

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
2 October 2008 (02.10.2008)

PCT

(10) International Publication Number
WO 2008/116779 A1

(51) International Patent Classification:
G06F 21/00 (2006.01)

(74) Agent: **BERTHIER, Karine**; Thomson, 46 Quai A. Le Gallo, F-92648 Boulogne Cedex (FR).

(21) International Application Number:
PCT/EP2008/053181

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

(22) International Filing Date: 17 March 2008 (17.03.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
07300899.7 27 March 2007 (27.03.2007) EP

(71) Applicant (for all designated States except US): **THOMSON LICENSING** [—/FR]; 46 Quai A. Le Gallo, F-92100 Boulogne-Billancourt (FR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **ONNO, STEPHANE** [FR/FR]; 6, allée Claude Debussy, F-35760 Saint Gregoire (FR). **HEEN, Olivier** [FR/FR]; 20, rue des Tournesols, F-35410 Domloup (FR).

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

(54) Title: DEVICE AND METHOD FOR DIGITAL PROCESSING MANAGEMENT OF CONTENT SO AS TO ENABLE AN IMPOSED WORK FLOW

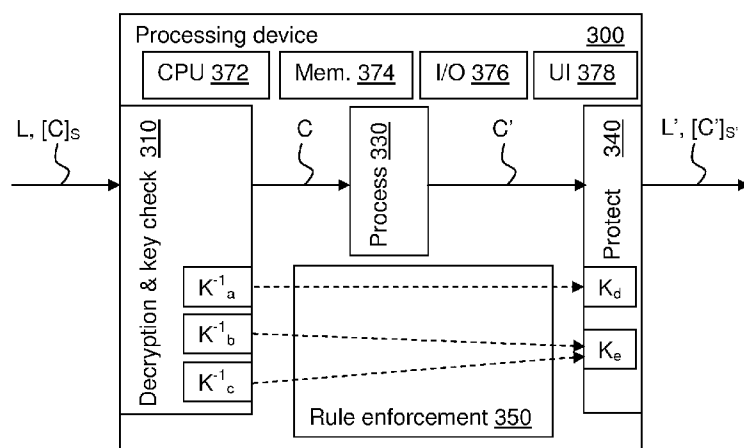


Figure 3

(57) Abstract: A device (200, 300, 600) receives (402) protected content ([C]s) and a license (L) for the content (C), unprotects (408, 410) the content using an input key (K_i^{-1}) and retrieves (404) a rule associated with the input key. The device then processes (412) the content to create new content (C'), retrieves at least one output key (K_j) associated with the input key in the retrieved rule, protects (414, 416) the content using the output key and sends the newly protected content ([C']s) and the corresponding license (L'). It is thus possible to impose a work flow as it is necessary for a device to store a particular key in order to access the content and as the rule imposes a particular output key depending on the input key. In a preferred embodiment, the content is scrambled using a symmetrical key (S) that is encrypted by an asymmetrical key in the license. An alternate embodiment uses watermarking techniques instead of encryption. The invention finds particular use in video processing.

**DEVICE AND METHOD FOR DIGITAL PROCESSING MANAGEMENT OF
CONTENT SO AS TO ENABLE AN IMPOSED WORK FLOW**

FIELD OF THE INVENTION

5 The invention is generally directed to digital content protection, and more specifically to protection of such content in a processing chain.

BACKGROUND OF THE INVENTION

10 This section is intended to introduce the reader to various aspects of art, which may be related to various aspects of the present invention that are described and/or claimed below. This discussion is believed to be helpful in providing the reader with background information to facilitate a better understanding of the
15 various aspects of the present invention. Accordingly, it should be understood that these statements are to be read in this light, and not as admissions of prior art.

20 Content, such as multimedia content - e.g. films and music - documents, photos and so on often need to be processed before it is released for the enjoyment of the end user.

25 Films, for example, pass many processing steps from the actual recording to the release: de-rushing, mixing, addition of digital effects, dubbing, subtitling, and so on.

 It will be readily appreciated that a content provider has two requirements for a processing (also called post-processing) system: 1) strict and traceable processing operations, and 2) easy transmission and

duplication of the content. The person skilled in the art will appreciate that prior art systems satisfy one or the other requirement, but not both.

Analogue systems generally satisfy the first
5 requirement. As content is stored on tapes or film reels, it is relatively easy to control the processing: a particular content remains with a certain department until the tape is sent to the next department. In addition, it is also possible to trace the tape in case
10 of theft. On the other hand, transmission of the content is less straight-forward, as this requires sending the physical tape, which naturally is difficult, particularly if long distances are involved. It is also difficult to provide the content to more than one entity at once, as
15 the content has to be physically duplicated. In addition, erasing and/or destroying content after use may also provide constraints on the users.

Digital systems provide easy transmission and duplication of content. However, it is much more
20 difficult to control the processing of the content: if the content resides on a server, it is very difficult to control who has access to it and errors may often be made if one department erroneously believes that the previous department has finished processing the content.

25 Figure 1 shows an exemplary processing system in which the invention may be used. The system 100 comprises a subtitling device 110, a colour management device 120, a dubbing device 140, a digital special effects device 150, a storage device 160, and an emission clearance
30 device 130, all connected by a network 170.

In the system of Figure 1, it may for example be required that content pass colour management 120 and digital effects 150 (in no particular order) before being sent to dubbing 140 and optionally further to subtitling 110, before passing through emission clearance 130. As every device has access to the storage 160, it is difficult to control that the workflow is respected.

This difficulty in digital systems is inherent in Digital Rights Management (DRM) Systems. DRM controls access to the content according to usage restrictions. The content is encrypted and a separate license is provided to the end user.

A DRM architecture comprises a content provider, a content distributor, a license issuer, and content users, and has the following characteristics: 1) they are built around the servers, 2) an end user is not allowed to create new content and licenses from the obtained content, and 3) the right to decrypt the content is global - the user either has it or he doesn't.

It will thus be appreciated that the prior art DRM solutions are not appropriate to fulfil the two requirements listed hereinbefore.

It can thus be appreciated that there is a need for a solution that enables a processing system in which digital content may be easily distributed and duplicated, while it also imposes strict processing operations, this solution being called Digital Processing Management (DPM) .

The present invention provides such a solution.

SUMMARY OF THE INVENTION

In a first aspect, the invention is directed to a method of processing content. Protected content is received and unprotected using a decryption key from a set of stored decryption keys. The content is processed to obtain processed content that is protected using at least one encryption key from a set of stored encryption keys. Each decryption key is linked to at least one encryption key of the set of stored encryption keys and the at least one encryption key is selected by selection of the at least one encryption key linked to the decryption key used for decryption. The selected at least one encryption key is different from the decryption key used for decryption if symmetrical encryption is used, and the selected at least one encryption key does not belong to the same key pair if asymmetrical encryption is used.

In a preferred embodiment, the received protected content is scrambled by a scrambling key, which in turn is encrypted using an asymmetrical encryption algorithm. The content is unprotected by decrypting the encrypted scrambling key using the decryption key to obtain the scrambling key, and unscrambling the scrambled content using the scrambling key.

It is preferred that the step of protecting the processed content comprises generating a new scrambling key; scrambling the processed content using the new scrambling key; and encrypting the new scrambling key using the asymmetrical encryption algorithm with the at least one encryption key. It is advantageous that the encrypted scrambling keys are incorporated in licenses

linked to the protected content, and further that a license further comprises comments.

It is also preferred that the decrypting the encrypted scrambling key comprises iteratively utilising
5 a plurality of decryption keys until the encrypted scrambling key is successfully decrypted.

In a further preferred embodiment, the received protected content is protected by a robust watermark and the robustly watermarked content is watermarked by a
10 fragile watermark. The protected content is unprotected by removing the fragile watermark, and removing the robust watermark.

The method is particularly suited for multimedia content.

15 In a second aspect, the invention is directed to a device for processing protected content. The device comprises means for unprotecting the protected content using a decryption key from a set of stored decryption keys; means for processing the content; means for
20 protecting the content using at least one encryption key from a set of stored encryption keys; and means for storing a plurality of input keys and output keys. Each decryption key is linked to at least one encryption key of the set of stored encryption keys. The device also
25 comprises means for selecting the at least one encryption key by selection of the at least one encryption key linked to the decryption key used for decryption. The selected at least one encryption key is different from the decryption key used for decryption if symmetrical
30 encryption is used, and the selected at least one

encryption key does not belong to the same key pair if asymmetrical encryption is used.

In a preferred embodiment, the received content is scrambled by a scrambling key, the scrambling key being
5 encrypted using an asymmetrical encryption algorithm, and the means for unprotecting the protected content are adapted to decrypt the encrypted scrambling key using the decryption key to obtain the scrambling key; and
10 unscramble the scrambled content using the scrambling key.

It is advantageous that the device further comprises means for generating a new scrambling key, and that the means for protecting the processed content are adapted to
15 scramble the processed content using the new scrambling key; and encrypt the new scrambling key using the asymmetrical encryption algorithm with the at least one encryption key.

It is also advantageous that the means for unprotecting the encrypted scrambling key are adapted to
20 iteratively utilise a plurality of decryption keys until the encrypted scrambling key is successfully decrypted.

In a further preferred embodiment, wherein the received content is protected by a robust watermark, and the robustly watermarked content is watermarked by a
25 fragile watermark, the means for unprotecting the protected content are adapted to remove the fragile watermark, and remove the robust watermark.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred features of the present invention will now
30 be described, by way of example, with reference to the

accompanying drawings, in which:
Fig. 1, already described, illustrates an exemplary
processing system in which the invention may be used;
Fig. 2 illustrates the general inventive idea of the
5 present invention;
Fig. 3 illustrates a device according to a preferred
embodiment of the invention;
Fig. 4 illustrates a flow chart of a method according to
a preferred embodiment of the invention;
10 Fig. 5 illustrates the use of the invention in an
exemplary processing system;
Fig. 6 illustrates an alternate use of the general
inventive idea; and
Fig. 7 illustrates a flow chart of an alternate
15 embodiment of the invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Fig. 2 illustrates the general inventive idea of the
present invention. Protected content 205 arrives at a
processing device 200 that checks 210 who issued the
20 content and, depending on the identity of the issuer or
group of issuers in case more than one issuer may prepare
the same kind of content, extracts a rule (further
discussed hereinafter). The processing device 200 then
unprotects 220 the content and uses the unprotected
25 content 225 for processing 230, which often produces
modified, unprotected content 235. The new content 235 is
then protected 240 based on the extracted rule that
enforces 250 a certain protection of the new content 235,
which outputs new protected content 245. It should be
30 noted, however, that processing need not necessarily
modify the content; the content may remain the same, such
as for example during emission clearance.

Preferred embodiment

The preferred embodiment uses cryptography to control the process. Each device stores a number of input keys to decrypt incoming content and a number of output keys to re-encrypt outgoing content. The stored keys are normally a subset of all the keys used in the system.

Figure 3 illustrates a device implementing the invention of the preferred embodiment, while Figure 4 illustrates a method according to a preferred embodiment of the invention.

The processing device 300 comprises at least one processor 372, at least one memory 374, communication means 376 that may comprise separate input and output units, and a user interface 378. It is preferred that the at least one processor 372 performs the functions performed by the functional units described hereinafter. The skilled person will appreciate that the processing device 300 comprises further hardware and software units, such as for example at least one data bus, although these are beyond the scope of the invention and have not been indicated in the Figure for reasons of clarity of illustration.

Every content in the system is associated with a license, preferably in the same file as the content, but it is also possible that the content and the associated license are stored in two different files linked to each other. A license L may be written as $\{S, \text{comments}\}_{K_i}$, where S is a, preferably, symmetric key with which the content was scrambled, "comments" is digital information such as for instance time stamps and names input by one

or more users, and $\{\}_{K_i}$ indicates the data within parenthesis is encrypted by an asymmetric encryption algorithm, such as RSA, using asymmetric key K_i . The comments may also comprise DRM rights, e.g. as expressed
5 in a Right Expression Language (REL). It will be appreciated that the present invention enables the integrity of such data along the processing workflow.

Further, the decryption key that corresponds to an encryption key K_i is denoted as K_i^{-1} .

10 A rule preferably comprises a type of processing device for which the rule is intended, an input decryption key K_i^{-1} and a corresponding output encryption key K_i . The rule states that, for the processing device, content that was decrypted using the input key shall be
15 encrypted using the output encryption key given by the rule. It should be noted that it is possible to use rules with one input decryption key that is linked to more than one output encryption key. This may for example be the case if content from a certain source shall be output in
20 more than one copy, or if the operator of the processing device is to be given a choice of output encryption keys. Especially if the latter cases are used simultaneously in the system, it is advantageous to include an operator in the rule to inform the device if multiple outputs and/or
25 operator choice is to be used.

The processing device 300 receives 402 data $L[C]_s$ comprising content $[C]_s$ scrambled (indicated by the square brackets) using scrambling key S , which preferably is symmetrical, and a license L comprising the scrambling
30 key S and possibly one or more comments, the license being encrypted using an asymmetrical encryption

algorithm with key K_i . It should be noted that the data may be sent to the processing device 300 as well as requested by it.

Upon reception of the data $L[C]_s$, a decryption and
5 key check module 310 selects 404 a rule among the plurality of rules stored in a memory 372.

As is shown in the Figure, the processing device 300 comprises three rules, for which input decryption keys K_a^{-1} , K_b^{-1} , and K_c^{-1} are indicated in the decryption and
10 processing module 310, output encryption keys K_d and K_e are indicated in the protection module 340, and a rule enforcing module 350 verifies that the rules are enforced. In the example, the first rule R1 has K_a^{-1} as input decryption key and K_d as output encryption key,
15 rule R2 has keys K_b^{-1} and K_e , and rule R3 has keys K_c^{-1} and K_e . It should be noted that R2 and R3 have different input decryption keys and the same output encryption key. The rules are preferably distributed in the system by a policy server (not shown) in order to make sure that one
20 or more processing chains is created.

If no such rule is available or if all of the stored rules have already been tried ("Not OK"), then the method stops at step 406 "End". However, if the decryption and key check module 310 successfully selects a rule ("OK"),
25 the method goes on in step 408 in which decryption of L with the decryption key K_i^{-1} of the rule.

The decryption and key check module 310 may verify if the decryption was successful, for example by including a standard public value, such as "deadbeef" at a
30 predetermined place in the license; if the value is

found, then the license was successfully decrypted. In case the decryption was not successful ("Not OK"), then the method goes back to step 404 where another, preferably the next, rule is chosen.

5 On the other hand, if the decryption was successful ("OK"), then the decryption and key check module 310 extracts the scrambling key S and any comments therein and descrambles 410 the scrambled content $[C]_s$ using the scrambling key S.

10 Once the content C has been descrambled, it is forwarded to the processing module 330 for processing 412 and, possibly, addition of and/or suppression of comments. The processing module 330 then forwards the normally modified content C' to a protection module 340
15 that first scrambles 414 the modified content C' with a new scrambling key S' and then creates 416 a new license L' by encrypting the new scrambling key S' and any comments by the key imposed by the rule enforcement module according to the selected rule that successfully
20 decrypted the license. The new data, comprising the license L' and the content $[C']_{s'}$, is then sent for example directly to a further device for further processing or to an external storage unit.

25 While the embodiment above describes the use of asymmetrical keys to protect the licenses, the person skilled in the art will appreciate that it is also possible to use symmetrical keys for this purpose, although such use reduces the security of the system somewhat.

Figure 5 illustrates the use of the invention in an exemplary network 500 comprising an import device 510, a digital special effects device 520, a colour management device 530, and an export device 540 connected by a local
5 area network 550.

The import device 510 imports content that, in the present example, is unprotected - illustrated by "No key" - scrambles the content and creates a license using key K_0 . The content may then be used by the digital special
10 effects device 520 and the colour management device 530, but not the export device 540, as the latter does not have the requisite input decryption key.

The digital special effects device 520 may, using key K_0^{-1} , access content coming from the import device 510, in
15 which case the content is output encrypted using key K_1 for use by the colour management device 530, but not by the export device 540. The digital special effects device 520 may also, using key K_2^{-1} , access content coming from the colour management device 530, in which case the
20 content is output encrypted using key K_3 for use by the export device 540, but not by the colour management device 530.

Analogously, the colour management device 530 may, using key K_0^{-1} , access content coming from the import
25 device 510, in which case the content is output encrypted using key K_2 for use by the digital special effects device 520, but not by the export device 540. The colour management device 530 may also, using key K_1^{-1} , access content coming from the digital special effects device
30 520, in which case the content is output encrypted using

key K_3 for use by the export device 540, but not by the colour management device 530.

5 The export device 540 may, using key K_3^{-1} , use content coming from either the digital special effects device 520 or the colour management device 530, provided that the content was encrypted using key K_3 . The export device 540 then exports the content, in the example unencrypted as is indicated by "No key" in the Figure.

10 It will thus be appreciated that the invention enforces the workflow in the exemplary system. Content that is introduced into the system by the import device 510 must pass through both the digital special effects device 520 and the colour management device 530, although the order is in the present case irrelevant, before the
15 export device 540 can export the content.

While the preferred embodiment described video processing, it will be appreciated that the invention may also be applied to other environments in which it is important or desirable to impose strict work flows, such
20 as in programming where the different files may be protected, for printed media where for example different articles and pictures may be protected, or for documents to which modifications should be made and/or digital signatures should be affixed in a certain order.

25 Figure 6 illustrates an alternate use of the invention. A mail handling device 600 comprises at least one processor 672, at least one memory 674, communication means 676 that may comprise separate input and output units, and preferably a user interface 678.

The mail handling device 600 is adapted to perform a sort of "Out of Office" function, i.e. automatic transfer of incoming mails. While the exemplary embodiment is shown with encrypted incoming mails, it is to be understood that it may also be used with non-encrypted incoming mails (in which case an input decryption key may be said to be zero, i.e. the output of the decryption equals the input).

In the mail handler, the rules R stipulate that mail coming from a certain sender is to be decrypted using a certain input decryption key, encrypted using a certain output encryption key, and sent to the destination provided by the rule. It should be noted that it is possible to have one input message give rise to a plurality of encrypted output message, each output message being destined for a specific destination (illustrated in the Figure by having input key K_c^{-1} linked to output keys K_e and K_f).

It will thus be appreciated that the invention may also be used for secure automatic transfer of electronic mail.

Alternate embodiment

Where the preferred embodiment employed cryptography, the alternate embodiment employs watermarks.

The embodiment uses a robust watermark for traceability and confidentiality, and a fragile watermark that ensures integrity together with the robust watermark. It should be noted that the invention may employ any state of the art robust and fragile watermarking algorithms.

In the alternate embodiment, constant messages are given in a processing system. For example, the robust watermark may use "dead" and the fragile watermark "beef". The robust watermark of content C using key K may thus be denoted $\{C, \text{dead}\}_K$. The fragile watermark is denoted $\{C, \text{beef}\}$. Licensed content L may be denoted $\{\{C, \text{dead}\}_K, \text{beef}\}$, i.e. the fragile watermark is inserted in the content already watermarked with the robust watermark, following well-known good practice.

Figure 7 illustrates a flow chart illustrating content processing according to the alternate embodiment.

The processing device receives licensed content L in step 702. In step 704, the fragile watermark is searched for by verifying the equality $\{L\}=\text{beef}$. In step 706, the robust watermark is searched for iteratively using rules stored in the device, each rule comprising an input key K_i and an output key K_j . This is done by verifying the equality $\{\{C, \text{dead}\}_{K_a}\}_{K_i}=\text{dead}$, where K_a is the key used to insert the robust watermark and K_i is the input key of the current rule.

In step 708, it is checked to see what watermark, if any, was found. If no watermark was found, the method ends in step 710. If one of the two watermarks was found, but not the other, then an error is reported in step 712. Finally, if both the robust watermark and the fragile watermark were found, then the method goes on to remove the robust watermark in step 714 to produce unprotected content C.

As the fragile watermark is designed to be destroyed as soon as the content is modified, there is no need to specifically remove this watermark.

Once the unprotected content C is obtained, it may be
5 modified in step 716 to obtain new content C'. After
processing, a new robust watermark is added to the new
content C', using the output key that according to the
rule corresponds to the correct input key. Then, in step
720, a fragile watermark is added to the robustly
10 watermarked content so as to create new licensed content
L' that is sent in step 722.

A person skilled in the art will appreciate that it
is possible to combine embodiments of the invention, for
example by using the cryptographic solution of the
15 preferred embodiment in a digital environment, the
watermark solution of the alternative embodiment, when
the content "goes analogue", and then back again to the
cryptographic solution when the content re-enters the, or
another, digital environment.

20 The skilled person will also appreciate that it is
possible to use both the cryptographic solution and the
watermark solution at the same time and for the same
content. This requires successful double verification of
the protection in order to be able to access the content.

25 It will thus be appreciated that the method provides
an alternate way of protecting content and imposing
strict a work flow.

As will be appreciated, the present invention enables
enforcement of strict workflows, for example for

processing video content, and also protection of such content.

It will be understood that the present invention has been described purely by way of example. Each feature
5 disclosed in the description and (where appropriate) the claims and drawings may be provided independently or in any appropriate combination. Features described as being implemented in hardware may also be implemented in software, and vice versa. Connections may, where
10 applicable, be implemented as wireless connections or wired, not necessarily direct or dedicated, connections.

Reference numerals appearing in the claims are by way of illustration only and shall have no limiting effect on the scope of the claims.

Claims

1. A method of processing content (C) comprising the steps of:

- 5 - receiving (402, 702) protected content ($[C]_s; L$);
 - unprotecting (408, 410; 714) the content using a decryption key (K^{-1}_i) from a set of stored decryption keys;
 - processing (412, 716) the content to obtain
10 processed content (C'); and
 - protecting (414, 416; 718, 720) the processed content using at least one encryption key from a set of stored encryption keys;
 characterised in that each decryption key is linked to
15 at least one encryption key of the set of stored encryption keys; and
 in that the method further comprises the step of selecting (404) the at least one encryption key, wherein the at least one encryption key linked to the decryption
20 key used for decryption is selected;
 wherein the selected at least one encryption key is different from the decryption key used for decryption if symmetrical encryption is used, and the selected at least one encryption key does not belong to the same key pair
25 if asymmetrical encryption is used.

2. The method as claimed in claim 1, wherein the received protected content is scrambled by a scrambling key (S), the scrambling key being encrypted using an asymmetrical encryption algorithm, wherein the step (408, 410) of
30 unprotecting the content comprises the steps of:

- decrypting (408) the encrypted scrambling key ($\{S\}_{K_r}$) using the decryption key to obtain the scrambling key; and

- unscrambling (410) the scrambled content ($[C]_s$) using the scrambling key (S).

3. The method as claimed in claim 2, wherein the step of protecting (414, 416) the processed content (C') comprises the steps of:

- generating (414) a new scrambling key (S');
10 - scrambling (414) the processed content using the new scrambling key; and
- encrypting (416) the new scrambling key using the asymmetrical encryption algorithm with the at least one encryption key.

15 4. The method as claimed in claim 3, wherein the encrypted scrambling keys are incorporated in licenses (L) linked to the protected content.

5. The method as claimed in claim 4, wherein a license (L) further comprises comments.

20 6. The method as claimed in claim 2, wherein the step of decrypting the encrypted scrambling key comprises iteratively utilising a plurality of decryption keys until the encrypted scrambling key is successfully decrypted.

25 7. The method as claimed in claim 1, wherein the received protected content is protected by a robust watermark, and the robustly watermarked content is watermarked by a fragile watermark, wherein the step of unprotecting (714) the protected content comprises the steps of:

- 30 - removing the fragile watermark, and

- removing (714) the robust watermark.

8. The method as claimed in any preceding claim, wherein the content is multimedia content.

9. A device for processing protected content comprising:

5 means (220, 310) for unprotecting the protected content using a decryption key (K^{-1}_i) from a set of stored decryption keys;

means (230, 330) for processing the content;

10 means (240, 340) for protecting the content using at least one encryption key from a set of stored encryption keys;

means (374) for storing a plurality of input keys and output keys;

characterised in that

15 each decryption key is linked to at least one encryption key of the set of stored encryption keys;

the device comprises means (350) for selecting the at least one encryption key by selection of the at least one encryption key linked to the decryption key used for
20 decryption;

wherein the selected at least one encryption key is different from the decryption key used for decryption if symmetrical encryption is used, and the selected at least one encryption key does not belong to the same key pair
25 if asymmetrical encryption is used.

10. The device as claimed in claim 9, wherein the received content is scrambled by a scrambling key, the scrambling key being encrypted using an asymmetrical encryption algorithm, wherein the means (220, 310) for
30 unprotecting the protected content are adapted to:

- decrypt the encrypted scrambling key using the decryption key to obtain the scrambling key; and
- unscramble the scrambled content using the scrambling key.

- 5 11. The device as claimed in claim 10, further comprising means (340) for generating a new scrambling key, and wherein the means (240, 340) for protecting the processed content are adapted to:
- scramble the processed content using the new
- 10 scrambling key; and
- encrypt the new scrambling key using the asymmetrical encryption algorithm with the at least one the encryption key.

12. The device as claimed in claim 10, wherein the means
- 15 (220, 310) for unprotecting the encrypted scrambling key are adapted to iteratively utilise a plurality of decryption keys until the encrypted scrambling key is successfully decrypted.

13. The device as claimed in claim 9, wherein the
- 20 received content is protected by a robust watermark, and the robustly watermarked content is watermarked by a fragile watermark, wherein the means (220) for unprotecting the protected content are adapted to:
- remove the fragile watermark, and
- 25 - remove the robust watermark.

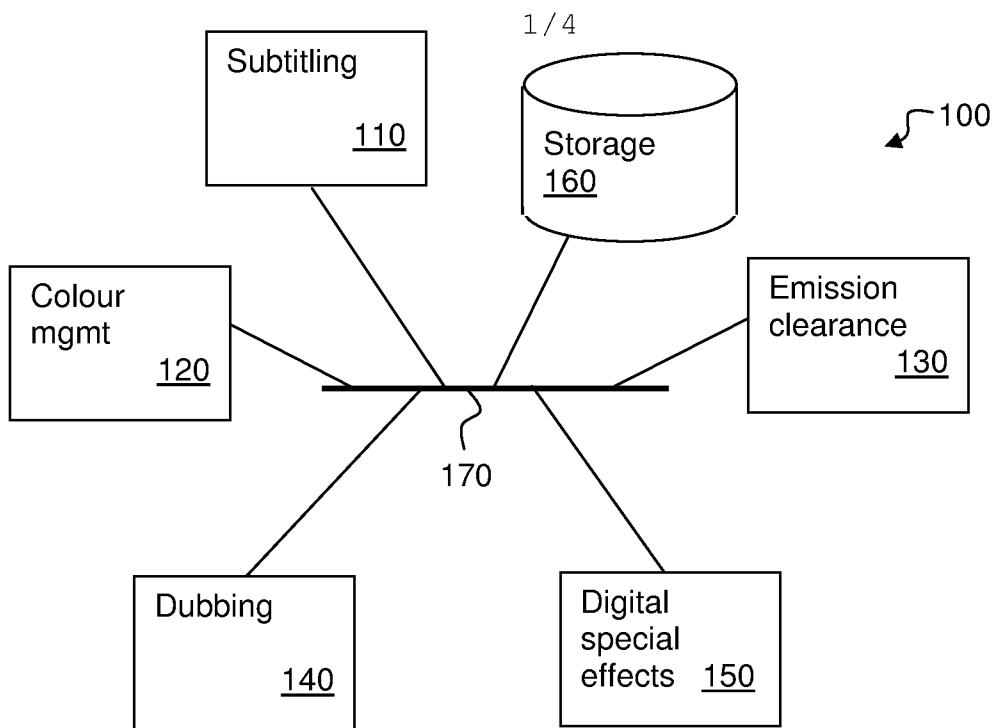


Figure 1

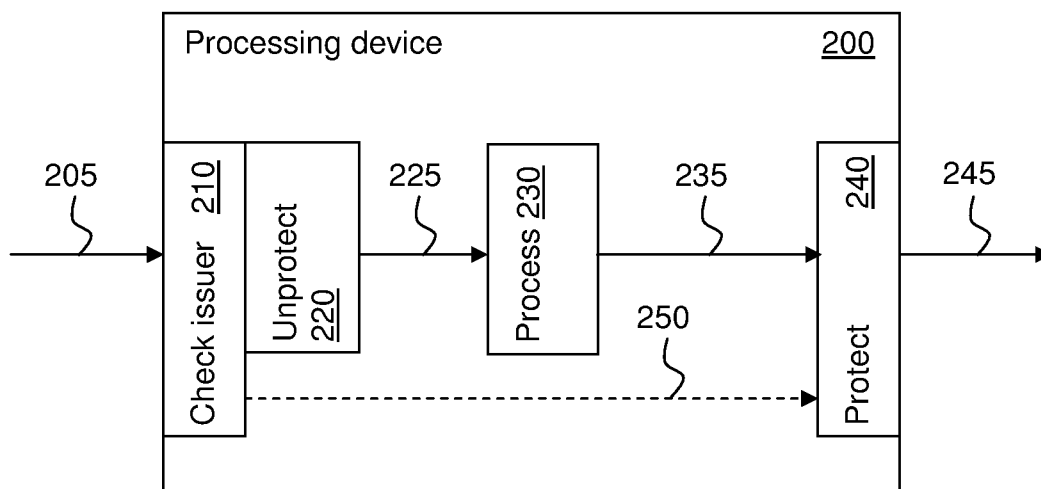


Figure 2

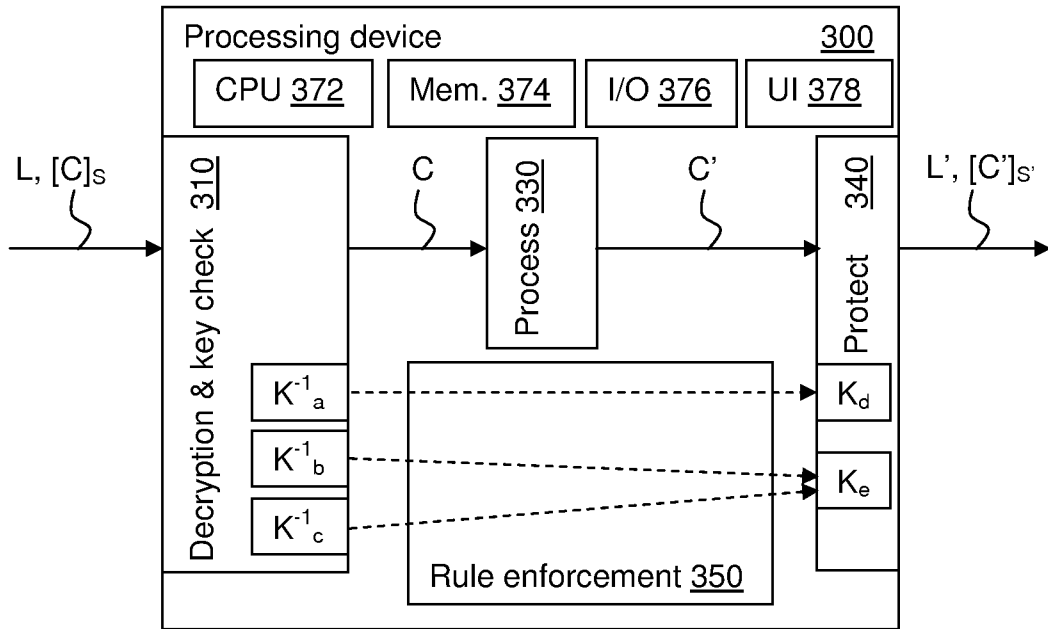


Figure 3

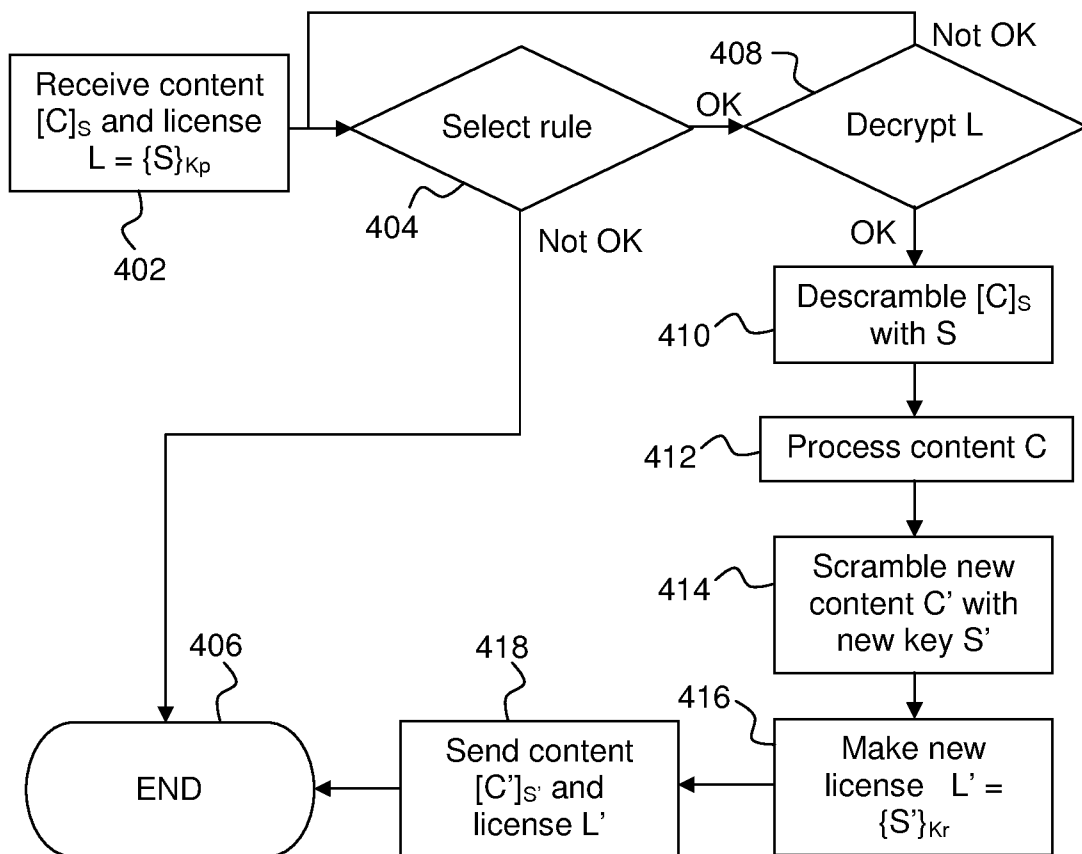


Figure 4

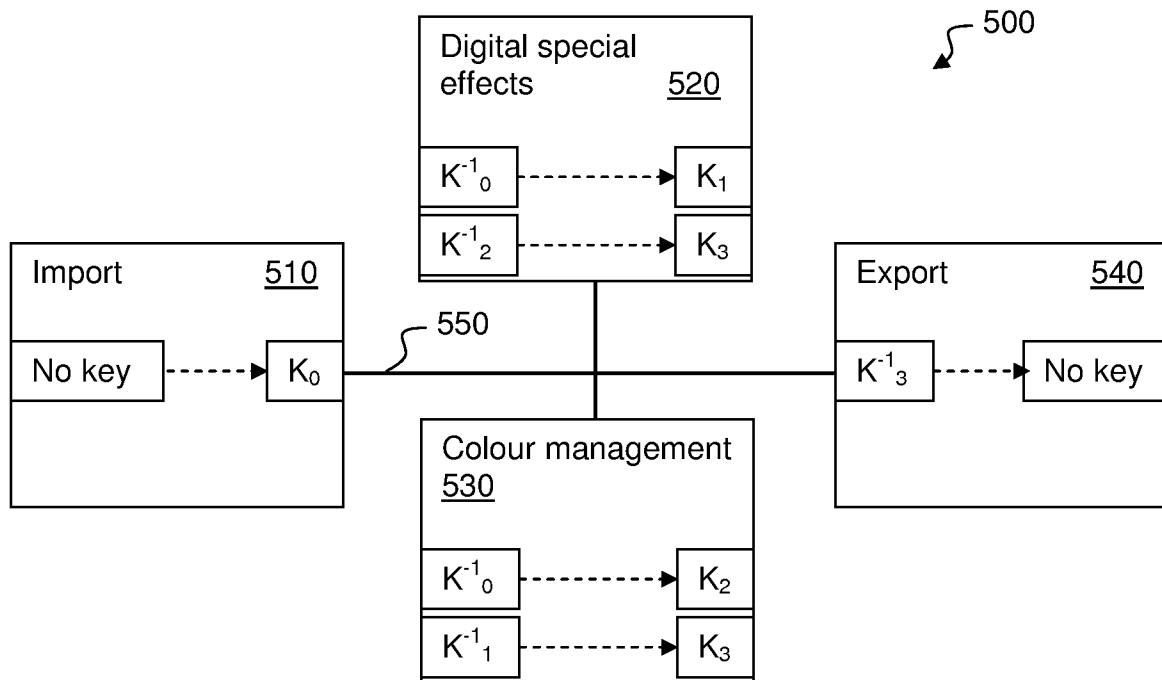


Figure 5

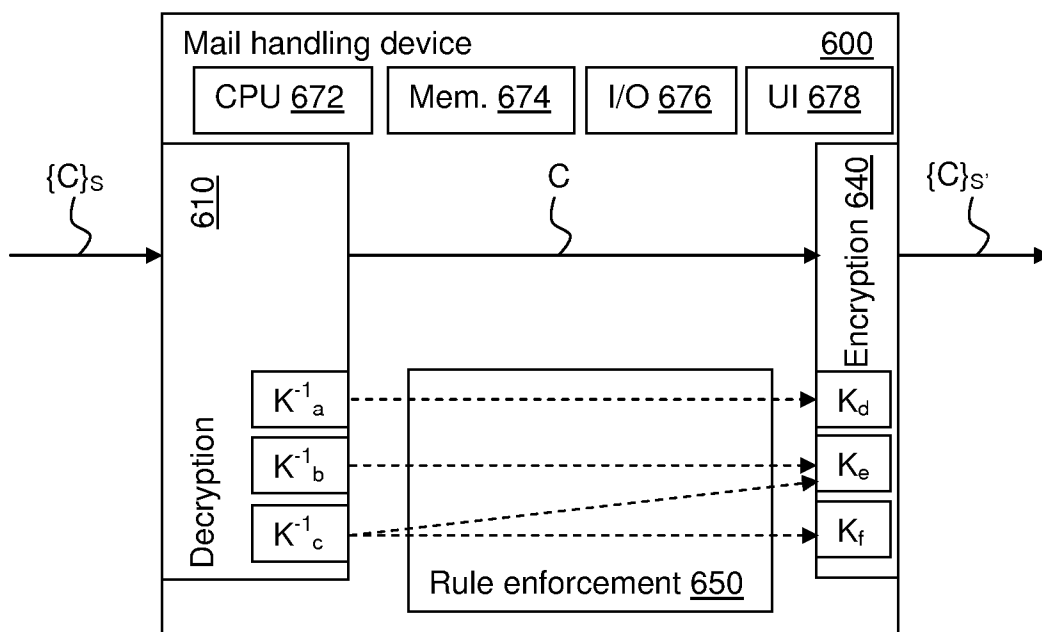


Figure 6

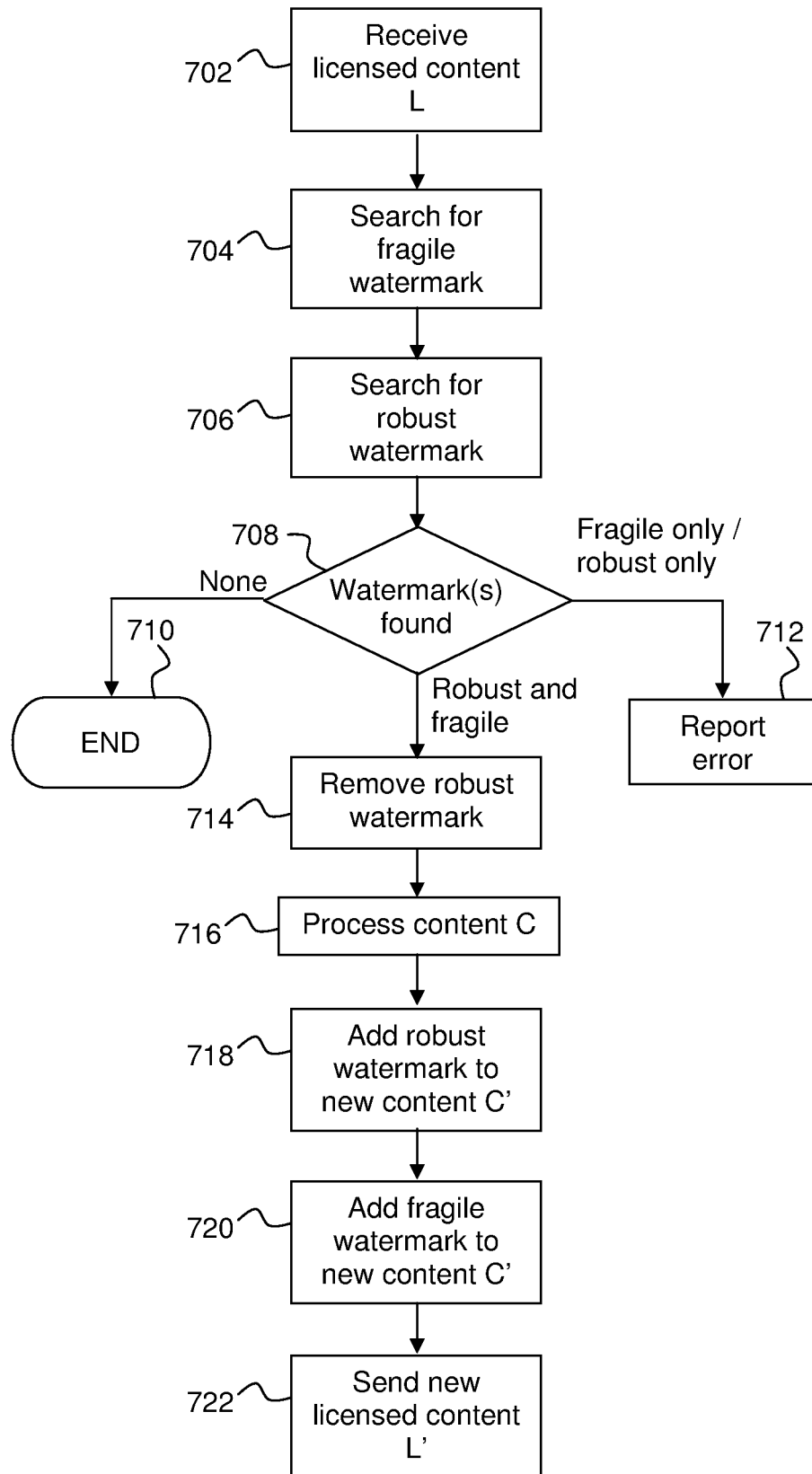


Figure 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/053181

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F G06T

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

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

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No..
X	US 2003/115450 A1 (SMITH JEFFREY C [US]) 19 June 2003 (2003-06-19) abstract paragraph [0021] - paragraph [0022] paragraph [0029] paragraphs [0040] - [0048]	1-13
X	EP 0 669 741 A2 (IBM [US]) 30 August 1995 (1995-08-30) page 2, line 44 - line 48	1-13
A	US 2003/217264 A1 (MARTIN ANDREW K [US] ET AL) 20 November 2003 (2003-11-20) paragraphs [0003] - [0005] paragraphs [0014], [0018], [0020]	1-13
	-/--	

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

☒ See patent family annex.

* Special categories of cited documents :

A document defining the general state of the art which is not considered to be of particular relevance

E earlier document but published on or after the international filing date

L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

O document referring to an oral disclosure, use, exhibition or other means

P document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

& document member of the same patent family

Date of the actual completion of the international search

16 June 2008

Date of mailing of the international search report

20/06/2008

Name and mailing address of the ISA/

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

Authorized officer

Alecu, Mihail

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2008/053181

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MARSHAK R T: "IBM'S FLOWMARK OBJECT-ORIENTED WORKFLOW FOR MISSION-CRITICAL APPLICATIONS" WORKGROUP COMPUTING REPORT, vol. 17, no. 5, 1 May 1994 (1994-05-01), pages 3-13, XP000568699 ISSN: 1057-8889 the whole document	
A	FRIDRICH J: "HYBRID WATERMARK FOR TAMPER DETECTION IN DIGITAL IMAGES" INTERNATIONAL SYMPOSIUM ON SIGNAL PROCESSING AND ITS APPLICATIONS. PROCEEDINGS, vol. 1, 22 August 1999 (1999-08-22), pages 301-304, XP000937952 the whole document	7,13
A	DEGUILLAUME F ET AL: "Secure hybrid robust watermarking resistant against tampering and copy attack" SIGNAL PROCESSING, AMSTERDAM, NL, vol. 83, no. 10, October 2003 (2003-10), pages 2133-2170, XP004452923 ISSN: 0165-1684 the whole document	7,13
A	US 5 982 891 A (GINTER KARL L [US] ET AL) 9 November 1999 (1999-11-09) column 37, line 50 - line 54 column 162, line 4 - line 22 column 163, line 13 - line 15 column 214, line 8 - line 24	1-13
A	US 6 834 110 B1 (MARCONCINI FRANCO [IT] ET AL) 21 December 2004 (2004-12-21) column 18, line 15 - column 20, line 41 column 21, line 55 - line 60 column 25, line 31 - column 30, line 11	1-13

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2008/053181

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003115450	A1	19-06-2003	NONE
EP 0669741	A2	30-08-1995	DE 69532254 D1 22-01-2004 DE 69532254 T2 30-09-2004 JP 2711226 B2 10-02-1998 JP 7250059 A 26-09-1995 US 5479514 A 26-12-1995
US 2003217264	A1	20-11-2003	NONE
US 5982891	A	09-11-1999	AU 711733 B2 21-10-1999 AU 6326696 A 18-09-1996 CA 2212574 A1 06-09-1996 CN 1601429 A 30-03-2005 CN 1183841 A 03-06-1998 CN 1577205 A 09-02-2005 CN 1722049 A 18-01-2006 CN 1869997 A 29-11-2006 CN 1900942 A 24-01-2007 CN 1912885 A 14-02-2007 CN 1936912 A 28-03-2007 CN 1900943 A 24-01-2007 EP 0861461 A2 02-09-1998 HK 1073899 A1 07-12-2007 JP 10512074 T 17-11-1998 JP 3996532 B2 24-10-2007 JP 2004265358 A 24-09-2004 JP 3950076 B2 25-07-2007 JP 2004005558 A 08-01-2004 JP 2004005601 A 08-01-2004 JP 3905489 B2 18-04-2007 JP 2004139550 A 13-05-2004 JP 2004030600 A 29-01-2004 JP 2004005614 A 08-01-2004 JP 2004005625 A 08-01-2004 JP 2004005629 A 08-01-2004 JP 2006073004 A 16-03-2006 JP 2006073005 A 16-03-2006 JP 4008937 B2 14-11-2007 JP 2006085691 A 30-03-2006 JP 2006085692 A 30-03-2006 JP 2006085693 A 30-03-2006 JP 4008938 B2 14-11-2007 JP 2006048716 A 16-02-2006 JP 2006053939 A 23-02-2006 JP 2006053940 A 23-02-2006 JP 2006079622 A 23-03-2006 JP 4005619 B2 07-11-2007 JP 2006260587 A 28-09-2006 JP 4084392 B2 30-04-2008 JP 2006268867 A 05-10-2006 JP 2006209803 A 10-08-2006 JP 2006209804 A 10-08-2006 JP 2007183982 A 19-07-2007 JP 2007220131 A 30-08-2007 JP 2008097645 A 24-04-2008 WO 9627155 A2 06-09-1996 US 6427140 B1 30-07-2002

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2008/053181

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5982891	A	US 6658568 B1	02-12-2003
US 6834110	B1	CN 1306259 A	01-08-2001
	21-12-2004	US 2003135464 A1	17-07-2003