(12) UK Patent Application (19) GB (11) 2 367 668 (13) A

(43) Date of A Publication 10.04.2002

(21) Application No 0112627.5

(22) Date of Filing 23.05.2001

(30) Priority Data
(31) 0012790 (32) 25.05.2000 (33) GB

(51) INT CL[7]
G06F 17/30 1/00

(52) UK CL (Edition T)
G4A AAP AUDB

(56) Documents Cited
EP 1130490 A1

(58) Field of Search
UK CL (Edition T) G4A AAP AUDB
INT CL[7] G06F 1/00 17/30
Online : WPI,EPODOC,PAJ,INSPEC,ELSEVIER,TDB, WWW

(71) Applicant(s)
SealedMedia Limited
(Incorporated in the United Kingdom)
Sorbon, Aylesbury End, BEACONSFIELD, Buckinghamshire, HP9 1LW, United Kingdom

(72) Inventor(s)
Martin Richard Lambert

(74) Agent and/or Address for Service
W H Beck, Greener & Co
7 Stone Buildings, Lincoln's Inn, LONDON, WC2A 3SZ, United Kingdom

(54) Abstract Title
Search engine allowed access to encrypted data

(57) A "trusted" search engine 214 is provided with a means 302 to obtain rights to decrypted data on a digital fights management (DRM) system 306 for the purposes of indexing. The search engine then parses the decrypted content to produce a searchable index with which the end user can locate encrypted data alongside open unencrypted data for example on the internet. The indexer 216 may be issued with an identity which is recognised by the DRM system to differentiate it from other users and enabled search engines. The access rights may be selectively revoked or granted by the DRM system.

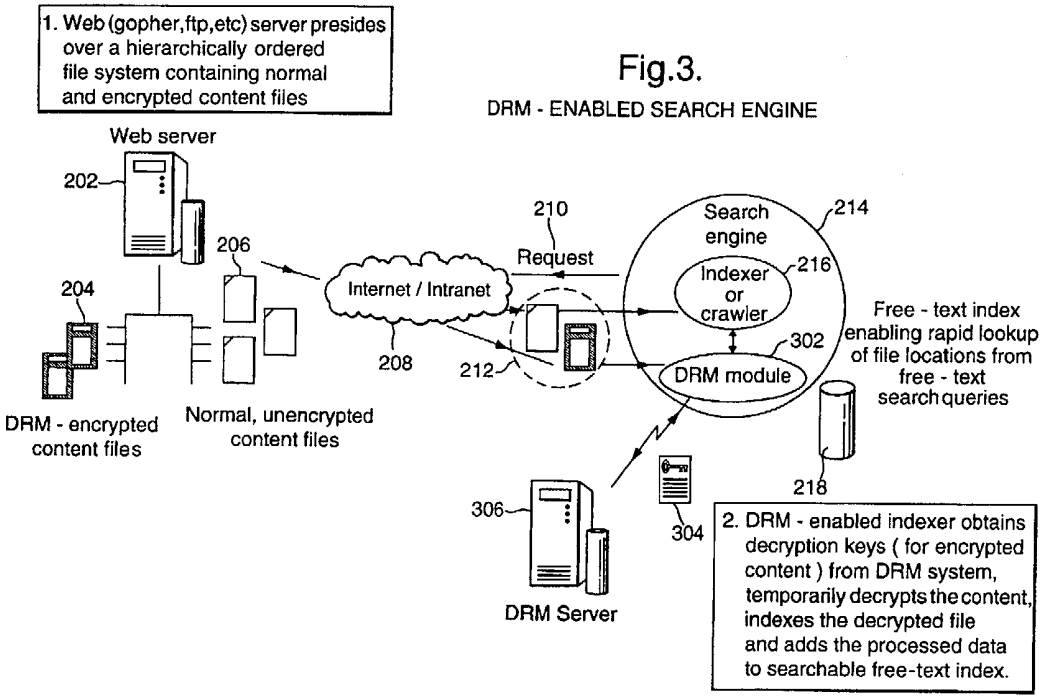


Fig.3.
DRM - ENABLED SEARCH ENGINE

GB 2 367 668 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

Fig.1.

DRM OVERVIEW (PRIOR ART)

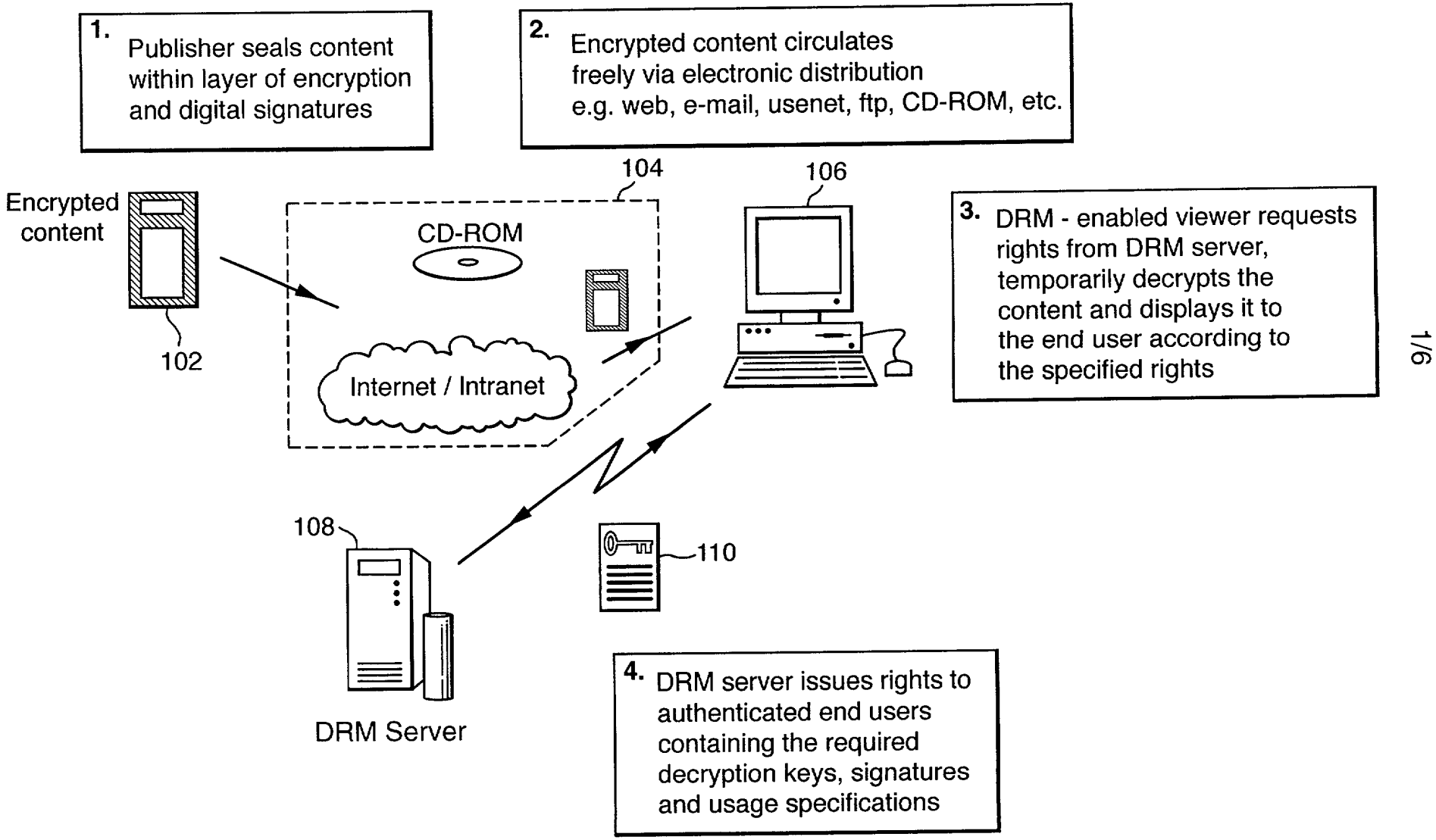
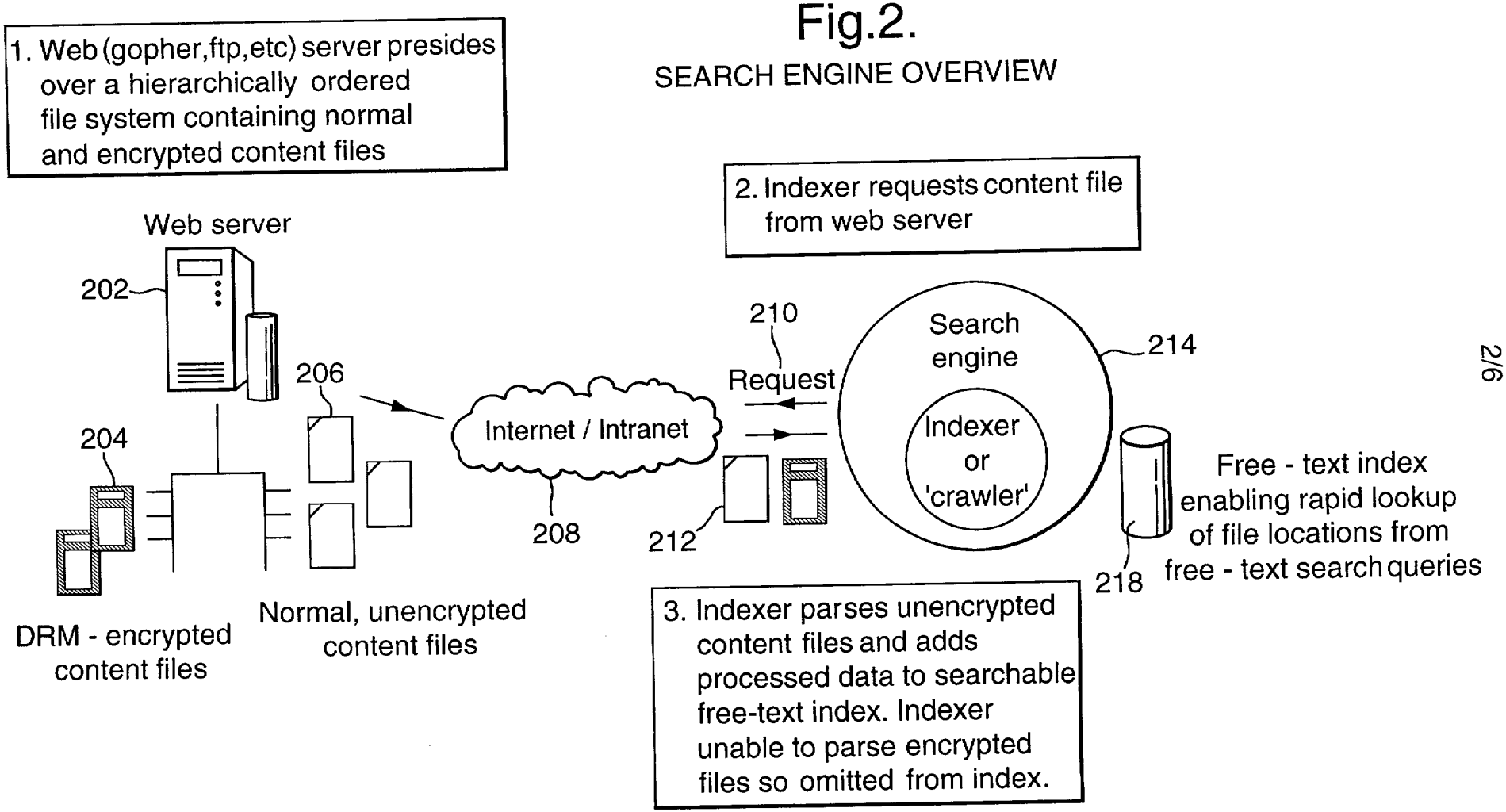


Fig.2.

SEARCH ENGINE OVERVIEW



1. Web (gopher,ftp,etc) server presides over a hierarchically ordered file system containing normal and encrypted content files

Fig.3.

DRM - ENABLED SEARCH ENGINE

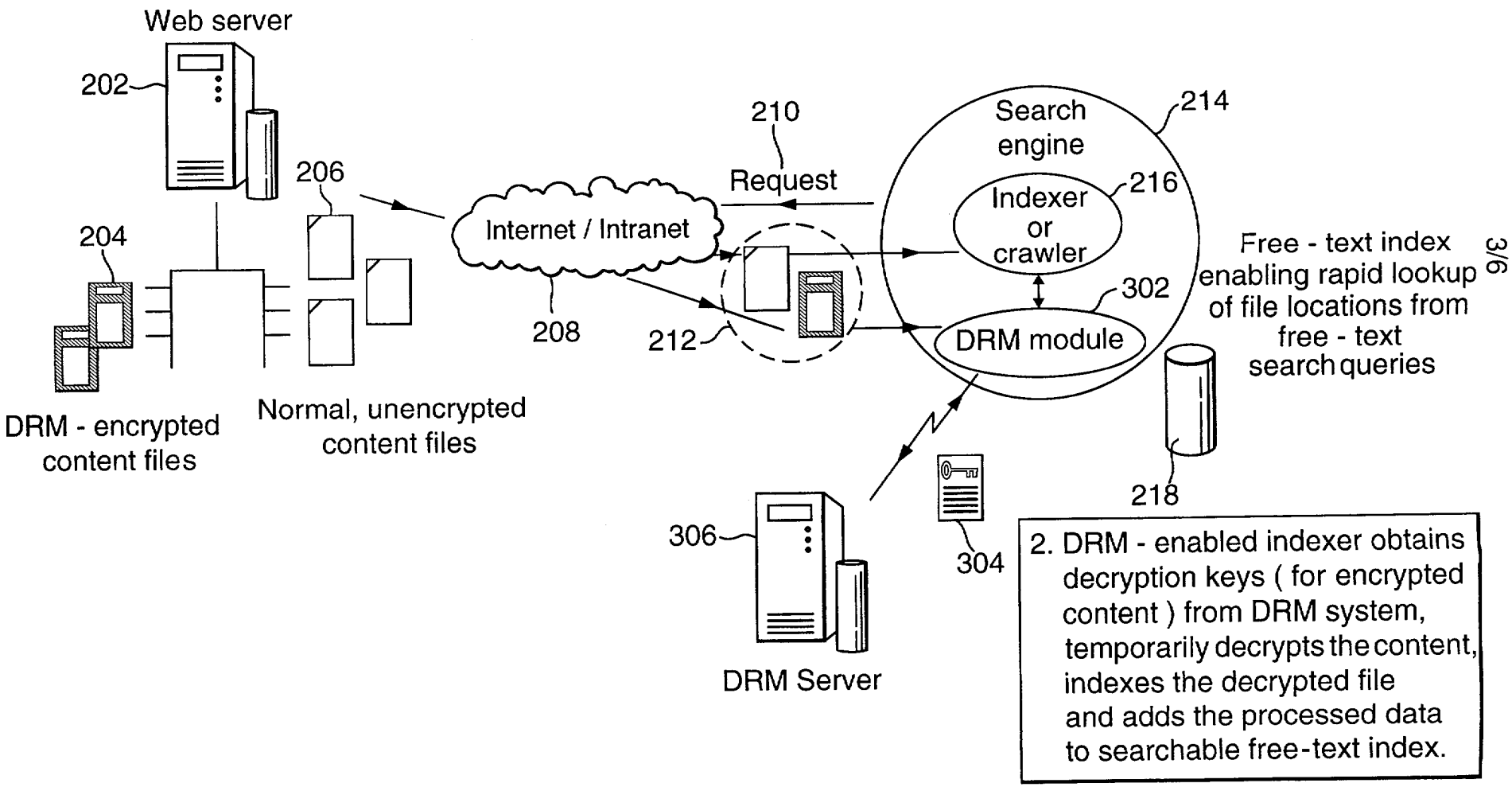
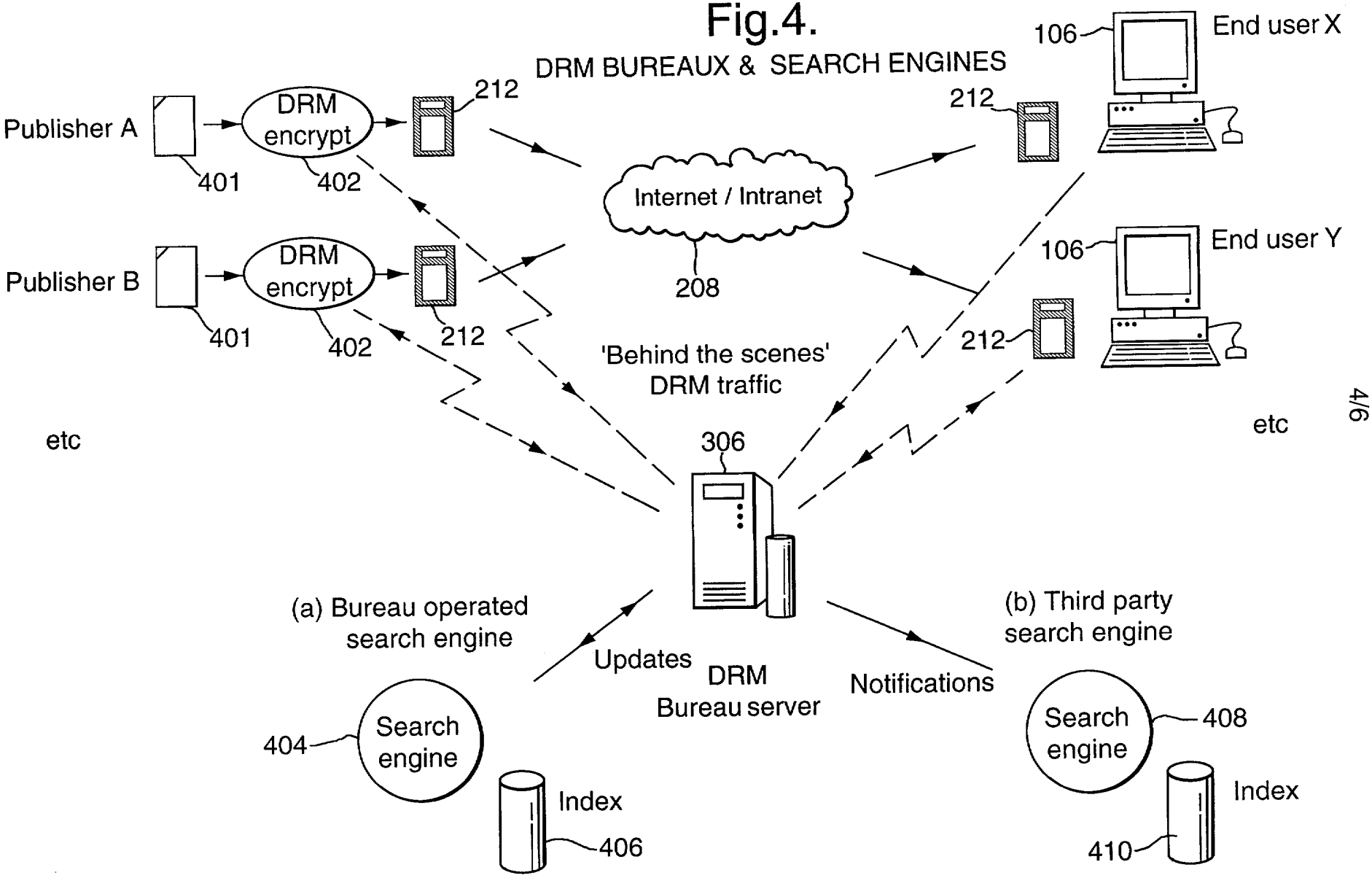


Fig.4.


DRM BUREAUX & SEARCH ENGINES
Publisher A
DRM encrypt
401
402
212
Publisher B
DRM encrypt
401
402
212
Internet / Intranet
208
106
End user X
212
106
End user Y
212
'Behind the scenes' DRM traffic
etc
etc
306
(a) Bureau operated search engine
Updates
DRM Bureau server
Notifications
(b) Third party search engine
404
Search engine
Index
406
Search engine
408
Index
410

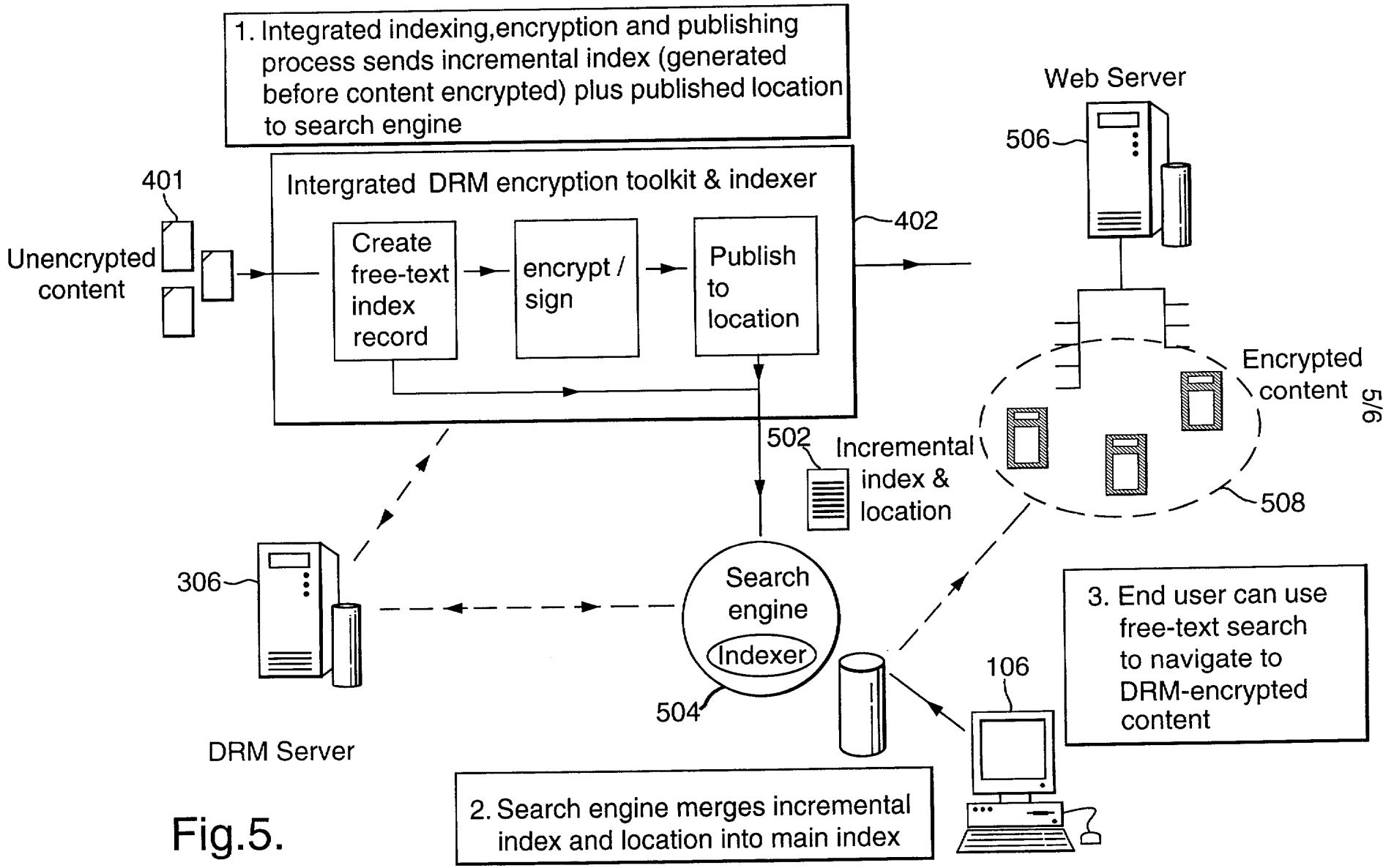
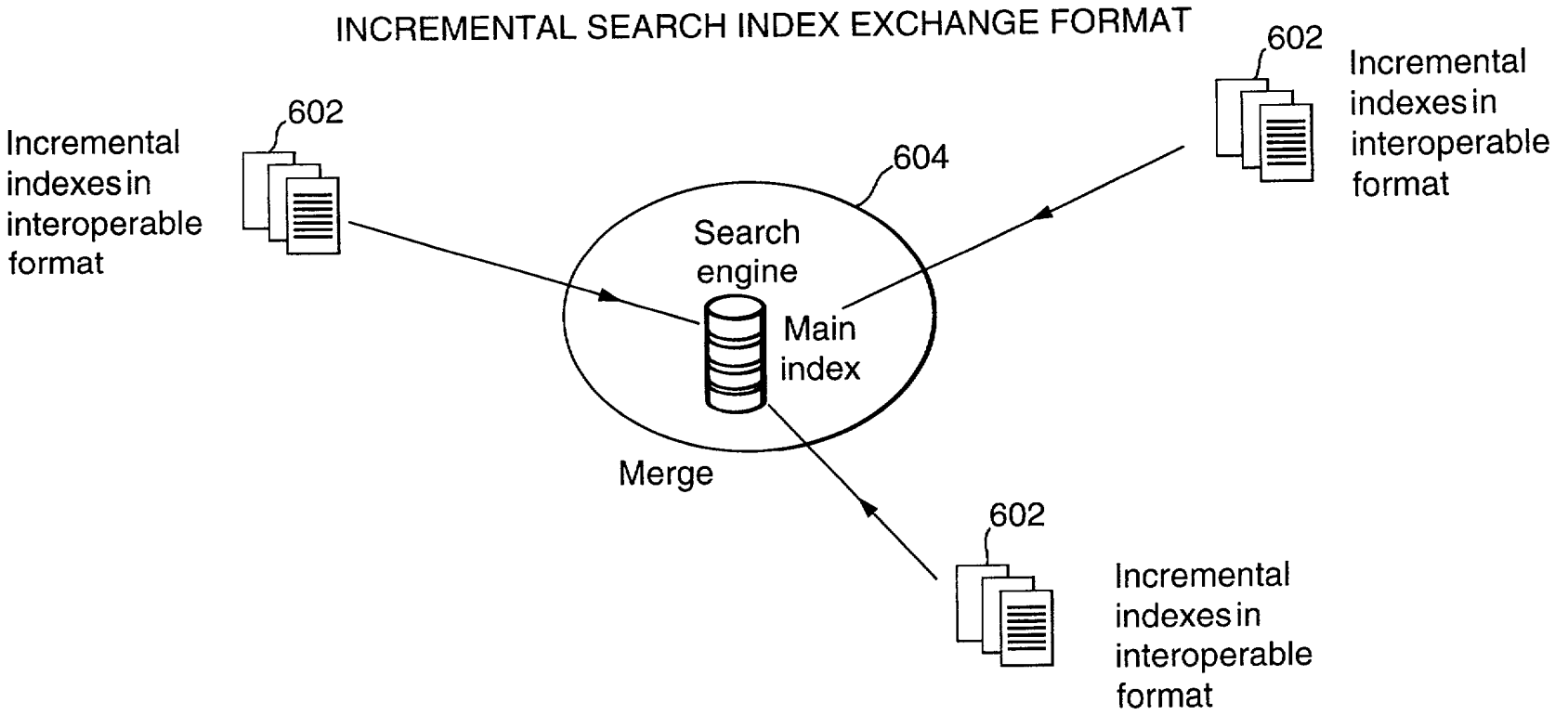


Fig.5.

INDEX AT THE TIME OF ENCRYPTION

Fig.6.


INCREMENTAL SEARCH INDEX EXCHANGE FORMAT
602
Incremental indexes in interoperable format
602
Incremental indexes in interoperable format
604
Search engine
Main index
Merge
602
Incremental indexes in interoperable format

SEARCH ENGINE AND DIGITAL RIGHTS MANAGEMENT

The present invention is in the field of search engines and digital rights management. The present invention has particular applicability to searching for content in a DRM environment where the content is encrypted.

If there is to be a viable commerce based upon the electronic distribution of valuable multimedia content (such as for example reports, images, music tracks, videos, etc.), then there must be some means of enforcing and retaining copyright control over the electronic content. There is now emerging a set of hardware and software solutions, generically known as digital rights management (DRM) solutions, that aim to provide this copyright control while, to a varying degree, also enabling new commercial models suited to the Internet and electronic delivery. Common to virtually all these solutions is the requirement that the multimedia content files be distributed within a persistent tamperproof encryption wrapper (the idea being that a million copies of encrypted content is no more valuable than one). Very simply, DRM works by carefully providing the consumers of this encrypted content with secret decryption keys that provide temporary access to the content for some controlled purpose, e.g. viewing, printing, playing, etc. without ever providing access to the raw decrypted content that could be used for unauthorised reuse or redistribution.

Figure 1 illustrates schematically an overview of how typical DRM systems work. Referring to Figure 1, a "publisher" of digital content seals their digital content

files, buffers or streams within a layer of encryption and digital signatures into a DRM-encrypted content format 102. The encryption makes it difficult for malicious consumers to obtain access to the raw decrypted content (and make unauthorised copies for redistribution). The digital signatures prevent malicious consumers from tampering with the encrypted content (perhaps to pass off the content as their own) by enabling the DRM system to detect the smallest change to the encrypted content. The DRM-encrypted content 102 can then be delivered to consumers via any electronic distribution medium 104, e.g. web, ftp, email, CD-ROM, etc. The publisher need not worry about protecting the DRM-encrypted content 102 in transit to the consumer since it is inherently protected by its encryption layer and digital signatures.

Less sophisticated DRM systems sometimes bundle individual consumer access rights with the content, either within the encryption layer or at least protected by the digital signatures. The advantage of bundling rights with the content is that the consumer can obtain both the content and the rights at the same time. Disadvantages include extreme inflexibility in the rights management policies that can be implemented and an enormous versioning problem (since there needs to be a separate version of encrypted content 102 for each consumer and a new version of the encrypted content whenever the rights change).

More sophisticated DRM systems deliver the rights separately from the content (from a DRM server 108). The rights are encoded in some electronic format 110 (i.e. electronic "rights") and specify the permitted relationship between consumers and DRM-encrypted content sets (and

subsets), e.g. which content the consumer can access, what they are permitted to do with it (e.g. printing), and for how long.

A specialised viewer (the DRM client 106) resident on the consumer device is required to obtain, manage and interpret the rights, temporarily decrypt the encrypted content and view/play it within a secure environment (so that the consumer cannot obtain access to the raw decrypted content or the decryption keys) subject to the restrictions implied by the consumer's rights (e.g. view but do not print a document). The DRM server 108 is responsible for issuing rights to requesting DRM clients 106. Current DRM systems typically issue rights to authenticated consumers at the time of purchase (or grant) and the rights are transferred to permanent storage on the consumer device 106.

In general, "content sets" can be thought of as a related set of one or more digital content files, buffers or streams. In general, "rights" can be thought of as an electronic description (explicit or by implication) of the association between consumers (or consumer devices) and DRM-protected content sets. Rights can optionally specify means of identifying the consumer (or consumer device) to which the rights 'belong'; means of identifying the content sets and subsets to which the rights apply; encryption keys and checksums (cryptographic or otherwise); and the specific access rights granted to the consumers (and/or their consumer devices) over those content sets (e.g. whether or not the consumer can print a document, the duration of access, etc.). Rights can be encoded in any machine-readable form (e.g. parsable languages, specialised

data structures, etc.) and are used internally by the DRM system to grant, deny or meter consumer access to encrypted content.

A problem raised by the proliferation of DRM-encrypted content is that the search engines that are typically used by Internet users to locate content on the Internet cannot pierce this encryption layer to build their indexes and therefore DRM-encrypted content will be difficult to locate. Search engines come in many varieties but the basic concept is simple: they are either directed to a site or follow links to a site and build complex indexes for the content that end users can subsequently use to locate content by specifying free text or more specialised searches. Search engines are used to index content from across the entire Internet (e.g. Lycos, Excite, etc.) or locally on a particular site (e.g. the Microsoft search engine that performs free text search across Microsoft's site and internal knowledge repositories).

Figure 2 illustrates schematically how a typical search engine operates. A server computer 202 controls access to both DRM-encrypted content 204 and to normal unencrypted content 206. In either case (DRM-encrypted content 204 or unencrypted content 206), the server 202 provides the content (designated by reference numeral 212 in Figure 2) via a network 208 (e.g. the Internet or an intranet) to a search engine 214. The search engine 214 is operating under the control of an indexer 216 (or "crawler") that sends requests 210 to the server 202. The search engine 214 parses the received content 212 and adds processed data to a searchable free text index 218. Because the search engine 214 is unable to parse the

received content 212 that corresponds to DRM-encrypted content 204, the DRM-encrypted content 204 is not indexed.

According to a first aspect of the present invention, there is provided a search engine that parses content encrypted by a digital rights management (DRM) system to produce a searchable index of the DRM-encrypted content, the search engine comprising: a DRM module that communicates with a DRM system to obtain access rights in order to be able to decrypt DRM-encrypted content for purposes of indexing; and, an indexer that parses the decrypted content to produce a searchable index.

According to a second aspect of the present invention, there is provided a method of producing a searchable index using a search engine that parses content encrypted by a digital rights management (DRM) system to produce a searchable index of the DRM-encrypted content, the method comprising the steps of: a DRM module of the search engine communicating with a DRM system to obtain access rights in order to be able to decrypt DRM-encrypted content for purposes of indexing; and, an indexer of the search engine parsing the decrypted content to produce a searchable index.

According to a third aspect of the present invention, there is provided a digital rights management (DRM) system, the system comprising: a DRM server that maintains location information for DRM-encrypted content managed by the server; the DRM server being adapted to communicate location information to a DRM-enabled search engine configured to index the DRM-encrypted content, to provide

for a unified, trusted search over the DRM-encrypted content managed by the DRM server.

According to a fourth aspect of the present invention, there is provided a method of providing for a unified, trusted search over digital rights management (DRM) encrypted content managed by a DRM server that maintains location information for DRM-encrypted content managed by the server, the method comprising the step of: the DRM server communicating location information to a DRM-enabled search engine configured to index the DRM-encrypted content thereby to provide for a unified, trusted search over the DRM-encrypted content managed by the DRM server.

According to a fifth aspect of the present invention, there is provided a digital rights management (DRM) system, the system comprising: a DRM server that maintains location information for DRM-encrypted content managed by the DRM server; the DRM server being adapted to issue a DRM-enabled search engine with the rights to index DRM-encrypted content managed by the DRM server and to direct a said DRM-enabled search engine to the location of the DRM-encrypted content by the DRM server.

According to a sixth aspect of the present invention, there is provided a method of enabling a search engine to index digital rights management (DRM) content managed by a DRM server that maintains location information for DRM-encrypted content managed by the server, the method comprising the steps of: the DRM server issuing the DRM-enabled search engine with the rights to index DRM-encrypted content managed by the DRM server and directing

the DRM-enabled search engine to the location of the DRM-encrypted content.

According to a seventh aspect of the present invention, there is provided a digital rights management (DRM) system, the system comprising: a DRM encryption toolkit arranged to produce an index of unencrypted content before encrypting the unencrypted content to produce DRM-encrypted content, and arranged to issue the index and location of the DRM-encrypted content to a search engine to enable a said search engine to merge the index and location of the DRM-encrypted content into a complete search engine index.

According to an eighth aspect of the present invention, there is provided a method of producing a searchable index of digital rights management (DRM) encrypted content, the method comprising the steps of: a DRM encryption toolkit producing an index of unencrypted content before encrypting the unencrypted content to produce DRM-encrypted content such that a search engine can merge the index and location of the DRM-encrypted content into a complete search engine index.

According to a ninth aspect of the present invention, there is provided a digital rights management (DRM) system including an indexing capability, the system comprising: a DRM encryption toolkit arranged to produce an index in an interoperable index format capable of being merged into a complete index of at least one search engine.

According to a tenth aspect of the present invention, there is provided a digital rights management (DRM) data structure comprising publicly accessible data, placed in with DRM-protected information but visible through a DRM encryption layer, that is descriptive of the contents of the DRM-protected information and that is to be indexed.

According to an eleventh aspect of the present invention, there is provided a storage medium having stored thereon/therein a data structure as described above.

According to a twelfth aspect of the present invention, there is provided a method of protecting information by digital rights management (DRM), the method comprising the steps of: protecting the information using DRM; and, placing publicly accessible data in with the DRM-protected information such that the publicly accessible data is visible through the DRM encryption layer, the publicly accessible data being descriptive of the contents of the DRM-protected information and being indexable by a search engine.

In accordance with a preferred embodiment of the present invention, DRM-encrypted content is "opened up" to "trusted search", without compromising copyright control, thus allowing end users to locate DRM-encrypted content alongside open unencrypted content. The indexer (or crawler) of a search engine is provided a DRM module for communication with a DRM server so that the indexer can access even the DRM-encrypted content nominally as if it were a human end user of the content. The indexer may be issued with a DRM-recognised "identity" so as to

distinguish itself from other end users and other DRM-enabled search engines. Thus, the search engine can programmatically access the content, subject to being able to obtain permission from the DRM system.

Embodiments of the present invention will now be described by way of example with reference to the accompanying drawings, in which:

Figure 1 illustrates schematically an overview of conventional digital rights management (DRM) systems;

Figure 2 illustrates schematically an overview of a conventional search engine;

Figure 3 illustrates schematically the use of an example of a "DRM-enabled" search engine in accordance with an embodiment of the present invention;

Figure 4 illustrates schematically an example of how a DRM-enabled search engine may interoperate with a DRM service bureau in accordance with an embodiment of the present invention;

Figure 5 illustrates schematically an example of a DRM system in which indexing is done at the time of encryption in accordance with an embodiment of the present invention; and,

Figure 6 illustrates schematically an example of the use of an incremental search index exchange format in accordance with an embodiment of the present invention.

In accordance with the preferred embodiment of the present invention, DRM-encrypted content is "opened up" to "trusted search", without compromising copyright control, thus allowing end users to locate DRM-encrypted content alongside open unencrypted content.

Figure 3 illustrates schematically an example of an embodiment of the present invention. Like the prior art Figure 2 embodiment, a request 210 is made to access particular content available via a network 208 which may be or include the Internet, an intranet or other network. The indexer (or crawler) 216 of the search engine 214 has a DRM module 302 for communication with a DRM server 306 so that it can access the content nominally as if it were a human end user of the content. In some embodiments, the indexer 216 is issued with a DRM-recognised "identity" so as to distinguish itself from other end users and DRM-enabled search engines. Thus, the search engine 214 can programmatically access the content, subject to being able to obtain permission from the DRM solution. That is, where a human would use a secure DRM-controlled viewer to read or play encrypted content, the "crawler" 216 is provided with the secure DRM-controlled module 302 to be able to programmatically access and index encrypted content.

When the crawler 216 attempts to index the encrypted content within the content 212, the crawler 216 is granted or denied access to the encrypted content depending upon whether the content owner has indicated to the DRM server 306 to authorise the DRM module 302 to associate the crawler 216 with the rights to access and index that encrypted content. For most DRM solutions, this

authorisation involves the crawler 216 requesting and receiving from the DRM server 306 a cryptographic key 304 for a given content file from the DRM solution, temporarily decrypting the file, and then performing its normal indexing procedure as if the file had never been encrypted. According to one embodiment, rights granted may be revoked. For example, a content owner may want to revoke access to a specific search engine.

Figure 4 illustrates schematically how a DRM bureau may interoperate with DRM-enabled search engines. That is, some DRM solutions are operated in a bureau fashion, by which it is meant that a third party organisation provides a DRM-based service that publishers can use to securely publish their content 401 to DRM-enabled consumers 106 without needing to support their own potentially expensive DRM infrastructure (e.g. rights-clearing servers, secure repositories, etc.). In most DRM architectures, this amounts to a network-accessible DRM server 306 that handles the "behind-the-scenes" rights management traffic (e.g. buying rights, storing rights, serving rights, etc.) that arises as consumers purchase and use DRM-encrypted content 212.

Depending upon how the DRM bureau server operates, it may over time accumulate a large amount of information about where encrypted files are located (from logging at the time of encryption and consumption, from the DRM encryption toolkits 402 and secure viewers executing in the client computers 106 respectively). Using trusted search capabilities such as was described above with reference to Figure 3, a DRM bureau server 306 can therefore provide a unified, trusted search over the set of DRM-encrypted

content 212 managed by that DRM server 306. This may, for example, be by operating a DRM-enabled search engine 404, or directing a third-party DRM-enabled search engine 408 to the content files 212. This search capability is typically available to all consumers accessing encrypted content via that DRM bureau and provides a unified search across all the encrypted content from participating publishers.

The DRM encrypt functionality 402 uses hardware or software components to actually encrypt the content files 401. The files are either encrypted by the publisher or on their behalf by a DRM service provider. Often, but not always, additional information is embedded alongside the content and within the encryption, e.g. information about the content, the publisher, where to go to obtain access rights, abstracts, watermarks, etc.

Figure 5 illustrates schematically an example of a system in which indexing is done at the time of encryption. Namely, the DRM encryption toolkit 402 has access to the "raw" content 401 prior to encryption so the toolkit 402 can itself integrate the search engine's indexing technology and generate an index record 502 for the content file 401 as part of the encryption process. This index record 502, together with an indication of the location of the encrypted file, is provided to the search engine 504 to be merged into a complete index. This is a useful concept since the final part of the electronic publishing process could be viewed (see reference numeral 502) as (i) index, (ii) encrypt, (iii) publish to accessible location, and (iv) send index record plus location to be merged into full search engine index. This reduces the rather hit and miss approach of publishing content and then endeavouring to

attract the attention of search engines to come and index recently published content.

The Figure 5 embodiment can be generalised to both the case of a DRM bureau that either encrypts the publisher's content on their behalf or provides tools to allow the publisher to encrypt their own content to make use of the bureau's DRM solution. In both cases, the encryption tool can, as described above, index the content file prior to encryption and either transmit the index information (a) to third party search engines, or (b) to the bureau for consolidation prior to transmission on to third party search engines (dramatically increasing indexing throughput), or (c) to a "unified" bureau search engine as described above.

In another embodiment, the publishers can add publicly accessible data (e.g. abstracts) to DRM-protected content, either at the time the content is encrypted by the DRM encryption toolkit 402 or afterwards, that is outside the encryption wrapper and can be indexed by search engines that have not been DRM-enabled. This data would be chosen to be descriptive of the DRM-protected content so that, when indexed by a search engine, it will lead the search engine to the DRM-protected content it describes.

In yet another embodiment, the publicly accessible data is protected from tampering by digital signatures, so that if the data is modified the DRM-enabled search engines 404 and DRM clients 106 can detect this tampering and ignore the tampered data.

In yet another embodiment, the publicly accessible data added to the DRM-encrypted content is metadata or keywords chosen by the publisher to correspond to terms sent to search engines, similar to meta tags in HTML pages.

In yet another embodiment, the publicly accessible data added to the DRM-encrypted content is automatically generated using search indexing technology which automatically generates a sequence of keywords from the DRM-protected content that is indexable by other search engines but from which the original DRM-protected content cannot be reconstituted.

Figure 6 illustrates schematically how multiple incremental indexes 602 resulting from the integration of search engine indexing technology into publishing components such as the DRM content encryption component are consolidated by a search engine merge function 604 into a "complete" index that is usable by the search engine to answer end user search requests. In one embodiment, the multiple search engines exchange and consolidate incremental search indexes in an interoperable electronic file format. The incremental search indexes have sufficient information to be efficiently merged into the complete index used for the actual search.

Embodiments of the present invention have been described with particular reference to the examples illustrated. However, it will be appreciated that variations and modifications may be made to the examples described within the scope of the present invention.

CLAIMS

1. A search engine that parses content encrypted by a digital rights management (DRM) system to produce a searchable index of the DRM-encrypted content, the search engine comprising:

a DRM module that communicates with a DRM system to obtain access rights in order to be able to decrypt DRM-encrypted content for purposes of indexing; and,

an indexer that parses the decrypted content to produce a searchable index.

2. A search engine according to claim 1, wherein the search engine has an identity that can be recognised by a said DRM system and wherein the access rights are obtained from said DRM system based on the identity.

3. A search engine according to claim 1 or claim 2, wherein the access rights issued to the search engine are limited to those required for indexing the DRM-encrypted content.

4. A search engine according to any of claims 1 to 3, wherein the search engine is issued the access rights to index a subset of available DRM-encrypted content.

5. A search engine according to any of claims 1 to 4, wherein the access rights are selectively granted and revoked.

6. A method of producing a searchable index using a search engine that parses content encrypted by a digital rights management (DRM) system to produce a searchable

index of the DRM-encrypted content, the method comprising the steps of:

a DRM module of the search engine communicating with a DRM system to obtain access rights in order to be able to decrypt DRM-encrypted content for purposes of indexing; and,

an indexer of the search engine parsing the decrypted content to produce a searchable index.

7. A method according to claim 6, comprising the steps of:

the search engine identifying itself to the DRM system and obtaining the access rights from said DRM system on the basis of the search engine's identity.

8. A method according to claim 6 or claim 7, wherein the access rights issued to the search engine are limited to those required for indexing the DRM-encrypted content.

9. A method according to any of claims 6 to 8, wherein the search engine is issued the access rights to index a subset of available DRM-encrypted content.

10. A search engine according to any of claims 6 to 9, wherein the access rights are selectively granted and revoked.

11. A digital rights management (DRM) system, the system comprising:

a DRM server that maintains location information for DRM-encrypted content managed by the server;

the DRM server being adapted to communicate location information to a DRM-enabled search engine configured to index the DRM-encrypted content, to provide for a unified, trusted search over the DRM-encrypted content managed by the DRM server.

12. A system according to claim 11, wherein the DRM server is adapted to communicate the location information to a said DRM-enabled search engine as the DRM server obtains the location information.

13. A system according to claim 11 or claim 12, comprising means for granting a said DRM-enabled search engine additional rights to enable it to decrypt and index additional DRM-encrypted content managed by the DRM server.

14. A method of providing for a unified, trusted search over digital rights management (DRM) encrypted content managed by a DRM server that maintains location information for DRM-encrypted content managed by the server, the method comprising the step of:

the DRM server communicating location information to a DRM-enabled search engine configured to index the DRM-encrypted content thereby to provide for a unified, trusted search over the DRM-encrypted content managed by the DRM server.

15. A method according to claim 14, wherein the DRM server communicates the location information to the DRM-enabled search engine as the DRM server obtains the location information.

16. A method according to claim 14 or claim 15, comprising the step of granting the DRM-enabled search engine additional rights to enable it to decrypt and index additional DRM-encrypted content managed by the DRM server.

17. A digital rights management (DRM) system, the system comprising:

a DRM server that maintains location information for DRM-encrypted content managed by the DRM server;

the DRM server being adapted to issue a DRM-enabled search engine with the rights to index DRM-encrypted content managed by the DRM server and to direct a said DRM-enabled search engine to the location of the DRM-encrypted content by the DRM server.

18. A method of enabling a search engine to index digital rights management (DRM) content managed by a DRM server that maintains location information for DRM-encrypted content managed by the server, the method comprising the steps of:

the DRM server issuing the DRM-enabled search engine with the rights to index DRM-encrypted content managed by the DRM server and directing the DRM-enabled search engine to the location of the DRM-encrypted content.

19. A digital rights management (DRM) system, the system comprising:

a DRM encryption toolkit arranged to produce an index of unencrypted content before encrypting the unencrypted content to produce DRM-encrypted content, and arranged to issue the index and location of the DRM-encrypted content to a search engine to enable a said search engine to merge

the index and location of the DRM-encrypted content into a complete search engine index.

20. A system according to claim 19, comprising a said search engine which is operated by a party other than the party operating the DRM encryption toolkit.

21. A system according to claim 19 or claim 20, comprising a DRM server and a said search engine which is operated in conjunction with the DRM server.

22. A system according to any of claims 19 to 21, wherein the system is arranged to consolidate index and location information from multiple DRM-encrypted files into a consolidated index and location format before the information is merged into a complete index of a search engine.

23. A method of producing a searchable index of digital rights management (DRM) encrypted content, the method comprising the steps of:

a DRM encryption toolkit producing an index of unencrypted content before encrypting the unencrypted content to produce DRM-encrypted content such that a search engine can merge the index and location of the DRM-encrypted content into a complete search engine index.

24. A method according to claim 23, wherein the search engine is operated by a party other than a party operating the DRM encryption toolkit.

25. A method according to claim 23 or claim 24, wherein the search engine is operated in conjunction with a DRM server.

26. A method according to any of claims 23 to 25, comprising the step of consolidating index and location information from multiple DRM-encrypted files into a consolidated index and location format before the information is merged into a complete index of a search engine.

27. A digital rights management (DRM) system including an indexing capability, the system comprising:

a DRM encryption toolkit arranged to produce an index in an interoperable index format capable of being merged into a complete index of at least one search engine.

28. A digital rights management (DRM) data structure comprising publicly accessible data, placed in with DRM-protected information but visible through a DRM encryption layer, that is descriptive of the contents of the DRM-protected information and that is to be indexed.

29. A data structure according to claim 28, wherein the publicly visible data is protected from tampering by a digital signature.

30. A data structure according to claim 28 or claim 29, wherein the publicly visible data is metadata placed in with the DRM-protected information.

31. A data structure according to any of claims 28 to 30, wherein the publicly visible data is generated using search engine indexing technology applied at the time the content is encrypted by a DRM system.

32. A storage medium having stored thereon/therein a data structure according to any of claims 28 to 31.

33. A method of protecting information by digital rights management (DRM), the method comprising the steps of:

protecting the information using DRM; and,

placing publicly accessible data in with the DRM-protected information such that the publicly accessible data is visible through the DRM encryption layer, the publicly accessible data being descriptive of the contents of the DRM-protected information and being indexable by a search engine.

34. A method according to claim 33, wherein the publicly visible data is protected from tampering by a digital signature.

35. A method according to claim 33 or claim 34, wherein the publicly visible data is metadata placed in with the DRM-protected information.

36. A method according to any of claims 33 to 35, wherein the publicly visible data is generated using search engine indexing technology applied at the time the content is encrypted by a DRM system.

37. A search engine, substantially in accordance with any of the examples as hereinbefore described with reference to and as illustrated by the accompanying drawings.

38. A method of producing a searchable index, substantially in accordance with any of the examples as hereinbefore described with reference to and as illustrated by the accompanying drawings.

39. A digital rights management (DRM) system, substantially in accordance with any of the examples as hereinbefore described with reference to and as illustrated by the accompanying drawings.

40. A method of providing for a unified, trusted search over digital rights management (DRM) encrypted content, substantially in accordance with any of the examples as hereinbefore described with reference to and as illustrated by the accompanying drawings.

41. A method of enabling a search engine to index digital rights management (DRM) content, substantially in accordance with any of the examples as hereinbefore described with reference to and as illustrated by the accompanying drawings.

42. A data structure substantially in accordance with any of the examples as hereinbefore described with reference to and as illustrated by the accompanying drawings.

43. A computer readable storage medium containing a digital rights management (DRM) data structure, substantially in accordance with any of the examples as

hereinbefore described with reference to and as illustrated by the accompanying drawings.

44. A method of protecting information by digital rights management (DRM), substantially in accordance with any of the examples as hereinbefore described with reference to and as illustrated by the accompanying drawings.

24/

Application No:	GB 0112627.5	**Examiner:**	Nik Dowell
Claims searched:	1 to 10, 14 to 16, 18, 23 to 26, 37, 38, 40, 41	**Date of search:**	30 January 2002

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.T): G4A (AAP, AUDB)

Int Cl (Ed.7): G06F (1/00, 17/30)

Other: Online : WPI, EPODOC, PAJ, INSPEC, ELSEVIER, TDB, WWW

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
A,E	EP 1 130 490 (M Ken) see especially column 33, line 16 to 55	-

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.