reasons 4.6, and minutes of oral proceedings, points 40-51). D4 is also rather short and of no particular technical complexity and the board has no reason to suspect that the representative was given insufficient time to consider D4 and the examining division's related argument. This was also not argued by the appellant in the grounds of appeal nor in response to the summons to oral proceedings, in which the above had been presented as

the board's preliminary opinion. The board therefore concludes that no deficiencies were apparent in the first instance proceedings.

The late filed request

2. According to Article 13 (1) RPBA, the board has discretion not to admit amendments to a party's case after it has filed its grounds of appeal. The discretion shall be exercised in view of the new subject-matter submitted, the current state of the proceedings and the need for procedural economy. In the present case, the amendments were filed late on Friday, 12 April 2013, and were received by the board only on Monday, 15 April 2013, *i.e.* a mere three days before the oral proceedings. However, since the amendments directly and successfully addressed all the board's concerns raised in the summons to oral proceedings and did not introduce any complication that the board was not able to deal with during oral proceedings and in the appellant's absence, the board exercises its discretion to admit the new request.

The invention

3. The application generally relates to the problem of detecting and acting upon unauthorized transmission of digital works over the Internet (see page 1, lines 11-14).

3.1 The application proposes to register protected digital works together with so-called "content-based fingerprints" which are obtained from the digital works by extracting a plurality of features from them.

3.2 Then network traffic is monitored. From each intercepted digital data packet a content-based fingerprint is generated and compared with the registered fingerprints so as to determine "a probability that the unknown content contains a registered copyrighted work" (see page 21, lines 22-28).

3.3 In case of a match indicating that the data packet contains a portion of a registered work a follow-up check is performed to establish whether the copyright owner may have authorized the transmission. The determination of whether the transmission is authorized is based on the source IP address or the recipient IP address (see page 8, lines 20-23; and page 26, lines 25-31).

3.4 Based on the result of this determination, especially if negative, appropriate "action" is taken such as recording, reporting or blocking transmission (see page 13, lines 24-31, and page 19, lines 28-31).

3.5 The application is particularly concerned with digital works comprising audio data such as music or video, and a method called the Stochastic Audio Matching Mechanism, abbreviated to SAMM, is discussed in detail (cf. page 17, line 8-12 and page 29, line 16 - page 47, line 20). However the description is explicit about the fact that digital works can be of any type, including text, software or other digital content (cf. page 4, line 10; page 12, lines 8-10; page 16, line 27 - page 17, line 14). Depending on the type of work, different fingerprinting methods have to be used which the description refers to as known in the art (see page 17, lines 8-10).

Article 123 (2) EPC

4. Claims 1 and 11 refer to "probabilistic identification comparison" between the fingerprints of the current digital signal and of one of the registered works "to determine a probability that the digital work in the transmission ... is a match to one of the registered works".

4.1 The board notes that the description discloses the term "probabilistic identification" literally only in the context of audio data with reference to the SAMM (see page 29, lines 19 and 27).

4.2 Claims 1 and 11 specify that the digital signal "comprises audio data", implying that the digital signal may also comprise other data (for instance, metadata such as the file name and the source and recipient IP addresses). They further specify that the "probabilistic identification comparison" is based on features extracted "from the ... digital signal". This does not imply however that the probabilistic identification is based solely on features extracted from the audio signal and cannot, therefore, be supported by SAMM alone.

4.3 The description however specifies that several "assessment criteria", *inter alia* based on the content-based fingerprint, "provides only a probability that the unknown content contains a registered copyright work". In the board's view, this provides original disclosure for the term "probabilistic identification comparison" in claims 1 and 11, Article 123 (2) EPC.

4.4 That said, the board considers that the skilled person would, in the given context, interpret the term "probabilistic identification" broadly to mean matching based on degrees of similarity and suitable thresholding - as opposed to binary matching which may only succeed or fail - but would not take it to imply that that similarity is based on a rigorous mathematical analysis of probabilities of identity.

5. The board also notes that the fact that a "feature is a collection of characteristics" is, literally, only disclosed in the context of SAMM (see page 30, lines 19-20). It is disclosed that a temporal sampling of an audio signal produces a "single feature" at each "single point in time" which consists of a "collection of the representative characteristics".

5.1 The board considers that the terms "features" and "characteristics" are technically equivalent in the given context. Moreover the term "feature", albeit widely used in the given context, is so broad that it is impossible in general to distinguish whether a piece of information constitutes a (single) "feature" or a "plurality of characteristics".

5.2 For digital works of arbitrary type the description discloses that "one or many of various features" may be extracted and that "features [are] obtained from a sampled work" (see page 26, lines 18-20, and page 28, lines 26-27). In view of the foregoing, the board is satisfied that the description as originally filed discloses the claimed wording of a "feature [being] a plurality of characteristics", Article 123 (2) EPC.

6. The description discloses that the monitored data transmission comprises a source IP address and a recipient IP address (see page 8, lines 16-23; page 18, lines 11-19 and fig. 2). It also discloses the determination of whether a transmission is authorized based on the "source address" or the "recipient"/"destination address" (see *e.g.* original claims 4, 6, 32 and 34) and that these are comprised in the "packet-based digital signal". In combination, the board considers that the skilled person would take this to teach, directly and unambiguously, the determination of whether a transmission is authorized "based on the source IP address or the recipient IP address", Article 123 (2) EPC.

7. In the decision under appeal the examining division found the then main and first auxiliary requests not to comply with Article 123 (2) EPC, based on the claimed terms "identifiers of registered work" (and its difference, if any, from the term "fingerprint"), the notion of "unique" identification and the claimed feature that "unidentified digital work" be monitored (reasons 1.1-1.3). Since the amended claims do not refer to "identifiers", "unique" identification or "unidentified" digital works any more, these objections, as the board understands them, need not be gone into further for the purposes of this decision.

8. In summary, the board is satisfied that the amended claims remain within the disclosure of the original application documents and are thus in conformance with Article 123 (2) EPC.

Article 84 EPC 1973

9. Since the amended claims do not refer to "monitoring ... unidentified digital works" any more, the objection under Article 84 EPC 1973 against this term in the decision (reasons 2), need not be gone into further either. The board has no occasion to raise any clarity objection of its own.

The prior art

10. D2 discloses a steganographic system used, *inter alia*, for the automatic detection of unauthorized transmission of copyrighted digital works (see abstract and page 48, lines 16-19), including audio (see *e.g.* page 4, lines 27-30). More specifically, D2 defines a library of so-called universal codes (see page 28, line 17 ff.) which may be embedded into a digital work - invisibly, but in a way that allows their retrieval by suitable recognition software (page 30, lines 21-22) - so as to link the work with its pertinent copyright owner (see page 30, line 38 - page 31, line 8).

10.1 D2 discloses an "Internet tollgate" which would "check incoming video" for the company's "internal signature codes" and certain header information and which would not pass any non-authorized material based on this check (see page 49, lines 7-12). Header information may be information "about the file as a whole" and include information about the author or copyright holder of the data (see page 46, lines 16-20). As an alternative, D2 also discloses "another piece of [the] ... network" which "performs mundane routine monitoring on Internet channels to look for unauthorized transmission of ...

proprietary creative property" (see page 49, lines 12-14).

10.2 D2 addresses the problem that "pirates" might modify a protected digital work so that the embedded codes can no longer be recognized (see page 49, lines 16-20) and discloses that this may be acceptable in some situations but not in others. It may be acceptable for the "enablement of authorized action based on the finding of the codes" - because, as the board reads it, a modified digital work will fail to enable the unauthorized action - but may be inacceptable "in the case of 'random monitoring ... for the presence of codes.'" (see page 49, lines 21-24) - because the illicit use of modified works will simply be missed.

11. D4 discloses, in the context of cryptography, that "hashing" was well-known in the art at least by 1996 as a way of "fingerprinting" files (see sec. 2.4). Hashing is however not suitable for probabilistic identification or the detection of unauthorized transmission of digital works as is now claimed. A method suitable for detecting copyright infringement must be robust against "evasion techniques such as adding a small segment to the beginning of an audio file" (see description, page 3, lines 24-27). This robustness is provided by "probabilistic identification". Hash values however map different input values to different hash values, however small the difference in the input is. This is useful for an electronic signature, which is meant to become invalid as soon as the signed document is only slightly manipulated, but not suitable for the claimed purpose of the claims. The board concludes that D4 is no longer relevant to the amended claims.

Article 56 EPC 1973

12. The decision under appeal starts its inventive step assessment from D2. The board agrees with this choice.

12.1 Claims 1 and 11 differ from D2 in two main respects:

a) Identification of digital works according to the claims is based on probabilistic identification of content-based fingerprints rather than on the detection of watermarks as used in D2.

b) The claims specify that an unauthorized transmission is determined based on the source or recipient IP address in addition to the fingerprint matching, whereas D2 discloses that digital data is validated based on watermark detection in combination with the verification of header data, which may include the author and the copyright owner of the digital work.

13. Regarding feature "a", as the board understands the decision under appeal, it argues (reasons 4.5) that the "mundane routine monitoring" according to D2 (see page 49, lines 12-14) suggests, if not implies, "well-known monitoring methods" other than watermarking.

13.1 In the board's understanding however (see point 10.1 above), D2 teaches "mundane routine monitoring" as a different way of employing the watermark-based identification method for transmission control which does not imply or suggest a different identification method (such as fingerprinting) altogether. At the same time, the board disagrees with the appellant that D2 teaches away from using a different identification method, such

as fingerprinting in place of watermarking. Rather, the board is of the opinion that the skilled person would always assess possible improvements of a given method or device.

13.2 The board considers that watermarking and fingerprinting are well-known ways of identifying a digital object with well-known respective advantages and disadvantages. Watermarking operates by incorporating "watermarks" into a digital object which can be automatically retrieved later on. Fingerprinting in contrast does not incorporate anything into the digital object but derives an identifier from the given content. The processing requirements for watermarking are typically smaller than those for fingerprinting, but watermarking cannot protect already released digital works and can be removed or disabled, leaving a digital work unprotected (see description, page 3, lines 8-12).

13.3 In the board's judgment therefore it would have been obvious for the skilled person seeking to improve the disclosure of D2 to consider fingerprinting as an alternative to watermarking to identify digital documents. Once this choice is made, the board further considers that the claimed use of fingerprints follows obviously, in particular the use of a registry, the calculation of a fingerprint from a digital signal in transmission and its comparison with the registered fingerprints. Even the claimed "probabilistic identification" is, in the broad interpretation given above (see point 4.4), considered to be a commonly known way of robust fingerprinting.

13.4 The board thus concludes that difference "a" is insufficient to establish an inventive step over D2.

14. Regarding feature "b", with reference to the IP addresses, the detection of unauthorized transmission as claimed is based on properties of the network or, more specifically, of the individual network components involved in a transmission. In contrast, D2 only discloses the use of meta data of the digital work itself (header information) and of individuals involved (author, copyright owner).

14.1 Difference "b" thus contributes to making the detection mechanism of D2 more network aware. As part of a network monitoring mechanism as claimed the board finds that this contribution makes a technical contribution to the art.

14.2 The board further considers that the evaluation of IP addresses is not suggested by the use of header information according to D2 nor by any of the other documents on file.

14.3 Therefore, by virtue of difference "b", the board comes to the conclusion that the claimed matter is based on an inventive step over D2 and the available prior art, Article 56 EPC 1973.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the examining division with the order to grant a European patent with the following documents:

claims, no.	
1-19	received on 12 April 2013
description, pages	
2, 3, 5-38, 40-47	as published
1, 4a, 39	received on 4 July 2007
4	received on 12 April 2013
drawings, sheets	
1/22-22/22	as published

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk