Internal distribution code:

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

Datasheet for the decision of 2 March 2018

Case Number: T 1966/12 - 3.5.04

Application Number: 09772427.2

Publication Number: 2297948

IPC: H04N7/16, H04L29/06, H04L9/06

Language of the proceedings: EN

Title of invention:
Methods and apparatuses for selective data encryption

Applicant:
Thomson Licensing

Headword:

Relevant legal provisions:
EPC Art. 56
EPC R. 111(2)

Keyword:
Inventive step - main and auxiliary requests (no)
Requirement of a reasoned decision (yes)

Decisions cited:

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: T 1966/12 - 3.5.04

D E C I S I O N
of Technical Board of Appeal 3.5.04
of 2 March 2018

Appellant: (Applicant)	Thomson Licensing 1-5, rue Jeanne d'Arc 92130 Issy-les-Moulineaux (FR)
Representative:	Huchet, Anne TECHNICOLOR 1-5, rue Jeanne d'Arc 92130 Issy-les-Moulineaux (FR)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 15 May 2012 refusing European patent application No. 09772427.2 pursuant to Article 97(2) EPC**

Composition of the Board:

Chairwoman	T. Karamanli
Members:	R. Gerdes
	A. Dumont

Summary of Facts and Submissions

I. The appeal is directed against the decision to refuse European patent application No. 09 772 427.2, published as international application WO 2010/000727 A1.

II. The patent application was refused by the examining division on the grounds that the subject-matter of claim 1 of the main request and of the auxiliary request lacked inventive step in view of:

D1: Kunkelmann T. et al.: "A Scalable Security Architecture for Multimedia Communication Standards", IEEE International Conference on Multimedia Computing and Systems '97, Proceedings, Ottawa, Ontario, Canada, 3 to 6 June 1997, Los Alamitos, CA, USA, IEEE Comput. Soc., US, pages 660-661, XP010239268.

In addition, the examining division found that claim 1 of the auxiliary request lacked clarity.

III. The applicant appealed against this decision and with its statement of grounds of appeal submitted claims of a main request and first and second auxiliary requests. These claims were based on those of the auxiliary request underlying the decision under appeal.

IV. The board issued a summons to oral proceedings and in an annex to the summons indicated *inter alia* that it doubted that the subject-matter of claim 1 according to all of the appellant's requests involved an inventive step (Article 56 EPC).

V. In response, with a letter dated 31 January 2018, the appellant submitted amended claims of a main request

and re-filed the claims of the first and second auxiliary requests.

VI. Oral proceedings were held before the board on 2 March 2018. As announced beforehand, the appellant was not represented at them. The chairwoman noted that the appellant had requested in writing that the decision under appeal be set aside and that a patent be granted on the basis of the claims of the main request or, in the alternative, of one of the first and second auxiliary requests, all requests as filed with the letter dated 31 January 2018.

She also noted that, according to the file, the appellant had alleged that a procedural error had occurred in the first-instance proceedings, but it had not requested reimbursement of the appeal fee.

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

"A method of decryption of an encrypted message [M] using a decryption key with key length k, the method comprising the steps, at a decryption device (910), of:

- determining if the encrypted message [M] is longer than, as long as or shorter than the key length k;

- in case the encrypted message [M] is longer than the key length k: decrypting exactly k bits of the encrypted message [M];

- in case the encrypted message [M] is as long as the key length k: decrypting the k bits of the encrypted message [M]; and

- in case the encrypted message [M] is shorter than the key length k:

  - concatenating the encrypted message [M] with at least one further encrypted message in order to obtain a lengthened message at least k bits long; and

  - decrypting exactly k bits of the lengthened message."

VIII. Claim 1 of the first auxiliary request is identical to claim 1 of the second auxiliary request. These claims differ from claim 1 of the main request in the first and penultimate features, which have been amended to read (additions marked in bold, deletions in strike-through):

"A method of decryption of an encrypted message [M] using a decryption key **K** with key length k, **the encrypted message [M] being payload of a packet and comprising encrypted data of a bit stream**, the method comprising the step~~s~~, at a decryption device (910), of:

...

- in case the encrypted message [M] is shorter than the key length k:

  - concatenating the encrypted message [M] with at least one further encrypted message in order to obtain a lengthened message at least k bits long, **the at least one further encrypted message comprising encrypted data of the bit stream and being payload of a further packet**; and

- decrypting exactly k bits of the lengthened message."

IX. In the decision under appeal the examining division held that the subject-matter of claim 1 of the then main request was distinguished from D1 by the step of "determining if the length of the at least [one] message M is longer, equal to or shorter than the key length k". This feature was "directed towards checking the size of a message against the size of the data to be encrypted from said message." The technical problem was therefore to avoid memory allocation errors when encrypting data. Checking the size of the data to be encrypted in order to avoid memory allocation errors was "common practice for both hardware and software implementations". In any case, block encryption required the block to be of a certain size; hence checking the block size was obvious (see Reasons, point 2.1.1).

The subject-matter of claim 1 of the then auxiliary request differed from claim 1 of the then main request in that it related to a decryption method corresponding to the encryption method of the main request. D1 disclosed that its encryption method had a corresponding decryption method (see Reasons, point 2.2.2).

X. The appellant's arguments which are relevant for the present decision may be summarised as follows:

D1 failed to disclose determining if the encrypted message was longer than, as long as or shorter than the key length k. It also failed to disclose the concatenating and subsequent decrypting steps of

claim 1 (see statement of grounds of appeal, pages 5 and 6).

The technical effect of the difference was that it enabled a certain level of security to be maintained. The corresponding technical problem was how to keep a certain security level in the encrypted messages. Another technical effect was that the amount of encryption was minimised while the security level was maintained. The corresponding technical problem was one of how to minimise encryption while keeping a certain level of security, how to further reduce encryption, or how to provide an alternative way of reducing encryption. The solution to these problems was not obvious from D1, since the method according to D1 operated on coefficients. It was not known in D1 how long the n coefficients would be once they were coded. Therefore, the method according to D1 had to perform various checks, e.g. "are all the bits marked 'to encrypt'?" and "have the n coefficients been marked as 'to encrypt'?" (see statement of grounds, pages 6 and 7).

With respect to the example in D1 (see figure 1) the appellant accepted that it seemed reasonable to interpret the second DCT block as a message "shorter than the key length k", and the spilling over from the second DCT block as a concatenation of the second and third DCT blocks. However, 2N bits were encrypted in this lengthened message, while the claim clearly required encrypting exactly k bits. It followed that the omission from D1 of the condition that a minimum number of DCT coefficients had to be encrypted did not provide the solution of claim 1 (see letter of reply dated 31 January 2018, page 4).

The appellant also argued that it had been deprived of a chance to argue against the examining division's decision. The technical problem had been formulated without identifying any technical effect provided by the difference between claim 1 and the closest prior art. At least, such a technical effect had not been communicated to the appellant (see statement of grounds, page 6, last paragraph).

Reasons for the Decision

1. The appeal is admissible.

The invention

2. The invention relates to partial encryption of a bitstream, in particular to partial encryption of image data such as in the JPEG2000 image compression standard and coding system.

To ensure a minimum encryption ratio that guarantees cryptographic security, it is recommended that the encrypted part of a message is at least as long as the encryption key, i.e. of length k. If a message is shorter than the encryption key, this message may be concatenated with at least one further message such that the lengthened message contains a sufficient number of bits for encryption. Messages may be the payload of packets that are used to transmit the bitstream (see pages 1 and 9 to 12 of the application as published).

Main request

3. It is common ground that D1 may be considered the closest prior art with respect to the subject-matter of claim 1.

3.1 D1 discloses a method of partial en/decryption applied to video data compressed using a JPEG video compression standard (see D1, abstract and chapter 1). The encryption method operates on DCT (discrete cosine transform) coefficients, taking advantage of the decreasing importance of coefficients in an image block by encrypting at least the first N bits of each DCT block (page 660, step 2 of the algorithm at the bottom of the right-hand column). N is the block size of the encryption method used; e.g. for the DES encryption method N is equal to 64. If the DCT coefficients of an image block contain fewer than N bits, encryption continues on the next block of DCT coefficients. D1 additionally requires a minimum number of DC and AC coefficients to be encrypted (step 1 of the algorithm). D1 describes a secure conferencing gateway with an encryptor using the encryption method and a decryptor using the corresponding decryption method (see chapter 4).

3.2 In its statement of grounds of appeal, page 5, lines 17 to 30, the appellant argued that D1 failed to disclose the following features:

(a) determining if the encrypted message [M] is longer than, as long as or shorter than the key length k,

(b) decrypting exactly k bits of the encrypted message (of a message that is longer than the key length k) and

(c) concatenating the encrypted message with at least one further encrypted message in order to obtain a lengthened message at least k bits long; and decrypting exactly k bits of the lengthened message (if the "encrypted message" is shorter than the key length k).

3.3 The method step of feature (a) is comparable to step 3 of the algorithm at the top of the left-hand column on page 661 of D1. The board considers the difference to reside in the fact that claim 1 requires a comparison of the length of the (encrypted) message with the key length k, which is not explicitly disclosed in step 3.

The concatenation of messages as specified in feature (c) is implicitly disclosed in D1 (see page 660, last paragraph of the right-hand column, step 2). Step 2 requires the retrieval of N bits (corresponding to the key length k in claim 1) from one or more blocks of DCT coefficients (corresponding to messages in claim 1). Hence, it presupposes the concatenation of these coefficients/messages.

However, the board agrees with the appellant that D1 does not show the decryption of exactly k bits in the case of features (b) and (c). Instead, the decryption in D1 uses two conditions to determine the bits which are to be decrypted. Firstly, the number of bits has to be at least N (and a multiple of N), and secondly, a minimum number of n_i or n_m DCT coefficients has to be encrypted.

3.4 The comparison of the length of the (encrypted) message with the key length k as specified in feature (a) relates to an implementation issue of how to determine

which bits of the current (and where necessary of the next) message are to be encrypted. The solution of determining in an intermediate step whether the current message is longer than, as long as or shorter than the key length k is straightforward for the skilled person, if not implicit. Marking bits of DCT coefficients as "to encrypt" requires awareness of when a DCT block is fully marked and when marking should continue on the next block. Regarding feature (a) the board also considers the reasoning in the decision under appeal to be conclusive (see point IX above).

3.5 Hence, the essential difference between claim 1 and D1 resides in the fact that the en/decryption method of D1 contains an additional rule which is taken into account for determining which bits to en/decrypt. In other words, the method of D1 is simplified by neglecting the second condition of its encryption algorithm.

3.6 The board considers the technical effect of features (b) and (c) to be a simplification of the algorithm of D1. The technical problem can accordingly be formulated as how to simplify the en/decryption of D1.

3.7 This simplification has foreseeable advantages and disadvantages, such as reduced computing effort and correspondingly decreased cryptographic security. As a consequence, the board regards the omission of the second condition of the algorithm of D1, i.e. en/decryption of a minimum number of n_i or n_m DCT coefficients, as being obvious in view of D1 and the common general knowledge of the skilled person.

3.8 The appellant alleged that features (b) and (c) had the technical effect of maintaining a certain level of security (see statement of grounds, page 7, lines 1 to 4). The board cannot agree that this effect is achieved over D1, because according to D1 at least N bits are encrypted, which is at least as secure as encrypting exactly N bits.

The appellant also argued that the amount of encryption was minimised while the security level was maintained. This assertion seems to be based on the intrinsic property of JPEG2000 or similar standards using "Codeblock Contribution to Packet" (see description, page 9, first paragraph of the "preferred embodiment").

Such a requirement of the encrypted data is, however, not apparent from claim 1. It is also noted that D1 starts from the same presumption as the invention, i.e. decreasing importance of transmitted data for the image composition, which allows encryption of only the first few of them (see D1, page 660, left-hand column, abstract, chapter 1, and right-hand column, first paragraph of chapter 3).

The appellant emphasised that D1 operated on coefficients. It was not known in D1 how long the n coefficients would be once they were coded. Therefore, D1 had to perform various checks, e.g. "are all bits marked 'to encrypt'?" and "have the n coefficients been marked as 'to encrypt'?" (see statement of grounds, pages 6 and 7). In this respect it is noted that D1 and claim 1 both assume a coded bitstream, "messages" or a "video stream" as input to the en/decryption. Hence, the board cannot see that the messages of claim 1 consist of different data than those of D1.

With respect to the example in D1, figure 1, the appellant accepted that it seemed reasonable to interpret the second DCT block as a message "shorter than the key length k", and the "spilling over" from the second DCT block as a concatenation of the second and third DCT blocks. However, 2N bits were encrypted in this lengthened message, while the claim clearly required encrypting exactly k bits. It followed that the omission from D1 of the condition that a minimum number of DCT coefficients had to be encrypted did not provide the solution of claim 1 (see letter of reply dated 31 January 2018, page 4).

The board agrees with the appellant's interpretation of D1, figure 1. However, claim 1 relates to the decryption of a (single) encrypted message, i.e. it does not contain any requirement as to how to proceed with subsequent messages. In particular, it does not specify how the "at least one further message" is to be handled after being concatenated and encrypted together with the "encrypted message". Claim 1 does not exclude the possibility that the "at least one further message" is subjected to further en/decryption.

The board in fact interprets the application (see page 11, last paragraph, to page 12, second paragraph) as saying that the encrypted part of each message should be at least as long as the encryption key k. If the "at least one further encrypted message" were to be exempted from further en/decryption, an extreme case could arise in which only one bit of the "at least one further encrypted message" would be encrypted (for example, if the key length was 128 bits and the "encrypted message" had only 127 bits). An encryption of the "at least one further encrypted message" modifying only one bit of that message would clearly

not meet the requirement for the encrypted part of a message to be at least as long as the encryption key k. It follows that "decrypting exactly k bits of the lengthened message" in claim 1 has to be interpreted as meaning that exactly k bits are decrypted when decrypting the "encrypted message". However, the claim is silent on whether the "at least one further encrypted message" (or some of it) is decrypted separately in another decrypting step (as in D1, figure 1).

Hence, the board was not convinced by the appellant's arguments.

3.9 As a result, the subject-matter of claim 1 would have been obvious to a person skilled in the art in view of D1 and thus lacks inventive step (Article 56 EPC).

First and second auxiliary requests

4. Claim 1 of the first auxiliary request is identical to claim 1 of the second auxiliary request. These claims essentially differ from claim 1 of the main request by specifying the following additional features:

(a) the encrypted message [M] being payload of a packet and comprising encrypted data of a bitstream and

(b) the at least one further encrypted message comprising encrypted data of the bitstream and being payload of a further packet.

4.2 The feature whereby the encrypted message and the further encrypted message comprise encrypted data of a bitstream is disclosed in D1, see figure 1. The

transmission of messages in packets is common practice in video transmission.

4.3 As a result, the board finds that the subject-matter of claim 1 according to the first and second auxiliary requests lacks an inventive step (Article 56 EPC).

Alleged procedural violation

5. In the statement of grounds of appeal, see page 6, last paragraph, the appellant stated that it had been deprived of a chance to argue against the examining division's decision. The technical problem had been formulated without identifying any technical effect provided by the difference between claim 1 and the closest prior art. At least, such a technical effect had not been communicated to the appellant.

5.1 The board considers this objection against the decision under appeal as an objection under Rule 111(2) EPC. According to established jurisprudence of the boards of appeal, the reasoning given in a decision open to appeal has to enable the appellant and the board of appeal to examine whether the decision was justified or not. A decision should discuss the facts, evidence and arguments which are essential to the decision in detail, and it has to contain the logical chain of reasoning which led to the relevant conclusion (see Case Law of the Boards of Appeal of the European Patent Office, 8th edition 2016, section III.K.4.2.1).

5.2 The technical effect and the technical problem are closely linked. In the decision under appeal the technical problem was formulated as "to avoid memory allocation errors when encrypting data". The board considers it to be implicit and immediately clear for

the experienced practitioner that the technical effect could be similarly formulated as avoiding memory allocation errors when encrypting data. Hence, the technical effect of distinguishing feature (a) can easily be derived from the reasoning in the decision under appeal. As a result, the board disagrees with the appellant's statement that it had been deprived of a chance to argue against the examining division's decision.

In addition, in the present case the technical effect of distinguishing feature (a) was not the essential, decisive issue on which the present appeal is based. The arguments in the statement of grounds of appeal do not address the technical effect of distinguishing feature (a), but concentrate on the alleged further distinguishing features (b) and (c), their resulting technical effect(s) and the associated technical problem (see pages 6 and 7).

5.3 Hence, the board is not convinced that a procedural violation occurred in the first-instance proceedings.

Conclusion

6. It follows from the above that none of the appellant's requests is allowable and that no fundamental deficiency is apparent in the first-instance proceedings. Therefore, the appeal is to be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairwoman:

L. Stridde T. Karamanli

Decision electronically authenticated