BESCHWERDEKAMMERN	**BOARDS OF APPEAL OF**	**CHAMBRES DE RECOURS**
DES EUROPÄISCHEN	**THE EUROPEAN PATENT**	**DE L'OFFICE EUROPEEN**
PATENTAMTS	**OFFICE**	**DES BREVETS**

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

Datasheet for the decision of 17 December 2008

Case Number: T 1030/06 - 3.5.01

Application Number: 03021759.0

Publication Number: 1403770

IPC: G06F 12/14

Language of the proceedings: EN

Title of invention:
System and method for securely buffering content

Applicant:
Broadcom Corporation

Opponent:
-

Headword:
Secure buffering/BROADCOM CORPORATION

Relevant legal provisions:
-

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

Keyword:
"Inventive step - skilled person - must be expected to carry out implementation steps"
"Inventive step - providing multiple processing units and common frame buffer in video processing apparatus (no)"
"Inventive step - providing direct connection between processing units - (no - self-evident)"
"Inventive step - use of different encoding schemes (no - routine design)"
"Inventive step - providing data with originating information (no - routine design)"

Decisions cited:
T 0623/97

Catchword:
See point 20 of the reasons.

Europäisches
Patentamt

European
Patent Office

Office européen
des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Case Number: T 1030/06 **-** 3.5.01

D E C I S I O N
of the Technical Board of Appeal 3.5.01 of 17 December 2008

Appellant:

Broadcom Corporation
5300 California Avenue
Irvine, CA 92617 (US)

Representative:

Jehle, Volker Armin
Bosch Jehle Patentanwaltsgesellschaft mbH
Flüggenstraße 13
80639 München (DE)

Decision under appeal:

Decision of the Examining Division of the European Patent Office posted 12 April 2006 refusing European application No. 03021759.0 pursuant to Article 97(1) EPC 1973.

Composition of the Board:

Chairman: S. Steinbrener
Members: W. Chandler
P. Schmitz

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division to refuse the application on the grounds that the subject-matter of independent claims 1 and 6 of the main and first to third auxiliary requests did not involve an inventive step (Article 56 EPC 1973) over US-A-5 825 879 (D1) and the skilled person's common general knowledge.

II. In the statement setting out the grounds of appeal, the appellant requested that the decision be set aside and that a patent be granted on the basis of a newly filed main request, or first to third auxiliary requests, all being amended versions of the corresponding refused requests. The appellant also made an auxiliary request for oral proceedings. In addition, reimbursement of the appeal fee was requested in case the appealed decision was rectified pursuant to Article 109(1) EPC 1973.

III. In the communication accompanying the summons to oral proceedings, the Board summarised the issues to be discussed and tended to agree with the examining division that all requests lacked inventive step.

IV. At the oral proceedings before the Board, the appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the main, or auxiliary requests 1 to 3 filed with the grounds of appeal. The request for reimbursement of the appeal fee was not maintained. At the end of the oral proceedings, the Chairman announced the decision.

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

"1. A signal processing unit (100) for securely buffering content, comprising:
two or more processing units (190, 200) coupled to a bus (250), the first processing unit (190) including

a second device (210) for securing content being sent to a storage device (110) being coupled to the signal processing unit (100) and a first device (220) for recovering content from the secured content received from the storage device (110),

the second processing unit (200) including a third device (230) for securing content being sent to the storage device (110) and a fourth device (240) for recovering content from the secured content received from the storage device (110),

thus, before content leaves the signal processing unit (100) for the storage device (110), the signal processing unit (100) secures the content, and

after the secured content enters the signal processing unit (100) from the storage device (110), the signal processing unit (100) recovers the content from the secured content, characterized in that

the first processing unit (190) is adapted to sent (*sic*) content directly to the second processing unit (200) via the bus (250), and
both the first processing unit (190) and the second processing unit (200) separately provide copy protection to the content stored in the storage device (110) or to the content transported between these signal processing units (190, 200) and the storage device (110) by means of the first, second, third and fourth devices (210, 220, 230, 240)."

Claim 1 of the first auxiliary request adds to the end of claim 1 of the main request:
"wherein the second device (210) is adapted to secure content originating from the first processing unit (190) using a particular form of encryption, and the fourth device (230) is adapted to secure content originating from the second processing unit (200) is secured using a different form of encryption."

Claim 1 of the second auxiliary request replaces the feature added in the first auxiliary request by:
"wherein the first device (220) is adapted to decrypt a first kind of encryption, the second device (210) is adapted to perform a second kind of encryption, the third device (240) is adapted to decrypt said second kind of encryption and the fourth device (230) is adapted to perform a third kind of encryption."

Claim 1 of the third auxiliary request adds to the end of claim 1 of the second auxiliary request:
"the content is including origination information, and said first and fourth devices (220, 240) are adapted to recognize by means of said origination information included in the content, from which processing unit (190, 200) the secure content is coming."

VI. The appellant argued essentially as follows:

Dl addressed the specific problem of securing video frame data in a frame buffer by using only one frame data encryptor and retrieving it from the frame buffer for display by using only one frame data decryptor. Thus, in D1, the data flowed in only one direction through the frame buffer. D1 did not disclose or suggest the claimed possibility of a security device with two or more processing units that could separately exchange secure content via a storage device in a bidirectional manner. This resulted in higher performance.

The prior art did not mention any measure to evaluate if the processes resulted in timing differences requiring the use of a buffer. Thus there was no suggestion to exchange the secured content directly between the decrypting unit and the encrypting unit as claimed.

Dl took the necessity and the existence of a frame buffer as unavoidable and did not contemplate working without one. Hence, the disclosure of Dl even led away from this favourable solution, since it disclosed that processing of video content was always only in connection with buffering in a memory. The path 408 between the image generation device 400 and the image display device 404 in Figure 4 of D1 was only used to exchange session keys and not for the direct exchange of frame data or other content as claimed. A direct connection provided faster and more secure communication since no memory was involved.

If the Board maintained the assessment that it would be an obvious matter of routine design to send the content "directly" between the relevant processors it was respectfully asked to quote prior art documents which showed this.

Even if there was a double application of the arrangement of D1, as suggested by the examining division, there would be four processing units each having only one encryption or decryption device since D1 did not suggest using two separate devices for securing and recovering content in each processing unit. There would also only be one form of encryption and no direct connection.

The use of different encryption schemes in the frame buffer, as claimed in claim 1 of the auxiliary requests, improved the security of the buffering. None of the cited prior art contained any indication to use different forms of encryption in parallel. Furthermore, the prior art gave no indication how to handle different forms of encryption in parallel. The Board's argument in the communication that this measure would be a matter of routine design "depending on the circumstances" was vague and lacked any basis in the cited documents. Although the skilled person would be able to understand the invention and the prior art, he would not be able to further develop or create ideas.

An "unexpected effect" of using different forms of encryption clearly resided in the fact that the present invention provided a method or signal processing unit wherein different security schemes could be used simultaneously. The selection of security schemes could be preset or could be based upon, content type, content rate, origin of content or destination of content.

As another advantageous effect, subject of claim 1 of the third auxiliary request, the devices 220, 240 could recognise by means of origination information in the content from which processing unit the secure content was coming (see end of paragraph [0049] of published application).

The Board's view that this would be a self-evident requirement for a system with more than one processing unit resulted from an undue ex-post analysis. A skilled person could not have derived from the prior art the requirement for a system with more than one processing unit with the same tasks. Furthermore, a skilled person could not have taken from the prior art how to distribute specific processing tasks.

As a general point, obviousness could not be "accumulated" through the auxiliary requests and the skilled person should be able to derive all the characterising features of the relevant claim of each request starting from scratch.

Reasons for the Decision

1. The appeal complies with the requirements referred to in Rule 65(1) EPC 1973 and is therefore admissible.

The application

2. This application concerns the problem of securing data stored in an external storage device used to buffer intermediate results between processing stages, for example, of a signal processor in a set-top box (see application, paragraphs [0003] and [0004]). The basic idea of the invention is to encrypt the data to be stored before it leaves the signal processor and decrypt it again after reading it (see Figure 3 and paragraphs [0044] and [0045]).

3. Claim 1 of the refused main request concerned the embodiment of Figure 4 that has two processors 190, 200 that each encrypt and decrypt the data written and read to the storage device 110 (see paragraph [0046]). The auxiliary requests added the aspects of using different forms of encryption and recognising the origin of the content.

4. In appeal, the claimed idea in each request has been further expanded to include the possibility that in addition to sending data via the storage device 110, the first processor 190 can send it directly to the second processor 200 via a bus 250 (see column 8, lines 51 to 53 and column 9, lines 28 to 34 and 38 to 43).

The prior art

5. It is common ground that D1 discloses a secure video content processor using a hardware-based security "envelope" that encapsulates encrypted digital data from the time it is submitted to a computer for decoding and decompression until the time it is provided to a display device in an analog form. When data exits the hardware envelope in digital form, e.g. for buffering in the frame buffer, it is encrypted before exiting the envelope and then decrypted when the data returns to the hardware envelope. By protecting the data over the entire processing flow, an unauthorized copier will find it more difficult to "capture" the unencrypted digital representation (see column 2, lines 49 to 64).

Inventive step

6. The appellant has four requests, claim 1 of each request being successively more restricted. These were discussed in the oral proceedings before the Board in order. During the discussion of the last request, the appellant voiced the impression that the obviousness of the features was being "accumulated" through the various requests and argued that the skilled person should be able to derive all the characterising features of the relevant claim of each request starting from scratch. The Board agrees with this and accordingly for the avoidance of any doubt will first deal with claim 1 of the third auxiliary request, which contains all of the features in question.

7. The examining division found the claims before them obvious under two different interpretations of D1. Firstly, at point 2 of the decision, they considered the secure video content processor (SVCP) of Figure 3 as being the first processing unit of the claim, having a device for securing content (frame data encryptor 320) being sent to a storage device (frame buffer 300) and a device for recovering content (frame data decryptor 324) received from the storage device. The arrangement of the refused claim differed by having a second identical processing unit connected to the frame buffer.

8. According to the examining division's "second mapping" at point 5 of the decision, the SVCP body 401 of Figure 4 has two processing units (400 and 404), the first having a device for securing content (frame data encryptor 424) being sent to a storage device (frame buffer 428) and the second a device for recovering

content (frame data decryptor 444) from the storage device. The division also identified a device for recovering data (decryptor 416) in the first processing unit and a device for securing data (D/A converter 448) in the second processing unit. The arrangement of the refused claim then differed in that these additional devices for securing and receiving data were connected to the storage device.

9. In appeal, it is common ground that starting from D1, claim 1 of the third auxiliary request differs in that:

i) there is a second identical processing unit connected to the frame buffer, or that the additional devices for securing and receiving data are connected to the storage device (depending on the chosen "mapping");
ii) the first processing unit can send content directly to the second processing unit via a bus;
iii) the first device is adapted to decrypt a first kind of encryption, the second device is adapted to perform a second kind of encryption, the third device is adapted to decrypt said second kind of encryption and the fourth device is adapted to perform a third kind of encryption;
iv) the devices for recovering content recognize by means of origination information included in the content, from which processing unit the secure content is coming.

Feature iii) deserves some explanation since there is a mix-up in the naming of the third and fourth devices in the claim. The feature essentially specifies that the devices for securing content in the two processing units use different (second and third) forms of encryption and the second processing unit can decrypt data encrypted by the first processing unit. The device for recovering content in the first processing unit uses yet another (first) kind of encryption.

10. The Board considers that the latter part of the examining division's "second mapping" concerning the identification of the additional devices for recovering and securing data is not relevant, and that it is immaterial whether the starting point of D1 is considered to be a single processor with two devices or two processors each with one device (first part of "second mapping"). This is because in the Board's view, the problem solved in both cases is the general one of how to implement a video processing apparatus that securely uses a frame buffer.

11. Concerning the use of several processors, the Board does not agree with the appellant that this is not suggested by D1. Firstly, the opening part of the description of D1 at column 1, line 64 to column 2, line 1, indicates the generally well-known fact that digital video processing usually involves multiple processing stages that provide many opportunities to capture the data. Given that, as mentioned above, the invention may relate to a set-top box, which is one of the more general implementations mentioned in D1 at column 7, lines 16 to 19, the Board considers that D1 implies that a video signal processing unit would generally involve several processors. Secondly, D1 discloses at column 1, lines 44 to 48 the equally well-known fact that the above-mentioned processing stages often result in timing differences which necessitate a

frame buffer memory. In the Board's view, this implies that, in general, neighbouring processors in a signal processing application that involve timing differences would need to be connected via a frame buffer in the manner of D1, Figures 3 or 4. Thus, it would be obvious to consider implementing the video processing apparatus using several processing units and a common frame buffer.

12. Since the general idea of D1 is to encode the data before it exits the hardware envelope (of the processors) and decode it when it returns in order to protect it over the entire processing flow (see point 5, above), the Board considers it self-evident that the processors that use the buffer to overcome timing differences would each require a device for recovering content and a device for securing content, as in difference i) above.

13. Moreover, it follows by analogy that if two neighboring processes do not result in timing differences, they do not need to be connected via the frame buffer. In this case, the Board considers that it would be an obvious alternative to send the content "directly" between the relevant processors via a bus, according to difference ii).

14. The appellant’s arguments essentially all rely on the fact that D1 does not disclose the features that the multiple processing units exchange data either with the storage device in a bidirectional manner, or directly. However, again, such an explicit disclosure is not necessary since as explained above the Board finds that the features follow in an obvious manner having decided

to use several processors. In particular, the Board does not consider that D1 leads away from a direct connection, by the fact alone that it does not disclose one. Similarly, the Board does not think that it is necessary to quote prior art to show that a direct connection is an obvious possibility for transferring data between two devices.

15. The appellant considers that the feature of using different encryption schemes in difference iii) solves the problem of improving security. However, although the application deals with and mentions security in general, the Board cannot find any mention of this problem as being the result of the use of different encryption schemes. Moreover, the Board doubts that this feature alone would necessarily solve this problem since the security also depends on the strength of the additional schemes. On the other hand, the passage at paragraph [0049] of the application that discusses the selection of security schemes states:

> The selection of security schemes may be preset or may be based upon, for example, content type, content rate, origin of content or destination of content. For example, content originating from the first processing unit 190 may use a particular form of encryption while content originating from the second processing unit 200 may use a different form of encryption.

In the Board's view, the variety of criteria presented in this passage confirms that choosing an encryption scheme is also a necessary consequence of having decided to use several processors.

16. Moreover, the Board agrees with the examining division that the use of different encryption schemes is a matter of routine design depending on the circumstances. In this case, the circumstances that the skilled person would consider would include those mentioned in the above mentioned passage, e.g. type, rate, origin and destination of the content. Thus, in trying to implement a signal processing unit with two or more processing units sending and receiving secured content to and from the frame buffer, the skilled person would have to consider the circumstances of the content and provide an appropriate security scheme for the content to and from each processing unit.

17. It is self-evident that if one processing unit needs to process data from another processing unit, which is typically the case in a digital processing system using a sequence of interconnected processing stages, then it must be able to decrypt it. Thus for two processing units containing four encrypting/decrypting devices with one pair having a common encoding scheme, there could be up to three encoding schemes in total, which is all that is claimed in difference iii).

18. The appellant considers that the Board’s argument in the communication that this measure would be a matter of routine design "depending on the circumstances" is vague and lacks any basis in the cited documents. However, in the present case, the skilled person is a design engineer in the field of video processing. For such a person the choice of an encryption scheme is more like the choice of a fastener for a mechanical engineer. The choice depends on the required strength,

ease of implementation, cost etc. Various encryption schemes are known, having different properties, and the skilled person would choose the most appropriate for the type of data and the importance of the data at the relevant stage of the processing. This is what is meant by "depending on the circumstances". For example, data defining the whole image would need to be better protected than data defining only parts of an image, e.g. motion vectors from a motion estimation stage. The fact that different security schemes could be used simultaneously is not an "unexpected effect" that the Board might be able to recognise as an indication of inventive step. Firstly, it is not unexpected, but a direct, predictable consequence of using different forms of encryption. Secondly, as concluded above, it would follow in an obvious manner from the desire to protect different types of data.

19. The use of origination information identifying the source of data according to difference iv) is a common technique in data transmission schemes and the skilled person would consider using it if the origin of the data needs to be known and was not otherwise derivable. As pointed out by the examining division, this would not be required if only two processors are used as in the embodiments, but would be needed in the case of a conventional video processing system with more than two units sharing a common memory according to the problem being solved in the present case.

20. The appellant argued generally that although the skilled person would be able to understand the invention, he would not be able to develop further or create ideas. The Board can only agree with this

statement up to a point. The skilled person is a person of ordinary skill in the art which means not only having access to the state of the art and common general knowledge in the field, but also the capability to perform routine work and experimentation. Thus, the skilled person can be expected to seek out solutions and make choices to try to solve design problems that crop up. In the Board’s view, this is particularly so where the problem is to come up with an implementation of an apparatus having certain required functions as in the present case. The implementation of the first part of the solution (here the provision of several processors) often leads to further design decisions that must be made (here the choice of encryption scheme and the identification of the source of data) in order to produce a working system. The skilled person cannot be expected to abandon the implementation half-way through in the form of a "black box" with undefined means for carrying out the required functions, but must attempt if possible to put such means into practice using knowledge available to him (see also T 623/97 of 11 April 2002, at point 4.4). These would literally be "further ideas" in the sense that they could be new in the given context, but they should be routine and thus not inventive.

21. In summary, the Board considers that the claimed invention is an obvious solution to the problem of implementing a video processing apparatus that securely uses a frame buffer. In particular, the distinguishing features of a direct connection, different forms of encryption and recognising the origin of the data are all known, routine steps, displaying no synergetic or surprising effects. The skilled person would consider

these steps to solve design problems that would necessarily have to be solved in the implementation process.

22. Accordingly, the subject-matter of claim 1 of the third auxiliary request does not involve an inventive step (Article 56 EPC 1973). Since this is the most restricted claim, the same finding applies to the more general main, first and second auxiliary requests.

23. There being no further requests, it follows that the appeal must be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar:	The Chairman:
T. Buschek	S. Steinbrener