

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

Inventor(s): VESTERGAARD, Steve; TSUI, Che-Wai; KOLIC, Edward
Title: **DIGITAL MEDIA DISTRIBUTION METHOD AND SYSTEM**
Serial No.: 09/980582
Filed: 5 March 2001
Examiner: TO, Baotran N. Art Unit: 2135
Date: 25 August 2008

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

AMENDMENT

This communication is responsive to the Office Action mailed 27 March 2007 as extended, where applicable, by payment of extension of time fees pursuant to 37 CFR § 1.136(a).

A Request for Continued Examination under 37 CFR § 1.114 is enclosed herewith.

Please amend this application as follows:

- **Amendments to the Claims** are reflected in the listing of claims which begins on page 2 of this paper.
- **Remarks** begin on page 13 of this paper.

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in this application:

Listing of Claims:

1. (Currently Amended) A method of distributing electronic media, the method comprising:
 - receiving a file at a user computing device, the file comprising an integral decryption engine and encrypted media content;
 - requesting a decryption key from a remote server;
 - receiving the decryption key from the remote server at the user computing device over a communication network, the decryption key itself encrypted at the remote server with a user key, the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device such that the user computing device can use the user key to decrypt the decryption key; and
 - responding to receipt of said decryption key from said remote server at the user computing device by:
 - using the user key to decrypt the decryption key at the user computing device;
 - decrypting said media content at the user computing device using said integral decryption engine and the decryption key
- wherein receiving the file at the user computing device comprises receiving the file from a remote computer over the communication network that includes the remote server from which the decryption key is received but through a communication path that does not include the remote server from which the decryption key is received.

2. (Previously Presented) The method of claim 1, comprising, after decrypting the media content, viewing said media content by executing viewer software, the viewer software also integral with said file.
3. (Previously Presented) The method of claim 1, comprising, after decrypting the media content, viewing said media content by executing external viewer software linked to said file.
4. (Currently Amended) A method of managing distribution of proprietary electronic media, the method comprising:
 - receiving a single file at a user computing device, the single file comprising an integral decryption engine, encrypted media content and integral media playback software, the single file executable independently of other programs to:
 - obtain a decryption key from a remote server over a communication network, the decryption key itself encrypted at the remote server with a user key, the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device such that the user computing device can use the user key to decrypt the decryption key;
 - use the user key to decrypt the decryption key at the user computing device;
 - decrypt the media content using the integral decryption engine and the decryption key; and
 - view the media content using the integral media playback software

wherein receiving the single file comprises downloading said single file from a computer via the communication network;

wherein the communication network from which the single file is downloaded includes the remote server from which the decryption key is obtained; and

wherein downloading the single file from the computer via the communication network comprises downloading the single file from the computer through a communication path that does not include the remote server from which the decryption key is obtained.

5.-10. (Cancelled)

11. (Previously Presented) The method of claim 4, wherein said remote server tracks a number of decryption keys relating to the single file that have been issued by the remote server.

12.-16. (Cancelled)

17. (Previously Presented) A method according to claim 35 wherein the file is executable independently of other programs and wherein generating the user key, requesting the decryption key, using the user key to decrypt the decryption key and decrypting the media content are accomplished by executing the file.

18. (Previously Presented) A method according to claim 17 wherein the file also comprises integral media player software and wherein executing the file also causes execution of the integral media player software and playback of the media content.

19. (Cancelled)

20. (Previously Presented) A method according to claim 2 wherein decrypting the media content and viewing the media content are accomplished without storing a decrypted copy of the media content in memory accessible to a user of the user computing device.
21. (Previously Presented) A method according to claim 4 wherein decrypting the media content and viewing the media content are accomplished without storing a decrypted copy of the media content in memory accessible to a user of the user computing device.
- 22.-24. (Cancelled)
25. (Previously Presented) A method according to claim 1 wherein receiving the file at the user computing device comprises downloading the file from the remote computer using a peer to peer network, the remote computer different from the remote server from which the decryption key is received.
26. (Cancelled)
27. (Previously Presented) A method according to claim 1 comprising previewing a previewable portion of the media content prior to decrypting the media content using the integral decryption engine and the decryption key.
28. (Previously Presented) A method according to claim 4 wherein the single file is executable to view the media content using the integral media playback software without storing a decrypted copy of the media content in memory accessible to a user of the user computing device.

29.-30. (Cancelled)

31. (Previously Presented) A method according to claim 4 wherein the remote server tracks a number of decryption keys relating to the single file that have been issued by the remote server.

32. (Cancelled)

33. (Previously Presented) A method according to claim 4 comprising previewing a previewable portion of the media content prior to decrypting the media content using the integral decryption engine and the decryption key.

34. (Previously Presented) A method according to claim 1 comprising generating the user key at the user computing device.

35. (Previously Presented) A method according to claim 34 wherein decrypting the media content at the user computing device using the integral decryption engine and the decryption key comprises using the user key to decrypt the decryption key and to thereby obtain a decrypted decryption key.

36. (Previously Presented) A method according to claim 35 wherein using the user key to decrypt the decryption key is performed without storing the decrypted decryption key in memory accessible to a user of the user computing device.

37. (Cancelled)
38. (Previously Presented) A method according to claim 36 wherein decrypting the media content and viewing the media content are accomplished without storing a decrypted copy of the media content in memory accessible to a user of the user computing device.
39. (Cancelled)
40. (Previously Presented) A method according to claim 35 comprising previewing a previewable portion of the media content prior to decrypting the media content using the integral decryption engine and the decryption key.
41. (Previously Presented) A method according to claim 35 wherein receiving the file at the user computing device comprises downloading the file from the remote computer using a peer to peer network, the remote computer different from the remote server from which the decryption key is received.
42. (Previously Presented) A method according to claim 1 wherein decrypting the media content at the user computing device using the integral decryption engine and the decryption key comprises using the user key to decrypt the decryption key and to thereby obtain a decrypted decryption key.
43. (Previously Presented) A method according to claim 4, wherein execution of the single file causes the user computing device to generate the user key at the user computing device.

44. (Previously Presented) A method according to claim 43 wherein execution of the single file to decrypt the media content using the integral decryption engine and the decryption key comprises using the user key to decrypt the decryption key and to thereby obtain a decrypted decryption key.

45. (Cancelled)

46. (Previously Presented) A method of distributing electronic media, the method comprising:

receiving a file at a user computing device, the file comprising an integral decryption engine and encrypted media content;

generating a user key at the user computing device, the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device;

requesting a decryption key from a remote server;

receiving the decryption key from the remote server at the user computing device over a communication network, the decryption key itself encrypted at the remote server with the user key such that the user computing device can use the user key to decrypt the decryption key; and

responding to receipt of said decryption key from said remote server at the user computing device by:

using the user key to decrypt the decryption key and to thereby obtain a decrypted decryption key at the user computing device; and

decrypting said media content at the user computing device using said integral decryption engine and the decrypted decryption key;

wherein receiving the file at the user computing device comprises receiving the file from a remote computer over the communication network that includes the remote server from which the decryption key is received but through a communication path that does not include the remote server from which the decryption key is received.

47. (Cancelled)

48. (Previously Presented) A method according to claim 1 comprising:

sending the file from the user computing device to a second user computing device over the communication network over a second communication path that does not include the remote server;

upon receipt of the file at the second user computing device:

sending a request, from the second user computing device to the remote server, for the decryption key;

receiving the decryption key from the remote server at the second user computing device, the decryption key itself encrypted at the remote server with a second user key, the second user key bonded to the second user computing device by being based at least in part on one or more characteristics of the second user computing device such that the second user computing device can use the second user key to decrypt the decryption key; and

responding to receipt of the decryption key from the remote server at the second user computing device by decrypting the media content at the second user

computing device using the integral decryption engine and the decryption key.

49. (Previously Presented) A method according to claim 48 comprising, after receiving the file at the second user computing device, generating the second user key at the second user computing device.
50. (Previously Presented) A method according to claim 49 wherein decrypting the media content at the second user computing device using the integral decryption engine and the decryption key comprises using the second user key to decrypt the decryption key and to thereby obtain a decrypted decryption key.
51. (Cancelled)
52. (Previously Presented) A method according to claim 4 comprising:
- sending the file from the user computing device to a second user computing device over the communication network over a second communication path that does not include the remote server;
 - upon receipt of the file at the second user computing device:
 - sending a request, from the second user computing device to the remote server, for the decryption key;
 - receiving the decryption key from the remote server at the second user computing device, the decryption key itself encrypted at the remote server with a second user key, the second user key bonded to the second user computing device by being based at least in part on one or more characteristics of the

second user computing device such that the second user computing device can use the second user key to decrypt the decryption key; and

responding to receipt of the decryption key from the remote server at the second user computing device by decrypting the media content at the second user computing device using the integral decryption engine and the decryption key.

53. (Previously Presented) A method according to claim 52 comprising, after receiving the single file at the second user computing device, generating the second user key at the second user computing device.
54. (Previously Presented) A method according to claim 53 wherein decrypting the media content at the second user computing device using the integral decryption engine and the decryption key comprises using the second user key to decrypt the decryption key and to thereby obtain a decrypted decryption key.
55. (Previously Presented) A method according to claim 1 wherein the decryption key received at the user computing device is permanent such that decrypting the media content at the user computing device using the integral decryption engine and the decryption key may be performed multiple times at the user computing device using the integral decryption engine and the same decryption key.
56. (Previously Presented) A method according to claim 4 wherein the decryption key obtained at the user computing device is permanent such that subsequent executions of the single file decrypt the media content at the user computing device using the integral decryption engine and the same decryption key.

57. (Previously Presented) A method according to claim 1 wherein the user key is based on a digital fingerprint of the user computing device.

58. (Previously Presented) A method according to claim 4 wherein the user key is based on a digital fingerprint of the user computing device.

REMARKS

This communication is responsive to the Office Action dated 27 March 2008, as extended by payment of appropriate extension of time fees pursuant to 37 CFR § 1.136(a).

Claims 1-4, 11, 17, 18, 20, 21, 25, 27, 28, 31, 33-36, 38, 40-44, 46, 48-50 and 52-58 were pending prior to this paper. In this paper, the Applicant has amended claims 1 and 4. These amendments are submitted to be completely supported by the application as originally filed and to add no new matter. Claims 1-4, 11, 17, 18, 20, 21, 25, 27, 28, 31, 33-36, 38, 40-44, 46, 48-50 and 52-58 remain pending for prosecution.

A Request for Continued Examination pursuant to 37 CFR § 1.114 is enclosed herewith.

An Affidavit pursuant to 37 CFR § 1.132 sworn by one of the inventors, Steve Vestergaard, is also enclosed herewith.

Claims 1-3, 17, 18, 20, 25, 27, 34-36, 38, 40-42, 48-50, 55 and 57

The Examiner has raised the combination of US7,103,574 (Peinado et al., referred to herein as Peinado), US6,052,780 (Glover), US 2001/0011238 (Eberhard) and US6,892,306 (En-Seung et al., referred to herein as En-Seung) in connection with claim 1. The Applicant submits that claim 1 and all of the claims that depend from claim 1 patentably distinguish the combination of Peinado, Glover, En-Seung and Eberhard.

As understood by the Applicant, Peinado discloses an enforcement architecture for implementing digital rights management. Content (12) is distributed from a content server (22) to a user computing device (14) and, when an attempt is made to render content (12) using a rendering application (34), a digital rights management (DRM) system (32) resident on user computer (14) is invoked. The digital rights management system (32) includes a black box (30) obtained from a black box server (26). Digital rights management system (32) determines whether the user has the right to render content (12) and, if the right does not exist, requests the right from a license server (24).

Integral decryption engine

Following the Examiner' logic presented on pages 2-3 of the Office Action, the Examiner correctly acknowledges that Peinado does not disclose the following claim 1 features:

- the file comprising the encrypted media content received at the user computing device also comprises an integral decryption engine; and
- using the integral decryption engine together with the decryption key to decrypt the media content.

The Examiner expresses the view that these features missing from Peinado are disclosed by Glover and that it would be obvious to incorporate these features from Glover into the Peinado system. The rationale advanced by the Examiner for this contention of obviousness is the motivation “to provide the support for the specific form of corresponding decryption” as allegedly described in the Abstract of Glover.

The Applicant respectfully submits that it would not be obvious to modify the Peinado digital rights management (DRM) architecture to a provide media content file with an integral decryption engine.

The Applicant submits that Peinado teaches directly away from media content files with integral decryption engines by adopting a DRM architecture (32) that resides on the user computer (14). This aspect of Peinado is shown clearly in Fig. 4 and described at col. 2, ln. 51-53. The Peinado DRM system (32) resident on user computer (14) supports the specific forms of decryption associated with digital content (12) which is encrypted in accordance with the Peinado DRM architecture – i.e. by the Peinado authoring tool (18).

In accordance with the Peinado architecture, content (12) is encrypted (by authoring tool (18)) and sent from content server (22) to user computer (14). Peinado specifically states that the content package (12p) is distributed “without regard to any trust or security issues,” because security and trust issues are dealt with by the license server (24) and the DRM system (32) on the user’s computing device (14) – see col. 9, ln. 32-36. These Peinado statements teach directly away from bundling the Peinado content and a decryption engine together in a single file.

The Peinado DRM system (32) on user computer (14) includes a black box (30) – see Fig. 4. Black box (30) is the component of the Peinado DRM system (32) that performs encryption and decryption functions – see col. 12, ln. 3-4 and col. 15, ln. 13-15. In accordance with the teachings of Peinado, DRM system (32) obtains and/or upgrades black box (30) by interaction with a black box server (26) – see col. 11, ln. 67 to col. 12, ln. 2. The process of obtaining/upgrading the Peinado black box (30) from black box server (26) is explained in detail at col. 21, ln. 40 to col. 23, ln. 17. The Peinado system teaches that the content is obtained from content server (22) without regard for security issues because security issues are dealt with by a separate component responsible for decryption functions (black box (30)) which is obtained from a black box server (26) in a process completely separate from delivery of content (12). These aspects of Peinado teach directly away from providing a media content file with an integral decryption engine.

The Peinado black box (30) is specified to be “tightly tied to or associated with the user’s computing device (14)” which is specifically described to prevent transfer of black box (30) between users. More specifically, DRM system (32) provides hardware information about the user’s computing device (14) to black box server (26) and the black box (30) generated by black box server (26) incorporates this hardware information - see col. 22, ln. 63 to col. 23, ln. 7. Thus, the Peinado component responsible for decryption (black box (30)) originates from black box server (26) and incorporates prior information about the user computing device. This aspect of the Peinado system would not be possible if the decryption engine was incorporated into the media content file, since the file would not have any knowledge *a priori* about the user computing device. Accordingly, this aspect of Peinado teaches directly away from a media content file with an integral decryption engine.

Peinado discloses how the black box (30) on user computer (14) is evaluated at license server (24) to determine whether the black box (30) is sufficiently current. According to Peinado, the currency of black box (30) is an indicator that black box (30) has not been tampered with – i.e. that black box (30) is secure. This aspect of Peinado is described at col. 19, ln. 39-60. If black box (30) is not sufficiently current, then Peinado teaches that DRM system (32) on user computer (14) must upgrade black box (30) by requesting another black box from black box server (26). Thus, the Peinado component responsible for decryption (black box (30)) is required to be current in

order to obtain a license from license server (24) and is required to be updated by interaction with black box server (26) in order to demonstrate its veracity. These aspects of the Peinado system would not be possible if the decryption engine was incorporated into the media content file, since the file would not be updatable. Accordingly, these aspects of Peinado teach directly away from a media content file with an integral decryption engine.

Based on this reasoning, the Applicant submits that it would not be obvious to modify the Peinado digital rights management (DRM) architecture to provide the claim 1 feature of a media content file with an integral decryption engine.

Decrypting decryption key using user key

On page 5 of the Office Action, the Examiner correctly acknowledges that Peinado, Glover and Eberhard do not disclose the claim 1 feature that the user computing device can make use of the “user key” to decrypt the decryption key. The “user key” is recited in claim 1 to be the same key that is used to encrypt the decryption key at the remote server.

The Examiner expresses the view that this feature missing from the combination of Peinado, Glover and Eberhard is disclosed by En-Seung and that it would be obvious to incorporate this features from En-Seung into the Peinado system as modified by Glover and Eberhard. The rationale advanced by the Examiner for this contention of obviousness is the motivation “to prevent an individual from making a useful copy of the information” as allegedly described at col. 21, ln. 20-60 of Glover.

The Applicant has amended claim 1 to explicitly recite that the user key is actually used at the user computing device to decrypt the decryption key. More specifically, claim 1 has been amended to recite “using the user key to decrypt the decryption key at the user computing device”. Claim 1 also recites that the “user key” is used at the remote server to encrypt the decryption key. The Applicant submits that it would not be obvious to modify the Peinado system to incorporate the use of a single “user key” to encrypt the decryption key at a remote server and to decrypt the decryption key at the user computing device.

On page 3 of the Office Action, the Examiner expresses the view that the Peinado decryption key (referred to by Peinado as “KD”) corresponds with the decryption key recited in claim 1. As taught by Peinado, the decryption key (KD) is requested from license server (24) by DRM system (32). The Peinado process of requesting a license (including decryption key (KD)) is described in detail at col. 18, ln. 1 to col. 21, ln. 39. The Peinado decryption key (KD) is encrypted at license server (24) with the public key of black box (30) – referred to by Peinado as “PU-BB” – see col. 20, ln. 56-58. The black box public key (PU-BB) is provided to license server (24) by DRM system (32) as part of the license request – see col. 18, ln. 32-35. At user computing device (14), Peinado teaches that the private key of black box (30) – referred to as PR-BB – is used to decrypt the decryption key (KD), which is in turn used to decrypt the content. It is noted that the black box private key (PR-BB) used to decrypt the decryption key (KD) at user computing device (14) is different than the black box public key (PU-BB) used to encrypt the decryption key (KD) at license server (24). This process is commonly referred to today as “asymmetric encryption” or “public/private key pair encryption”.

Asymmetric encryption may be contrasted with “symmetric encryption”. Symmetric encryption involves using the same key to encrypt a message and to decrypt the message. Claim 1 (as amended) explicitly recites that the decryption key is encrypted at the remote server using a “user key” and decrypted at the user computing device using the same “user key”. This is an example of symmetric encryption.

The Applicant submits that it would not be obvious to modify Peinado to encrypt/decrypt the decryption key (KD) with a symmetrical user key. Firstly, the Peinado inventors were explicitly aware of the possibility of using symmetrical decryption, as Peinado expressly teaches that the decryption key (KD) encrypts the media content (12) using symmetrical encryption – see col. 6, ln. 65 to col. 7, ln. 1. Peinado expressly contrasts such a symmetrical encryption system with asymmetrical encryption (e.g. the black box key pair PU-BB/PR-BB used to encrypt/decrypt decryption key (KD)) – see col. 9, ln. 62 to col. 10, ln. 8. However, despite knowing about both symmetrical and asymmetrical encryption techniques, Peinado makes no suggestion that symmetric encryption could be used to encrypt/decrypt decryption key (KD). It follows that the

Peinado inventors did not consider it to be appropriate to use symmetric decryption to encrypt/decrypt decryption key (KD) in accordance with the Peinado architecture.

The use of symmetric encryption presents an operational issue for content delivery systems, as the single key must be available at the location where the message is encrypted and the location where the message is decrypted. However, sending the single key between the encryption location and the decryption location on a network presents a security risk, because the key could be intercepted by nefarious users or the like. This issue associated with symmetrical encryption is recognized by Peinado, as the entire Peinado architecture is a mechanism for transporting the symmetric content decryption key (KD) from the authoring tool (18)/content server (22) (i.e. the encryption location) to the user computer (14) (i.e. the decryption location) in a manner where the symmetric content decryption key (KD) is not exposed to nefarious users.

Some prior art systems addresses this issue with symmetric encryption by sending symmetric keys over different communication channels than the media content itself. This is an undesirable solution for internet-based content delivery, because it can be difficult or burdensome to establish a separate communication channel for delivery of the symmetric key to the user computer.

In the context of Peinado architecture, Peinado makes an express decision to use asymmetric encryption to encrypt/decrypt the decryption key (KD). This asymmetric decryption taught by Peinado avoids the need to communicate a symmetric key between license server (24) (i.e. the location of encryption of decryption key (KD)) and user computer (14) (i.e. the location of decryption of decryption key (KD)). Instead only the black box public key (PU-BB) is communicated from the user computer (14) to the license server (24) and the black box private key (PR-BB) is used for decryption at the user computer (14). If Peinado was modified to provide symmetric encryption for encrypting/decrypting decryption key (KD) as contended by the Examiner, then the Peinado system would be exposed to the risk that the symmetric key would be intercepted as the symmetric key was communicated between license server (24) and user computer (14). Such a security risk would defeat the entire purpose of the Peinado system – i.e. to provide an enforcement architecture that allows the controlled rendering or playing of digital content, where the digital content will only be rendered as specified by the content owner even

though the digital content is to be rendered on a device that is not under the control of the content owner (see col. 2, ln. 8-20).

Based on this reasoning, the Applicant submits that it would not be obvious to modify the Peinado system to incorporate the claim 1 feature of using a single “user key” to encrypt the decryption key at a remote server and to decrypt the decryption key at the user computing device.

Conclusions for claims 1-3, 17, 18, 20, 25, 27, 34-36, 38, 40-42, 48-50, 55 and 57

Based on the reasons expressed above, the Applicant contends that it would not be obvious to modify the Peinado digital rights management (DRM) architecture to provide media content file with an integral decryption engine or to incorporate the use of a single symmetric “user key” to encrypt the decryption key at a remote server and to decrypt the decryption key at the user computing device. Accordingly, the Applicant submits that claim 1 patentably distinguishes the combination of Peinado, Glover, Eberhard and En-Seung. Claims 2, 3, 17, 18, 20, 25, 27, 34-36, 38, 40-42, 48-50, 55 and 57 depend from claim 1 and are submitted to patentably distinguish the combination of Peinado, Glover, Eberhard and En-Seung for at least this reason.

Claims 4, 11, 21, 28, 31, 33, 43, 44, 52-54, 56 and 58

The Examiner has raised the combination of Peinado, Glover, US6,564,248 (Budge et al., referred to herein as Budge), Eberhard and En-Seung in connection with claim 4. The Applicant submits that claim 4 and all of the claims that depend from claim 4 patentably distinguish the combination of Peinado, Glover, Budge, En-Seung and Eberhard.

Integral decryption engine

Following the Examiner' logic presented on pages 10-11 of the Office Action, the Examiner correctly acknowledges that Peinado does not disclose the following claim 4 features:

- the file comprising the encrypted media content received at the user computing device also comprises an integral decryption engine; and
- using the integral decryption engine together with the decryption key to decrypt the media content.

The Examiner expresses the view that these features missing from Peinado are disclosed by Glover and that it would be obvious to incorporate these features from Glover into the Peinado system. The rationale advanced by the Examiner for this contention of obviousness is the motivation “to provide the support for the specific form of corresponding decryption” as allegedly described in the Abstract of Glover.

As discussed above in relation to claim 1, Peinado teaches directly away from providing a single media content file with an integral decryption engine. Providing an integral decryption engine with the media content file would prevent Peinado from operating as disclosed to base its decryption component (black box (30)) on hardware associated with the user computing device (14) and to update its decryption component (black box (30)). For these same reasons, the Applicant submits that it would not be obvious to modify the Peinado digital rights management (DRM) architecture to provide a media content file with an integral decryption engine as recited in claim 4.

Decrypting decryption key using user key

On page 12 of the Office Action, the Examiner correctly acknowledges that Peinado, Glover, Budge and Eberhard do not disclose the claim 4 feature that the user computing device can make use of the “user key” to decrypt the decryption key. The “user key” is recited in claim 4 to be the same key that is used to encrypt the decryption key at the remote server.

The Examiner expresses the view that this feature missing from the combination of Peinado, Glover, Budge and Eberhard is disclosed by En-Seung and that it would be obvious to incorporate this features from En-Seung into the Peinado system as modified by Glover, Budge and Eberhard. The rationale advanced by the Examiner for this contention of obviousness is the motivation “to prevent an individual from making a useful copy of the information” as allegedly described at col. 2, ln. 20-23 of Glover.

The Applicant has amended claim 4 to explicitly recite that the user key is actually used at the user computing device to decrypt the decryption key. More specifically, claim 4 has been amended to recite “use the user key to decrypt the decryption key at the user computing device”. Claim 4 also recites that the “user key” is used at the remote server to encrypt the decryption key.

For the same reasons discussed above in relation to claim 1, the Applicant submits that Peinado teaches directly away from this claim 4 feature by using an asymmetrical encryption system and it would therefore not be obvious to modify the Peinado system to incorporate the use of a single symmetric “user key” to encrypt the decryption key at a remote server and to decrypt the decryption key at the user computing device as recited in claim 4.

Conclusions for claims 4, 11, 21, 28, 31, 33, 43, 44, 52-54, 56 and 58

Based on the reasons expressed above, the Applicant contends that it would not be obvious to modify the Peinado digital rights management (DRM) architecture to provide a media content file with an integral decryption engine or to incorporate the use of a single symmetric “user key” to encrypt the decryption key at a remote server and to decrypt the decryption key at the user computing device. Accordingly, the Applicant submits that claim 4 patentably distinguishes the combination of Peinado, Glover, Budge, Eberhard and En-Seung. Claims 11, 21, 28, 31, 33, 43, 44, 52-54, 56 and 58 depend from claim 4 and are submitted to patentably distinguish the combination of Peinado, Glover, Budge, Eberhard and En-Seung for at least this reason.

Claim 46

The Examiner has raised the combination of Peinado, Glover, Eberhard and En-Seung in connection with claim 46. The Applicant submits that claim 46 patentably distinguishes the combination of Peinado, Glover, En-Seung and Eberhard.

Integral decryption engine

Following the Examiner' logic presented on pages 2-3 of the Office Action, the Examiner correctly acknowledges that Peinado does not disclose the following claim 46 features:

- the file comprising the encrypted media content received at the user computing device also comprises an integral decryption engine; and
- using the integral decryption engine together with the decryption key to decrypt the media content.

The Examiner expresses the view that these features missing from Peinado are disclosed by Glover and that it would be obvious to incorporate these features from Glover into the Peinado system. The rationale advanced by the Examiner for this contention of obviousness is the

motivation “to provide the support for the specific form of corresponding decryption” as allegedly described in the Abstract of Glover.

As discussed above in relation to claim 1, Peinado teaches directly away from providing a single media content file with an integral decryption engine. Providing an integral decryption engine with the media content file would prevent Peinado from operating as disclosed to base its decryption component (black box (30)) on hardware associated with the user computing device (14) and to update its decryption component (black box (30)). For these same reasons, the Applicant submits that it would not be obvious to modify the Peinado digital rights management (DRM) architecture to provide a media content file with an integral decryption engine as recited in claim 46.

Decrypting decryption key using user key

On page 5 of the Office Action, the Examiner correctly acknowledges that Peinado, Glover and Eberhard do not disclose the claim 46 feature that the user computing device can make use of the “user key” to decrypt the decryption key. The “user key” is recited in claim 46 to be the same key that is used to encrypt the decryption key at the remote server.

The Examiner expresses the view that this feature missing from the combination of Peinado, Glover and Eberhard is disclosed by En-Seung and that it would be obvious to incorporate this features from En-Seung into the Peinado system as modified by Glover and Eberhard. The rationale advanced by the Examiner for this contention of obviousness is the motivation “to prevent an individual from making a useful copy of the information” as allegedly described at col. 2, ln. 20-23 of Glover.

Claim 46 explicitly recites “using the user key to decrypt the decryption key and to thereby obtain a decrypted decryption key at the user computing device”. Claim 46 also recites that the “user key” is used at the remote server to encrypt the decryption key.

For the same reasons discussed above in relation to claim 1, the Applicant submits that Peinado teaches directly away from this claim 46 feature by using an asymmetrical encryption system and it would therefore not be obvious to modify the Peinado system to incorporate the use of a single

symmetric “user key” to encrypt the decryption key at a remote server and to decrypt the decryption key at the user computing device as recited in claim 46.

Conclusions for claim 46

Based on the reasons expressed above, the Applicant contends that it would not be obvious to modify the Peinado digital rights management (DRM) architecture to provide media content file with an integral decryption engine or to incorporate the use of a single symmetric “user key” to encrypt the decryption key at a remote server and to decrypt the decryption key at the user computing device. Accordingly, the Applicant submits that claim 46 patentably distinguishes the combination of Peinado, Glover, Eberhard and En-Seung.

Additional Comments – Claims 25 and 41

Claims 25 and 41 recite downloading the file containing the media content from a remote computer “using a peer to peer network”. The Examiner expresses the view that this feature is obvious in view of a combination of Peinado, Glover, Eberhard and En-Seung. More particularly, the Examiner contends that this peer to peer aspect of the Applicant's invention is disclosed by Peinado by elements 14, 22 and 24 of Figure 1 and by Eberhard at Figure 1 and paragraph [0012] – see pages 6 and 7 of the Office Action.

The Applicant submits that none of these references alone or in combination, describe the notion of sharing media content between users on a peer to peer network. In particular, the Figures and passages cited by the Examiner do not disclose or suggest this feature. Figure 1 of Peinado clearly describes a package (12p) containing media content that comes from a central content server (22) and not from a peer to peer network. Figure 1 of Eberhard clearly shows (and paragraph [0012] of Eberhard clearly describes) how media content arrives at the user's PC (110) via a publisher server (100) and not from a peer to peer network.

Accordingly, the Applicant submits that the combination of references cited by the Examiner fail to teach or suggest downloading the file containing the media content from a remote computer “using a peer to peer network” as recited in claims 25 and 41.

Further, as discussed above, the Applicant's claimed solution provides an “integral decryption engine” together with the media content. In the Peinado architecture, the decryption component (black box (30)) is separately downloaded from a black box server (26). The Applicant's system permits the decryption engine to be transferred between users over a peer to peer network together with the media content. In contrast, Peinado expressly teaches that black box (30) is “tightly tied to or associated with the user's computing device (14)” to prevent transfer of the decryption engine (black box (30)) between users. Moreover, Peinado teaches specific methods for preventing the transfer of the decryption engine (black box (30)) between users (e.g. over a peer to peer network) – see col. 22, ln. 63-col. 23, ln. 14.

Accordingly, Peinado teaches away from sharing between users in a peer to peer environment and the Applicant submits that it would not be obvious to modify Peinado to provide this feature.

Based on this reasoning, the Applicant submits that claims 25 and 41 further patentably distinguish the prior art of record.

Additional Comments – Claims 48 and 52

Claims 48 and 52 recite that after a file (containing media content and an integral decryption engine) is downloaded to a first user, the same file is subsequently sent directly from the first user computer to a second user computer, where it is decrypted using a similar process to that of the first user computer. The Examiner expresses the view that this feature is obvious in view of a combination of Peinado, Glover, Eberhard, En-Seung (in the case of claim 48) and in further view of Budge (in the case of claim 52).

The Applicant submits that none of these references alone or in combination, describe the notion of sharing media content directly between user computers. In particular, the Figures and passages cited by the Examiner on pages 8 and 14-15 of the Office Action do not disclose or suggest this feature. All of the references cited by the Examiner involve obtaining media content from a central server. Accordingly, the Applicant submits that the combination of references cited by the Examiner fails to teach or suggest sharing media content directly between user computers as recited in claims 48 and 52.

Further, as discussed above, the Applicant's claimed solution provides an “integral decryption engine” together with the media content. In the Peinado architecture, the decryption component (black box (30)) is separately downloaded from a black box server (26). The Applicant's system permits the decryption engine to be transferred directly between users (e.g. over a peer to peer network) together with the media content. In contrast, Peinado expressly teaches that black box (30) is “tightly tied to or associated with the user's computing device (14)” to prevent transfer of the decryption engine (black box (30)) between users. Moreover, Peinado teaches specific methods for preventing the transfer of the decryption engine (black box (30)) between users (e.g. over a peer to peer network) – see col. 22, ln. 63-col. 23, ln. 14. Accordingly, Peinado teaches away from direct sharing of a file containing an integral decryption engine between users and the Applicant submits that it would not be obvious to modify Peinado to provide this feature.

Based on this reasoning, the Applicant submits that claims 48 and 52 further patentably distinguish the prior art of record.

Affidavit Under 37 CFR § 1.132

The Applicant encloses herewith an Affidavit sworn by one of the inventors, Steve Vestergaard, pursuant to 37 CFR §1.132. The Affidavit includes evidence of: (i) the long felt need in the media industry for secure methods for distribution of digital media content; (ii) the unsatisfactory efforts of others to address this need; and (iii) the commercial success of the Destiny Group, the assignee of the technology claimed in this application.

The Applicant submits that the enclosed Affidavit provides further evidence of the non-obviousness of the currently pending claims.

Conclusions

In view of the foregoing amendments and arguments and the enclosed Affidavit, the Applicant respectfully submits that this application is now in condition for allowance and requests reconsideration and allowance of this application.

Respectfully submitted,

Application No. 09/980582
Amendment dated 25 August 2008
Reply to Office Action of 27 March 2008

Page 26 of 26

OYEN WIGGS GREEN & MUTALA

By:

Richard A. Johnson
Registration No. 56,080
Vancouver, Canada
tel: 604.669.3432
fax: 604.681.4081
e-mail: TARDocket@patentable.com