BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPÉEN 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 10 November 2015

Case Number:	T 2194/10 - 3.5.04
Application Number:	06825302.0
Publication Number:	1938602
IPC:	H04N7/167, H04N7/24
Language of the proceedings:	EN

Title of invention:
PARTIAL ENCRYPTION TECHNIQUES FOR MEDIA DATA

Applicant:
APPLE INC.

Headword:

Relevant legal provisions:
EPC 1973 Art. 84
RPBA Art. 13(1)

Keyword:
Claims - clarity (no)
Late-filed auxiliary requests - admitted (no)

Decisions cited:

Catchword:

This datasheet is not part of the Decision.
It can be changed at any time and without notice.

Beschwerdekammern
Boards of Appeal
Chambres de recours

European Patent Office
D-80298 MUNICH
GERMANY
Tel. +49 (0) 89 2399-0
Fax +49 (0) 89 2399-4465

Case Number: T 2194/10 - 3.5.04

DECISION
# of Technical Board of Appeal 3.5.04
of 10 November 2015

Appellant:
(Applicant)

APPLE INC.
1 Infinite Loop
Cupertino, CA 95014 (US)

Representative:

Gillard, Matthew Paul
Withers & Rogers LLP
4 More London Riverside
London
SE1 2AU (GB)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted on 8 June 2010 refusing European patent application No. 06825302.0 pursuant to Article 97(2) EPC.

Composition of the Board:

Chairman B. Müller
Members: C. Kunzelmann
M. Paci

Summary of Facts and Submissions

I. The appeal is against the decision of the examining division to refuse European patent application No. 06 825 302.0 under Article 97(2) of the European Patent Convention (EPC).

II. The application was refused on the grounds that the encryption method of claim 1 according to the main and first and second auxiliary requests then on file did not involve an inventive step in view of

D6: SCHULTZ, C. A.:
'FDPAM ISO/IEC 14496-1:2001/AMD3',
ISO/IEC JTC1/SC29/WG11 N4701,
March 2002, pages 1 to 57, XP001074708

and common general knowledge.

III. The applicant appealed and requested that the decision be set aside and a patent be granted.

IV. The board issued a communication pursuant to Article 15(1) of the Rules of Procedure of the Boards of Appeal (RPBA), annexed to a summons to oral proceedings. It indicated that it tended to agree with the finding in the decision that D6 allowed parameters to be selected in the encryption phase such that, at least in the case of video files according to the MPEG-4 standard, the functionality specified in claim 1 of the main request was achieved. The board also raised an objection under Article 84 EPC 1973 because the wording "not encrypting an initial portion of each of the blocks including all or a portion of the header" in claim 1 of the main request and the corresponding wording in claim 1 of the auxiliary requests specified an unclear multitude of options. Moreover, different options might occur in different frames. All possibilities of encrypting, partly encrypting and not encrypting the (block) header appeared to be encompassed. The description did not appear to clarify this wording. In particular, paragraph [0057] seemed to refer to the case of the initial offset (corresponding to the unencrypted initial portion) being zero for blocks which were not the first block for a given frame.

V. The appellant replied with a letter dated 9 October 2015 and filed amended claims according to new main and first to third auxiliary requests, thereby replacing all previous claims. It submitted that the requests should be admitted because they were filed in reaction to the Article 84 issues raised by the board.

VI. Claim 1 of the main request reads as follows:

"A method (400) for encrypting media data, said method comprising:
identifying (402) a media file (500) having media data to be encrypted, the media data being arranged in frames (Fl, F2, F3, F4, F5);
examining (404) the media data in the media file to locate frame boundaries for the frames within the media data;
dividing each of the frames into a plurality of blocks (B1, B2, B3, PB), each block including a header including header information;
retrieving (408) encryption parameters including an initial offset amount into a block to be utilized when encrypting the block; and
encrypting (410) each of the blocks in accordance with the encryption parameters to encrypt only a portion

(542, 604, 624) of the media data of each of the blocks and not encrypting an initial portion (602, 622) of each of the blocks, the initial portion including all or a portion of the header of the block."

VII. Claim 1 of the first auxiliary request reads as follows:

"A method (400) for encrypting media data, said method comprising:
identifying (402) a media file (500) having media data to be encrypted, the media data being arranged in frames (Fl, F2, F3, F4, F5);
examining (404) the media data in the media file to locate frame boundaries for the frames within the media data;
dividing each of the frames into a plurality of blocks (B1, B2, B3, PB), each block including a header including ~~header information~~ *symbols for encoding the media file*;
retrieving (408) encryption parameters including an initial offset amount into a block to be utilized when encrypting the block; and
encrypting (410) each of the blocks in accordance with the encryption parameters to encrypt only a portion (542, 604, 624) of ~~the media data of~~ each of the blocks ~~and not encrypting an initial portion of each of the blocks, the initial portion including all or a portion of the header of the block~~, *wherein the portion is a portion at least of the symbols and just a portion of the part of the block that comes after the header*."

New features with respect to claim 1 of the main request are in *italics* and omissions in ~~strikethrough~~.

VIII. Claim 1 of the second auxiliary request corresponds to claim 1 of the first auxiliary request, with the last feature (starting from the last "wherein") reading: "*wherein the portion includes a least some of the symbols and extends from a location within the header, as specified by the initial offset amount, to a location within the part of the block that comes after the header.*"

IX. Claim 1 of the third auxiliary request corresponds to claim 1 of the main request, with the following feature appended at the end: "; wherein each of the blocks (B1, B2, B3, BP) are the same size, and wherein at least a plurality of the frames (F1, F2, F3, F4, F5) within the media data have different sizes."

X. In a letter dated 4 November 2015, the appellant's representative informed the board that he had been advised not to attend the oral proceedings and requested a decision based on the written submissions.

XI. The board held oral proceedings on 10 November 2015 in the appellant's absence, in accordance with Rule 71(2) EPC 1973 and Article 15(3) RPBA. The chairman noted that the appellant had requested in its letter of 9 October 2015 that the decision under appeal be set aside and a patent be granted with the documents according to the main request or one of auxiliary requests 1 to 3, as identified in that letter.
At the end of the oral proceedings the chairman announced the board's decision.

XII. The reasons for the decision under appeal may be summarised as follows:

D6 was considered as the closest prior art. It disclosed selective decryption from the perspective of the decoder. In particular, it provided a parametric description infrastructure for MPEG-4 Intellectual Property Management and Protection (IPMP) from a user terminal point of view. The functionalities expressed in the first steps of claim 1 of the main request were equivalent to a content provider allowing a user terminal to request content encrypted under the IPMP framework, which content was structured into entities for compression processing (e. g. slices, objects, macroblocks) and entities for communication from the content provider to a user terminal (e. g. packets) in a frame aligned manner. The blocks specified in claim 1 were considered to be equivalent to MPEG-4 video packets, which were known to contain a header including header information. Such MPEG-4 video packets could be used as units of cipher-text. The syntax given in D6, Annex A, allowed non-content specific selective encryption to be chosen, wherein n segments ("nSegments") were to be decrypted or skipped interleavingly by the terminal. The length of each of the n segments could be specified by setting its respective value "RLE-Data". The first segment could remain unencrypted by setting the first value of "RLE-Data" to zero. This resulted in the functionality that an initial portion of each of the blocks (including all or a portion of the header) was not encrypted.
The implementation of the related selective encryption at an encoder could be performed by a person skilled in the art without the involvement of inventive step.

XIII. The appellant's arguments may be summarised as follows:

D6 did not clearly and unambiguously disclose that "nSegments" and "RLE-Data" could co-operate to produce a decryption method such that the decryption was performed only over a part of the video packet and not over an initial part of the video packet, with the initial part extending over at least a part of the header of the video packet. The examining division had considered the interpretation of Annex A of D6 as a matter of common general knowledge, but had not provided evidence for this common general knowledge. Nor had it provided evidence for the format of MPEG-4 files or evidence that a video packet of D6 was the same as an MPEG-4 video packet. Moreover, it was a mere assertion on the part of the examining division that the encryption method of claim 1 was obvious if D6 disclosed a complementary decryption method. The examining division had failed to address the feature that each block of the media file was encrypted in the specified way. The examining division had not used the problem-solution approach. The appellant also disputed that it was possible to select parameters in D6 so that the complementary encryption tool allowed media data to be encrypted according to the method of claim 1. The technical effect of the claimed encryption method over the encryption method complementary to the decryption method of D6 was that of expending the encryption effort entirely on the header, when the header contained standard information a hacker could easily guess.

The claims were clear. In particular claim 1 of the main request had been drafted to cover a limited set of options. All options discussed in the board's communication were disclosed in the application as filed, in particular in paragraphs [0056] and [0057]. Hence claim 1 should be allowed to cover these options.

Claim 1 allowed different encryption options to occur in different frames, as explained in paragraph [0050] of the application. This did not induce a lack of clarity. Claim 1 comprised the step of "not encrypting an initial portion of each of the blocks" and thus did not encompass the case of the header being entirely encrypted. In the case of the initial offset being zero, the partial encryption scheme so produced did not fall within the scope of claim 1.

Reasons for the Decision

1. The appeal is admissible.

2. Main request: admission (Article 13(1) RPBA)

2.1 According to Article 13(1) RPBA, "Any amendment to a party's case after it has filed its grounds of appeal ... may be admitted and considered at the Board's discretion. The discretion shall be exercised in view of inter alia the complexity of the new subject matter submitted, the current state of the proceedings and the need for procedural economy."

2.2 In the present case, the claims of all requests were filed long after the statement of grounds of appeal. Thus the board had to examine whether the requests were admissible under Article 13(1) RPBA. They were filed in the last phase of the written appeal proceedings, one month before before the oral proceedings. They were part of the appellant's last submission as to the substance.

2.3 Claim 1 of the **main request** has been amended, compared with claim 1 of the main request underlying the decision, by a minor reformulation which specifically deals with the objections under Article 84 EPC 1973 raised in the board's communication. This amendment did not raise new issues, and the board expected that it could deal with the main request in the oral proceedings despite the appellant's absence. Thus, the new main request did not increase the complexity of the case or cause procedural problems. Under these circumstances, the board, exercising its discretion under Article 13(1) RPBA, decided to admit the appellant's main request into the appeal proceedings.

3. Main request: clarity (Article 84 EPC 1973)

3.1 It is undisputed that claim 1 of the main request is worded in such a way as to include a multitude of options. This is a consequence of the negative formulation "not encrypting an initial portion of each of the blocks" in combination with the feature that the initial portion includes all or a portion of the header of the block.

3.2 Thus, examples of such options are as follows:

- A first option is, for each block in one frame, not encrypting all of the header.
- A second option is, for each block in one frame, not encrypting only a portion of the header.
- A third option is, for only some of the blocks in one frame, not encrypting all of the header.
- A fourth option is, for only some of the blocks in one frame, not encrypting only a portion of the header.

3.3 A multiplication of these examples arises from the fact that there are several frames in the media data and different options may occur in different frames. Indeed, the encryption parameters may be provided on a per frame or even per block basis, with each frame or block having a different set of encryption parameters (see paragraph [0050] of the application).

3.4 In the first and third options, a given block header is entirely unencrypted or only partly encrypted. In the second and fourth options, a given block header is entirely unencrypted or entirely encrypted. Thus, for a given block header, all possibilities of encrypting, partly encrypting, and not encrypting the block header are encompassed.

3.5 Also, the description does not clarify the meaning of this negative formulation, but additionally introduces further options. In this context, the relevant portions of the description are paragraphs [0056] and [0057] of the application, which describe partially encrypted blocks illustrated in figures 6A and 6B. These paragraphs disclose that the initial offset may be larger than the entire header of a block or not. Typically, a block will include various items of standard header information **at the beginning** of the block (see paragraph [0056], "standard" referring to compression standards, such as H.264, see paragraph [0050]). It follows that for the blocks envisaged in the present application the entire header may be unencrypted or only a part of the header may be unencrypted. Moreover, paragraph [0057] describes an embodiment in which the initial offset (X) is zero for blocks which are not the first block of a given frame. This is confirmed in paragraph [0058], which discloses that "In the case in which the offset parameter X is only used in the initial block of a given frame (as opposed to every block in the frame), then the percentage of encryption being performed can be estimated to be Y divided by Y + Z." Thus, the initial offset may be zero for blocks which are not the first blocks in a frame. This means that there may be no unencrypted initial portion in some of the blocks, depending on where they are located in the frame. On the other hand, one particular block in a frame (partial block PB) is not encrypted (see paragraphs [0049] and [0052]).

3.6 The appellant's argument that claim 1 could be understood as covering the above four options (which were all disclosed in the application) and that this indicated that the claim was clear did not convince the board. In the context of the application, the claim covers further options, leading to a multitude of options well beyond those identified above. This multitude is not clearly defined.

3.7 Also, the argument that claim 1 allowed different encryption options to occur in different frames and that this did not induce a lack of clarity did not convince the board that the claim is clear. The possibility of different encryption options in different frames results in an uncertainty as to which scenario is used in which frame, and the application does not disclose any criteria for deciding which scenario may be applied in which frame.

3.8 Also, the argument that claim 1 did not encompass the case of the header being entirely encrypted did not convince the board. First, there is no unambiguous definition of "the header" because there are typically many block headers in the media data. Second, the application discloses an embodiment of the invention in which the offset may be zero, i. e. the initial portion of a block (which typically includes the block header) may be encrypted (see paragraph 3.5 above). If this argument is understood to mean that there must be, in the encrypted media data, at least one block whose header is not entirely encrypted, it still does not explain which block this might be and which part of this block's header is unencrypted.

3.9 Thus, the unencrypted portion of the media data (and consequently the complementary encrypted portion) is not clearly defined.

3.10 In view of the above, the board finds that claim 1 of the main request is not clear (Article 84 EPC 1973).

4. First auxiliary request: admission (Article 13(1) RPBA)

4.1 Claim 1 of the first auxiliary request has been amended, compared with claim 1 of the main request underlying the decision under appeal, by omitting the feature which had been objected to in the board's communication. Thus the negative formulation "not encrypting an initial portion of each of the blocks including all or a portion of the header" is not present in claim 1 of the first auxiliary request. Instead, claim 1 now specifies the content of the portion to be encrypted ("wherein the portion is a portion at least of the symbols ...", wherein the symbols are symbols for encoding the media file).

4.1.1 These amendments lead to new issues. Whereas the board's objection (as far as Article 84 EPC 1973 was concerned) essentially related to the question of which portion of which block was encrypted and which portion of which block was unencrypted, present claim 1 raises fresh issues relating to the content of the encrypted portion. This increases the complexity of the case.

4.1.2 Moreover, if the first auxiliary request were admitted, the question would arise whether omitting the feature comprising the negative formulation from claim 1 actually overcomes the objection raised in the board's communication. The board notes that claim 1 of both the main and the first auxiliary request make reference to "an initial offset amount into a block to be utilised when encrypting the block".

4.1.3 Also, the appellant indicated in its letter of 9 October 2015 that support for the amendment specifying the content of the portion to be encrypted could be found in paragraph [0056] of the application, and that it was implicit from a part of this paragraph that the encrypted portion extended beyond the header and into the rest of the block. Thus, examination of whether the requirements of Article 123(2) EPC are met would involve an assessment of what is implicit in paragraph [0056]. This also increases the complexity of the case.

4.1.4 Furthermore, the appellant indicated in its letter dated 9 October 2015 that the inventive step of the claimed method was based on the effect that encryption effort could be expended. Hence, at least the amendment consisting in omitting the step of not encrypting an initial portion of each of the blocks also may have a bearing on the assessment of inventive step.

4.2 Taking into account the above issues and the fact that, due to the appellant's absence, these issues could not be discussed during the oral proceedings, the board did not expect to be able to deal with all the issues concerning the first auxiliary request in the oral proceedings, which meant that procedural economy would have been impaired had the first auxiliary request been admitted.

4.3 In view of the above, the board, exercising its discretion under Article 13(1) RPBA, decided not to admit the appellant's first auxiliary request into the appeal proceedings.

5. Second auxiliary request: admission (Article 13(1) RPBA)

5.1 Claim 1 of the second auxiliary request also does not include the negative formulation "not encrypting an initial portion of each of the blocks including all or a portion of the header" objected to in the board's communication. Like claim 1 of the first auxiliary request, it also specifies the content of the portion to be encrypted ("wherein the portion includes at least some of the symbols ...", wherein the symbols are symbols for encoding the media file).

5.1.1 The appellant indicated that support for this amendment could be found in paragraph [0056] of the application, and that it was implicit from a part of this paragraph that the encrypted portion extended beyond the header and into the rest of the block.

5.1.2 Thus the considerations under points 4.1.1 to 4.1.4 and 4.2 above also apply to claim 1 of the second auxiliary request.

5.2 In view of the above, the board, exercising its discretion under Article 13(1) RPBA, decided not to admit the appellant's second auxiliary request into the appeal proceedings.

6. *Third auxiliary request: admission (Article 13(1) RPBA)*

Claim 1 of the third auxiliary request is based on claim 1 of the second auxiliary request underlying the decision under appeal and has essentially the same minor reformulation as claim 1 of the main request. Thus, the board, for the reasons given in section 2 above, exercising its discretion under Article 13(1) RPBA, decided to admit the appellant's third auxiliary request into the appeal proceedings.

7. *Third auxiliary request: clarity (Article 84 EPC 1973)*

7.1 Claim 1 of the third auxiliary request corresponds to claim 1 of the main request, with the following feature appended at the end: "; wherein each of the blocks (B1, B2, B3, BP) are the same size, and wherein at least a plurality of the frames (F1, F2, F3, F4, F5) within the media data have different sizes."

7.2 The additional feature does not specify an additional step of the encrypting method, but instead further defines the media data, in particular the sizes of the frames and blocks, to which the encrypting method is applied.

7.3 Thus the considerations under points 3.1 to 3.5 above also apply to claim 1 of the third auxiliary request.

7.4 The appellant's arguments concerning the clarity of claim 1 of the third auxiliary request are the same as those submitted in the context of the main request (see page 8 of the letter of 9 October 2015). Thus the considerations under points 3.6 to 3.9 above also apply to claim 1 of the third auxiliary request.

7.5 In view of the above, the board holds that claim 1 of the third auxiliary request is not clear (Article 84 EPC 1973).

8. Since the first and second auxiliary requests are not admitted and the main and third auxiliary requests are not allowable, the appeal must be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

Beschwerdekammern des Europäischen Patentamts ✦ Boards of Appeal of the European Patent Office ✦ Chambres de recours de l'Office européen des brevets

K. Boelicke B. Müller

Decision electronically authenticated