(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 June 2008 (19.06.2008)

PCT

(10) International Publication Number
WO 2008/072022 A2

(51) International Patent Classification:
*G06Q 30/00* (2006.01)

(21) International Application Number:
PCT/IB2006/003556

(22) International Filing Date:
12 December 2006 (12.12.2006)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant and
(72) Inventor: **KING, Timothy** [ZA/ZA]; 4 The Point, Glengariff Road, Sean Point (ZA).

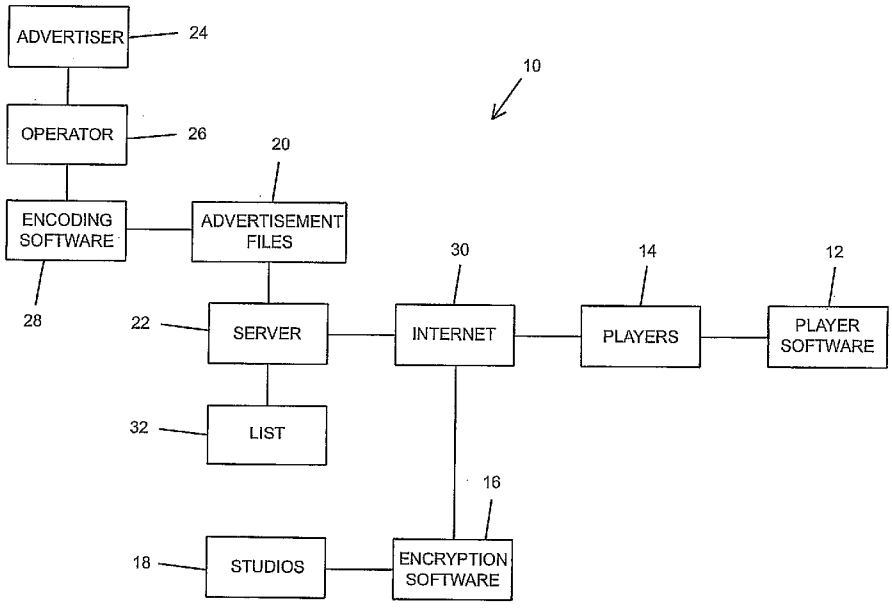
(74) Agent: **TRUTER, Kenneth, Colin**; Brian Bacon & Associates Inc., 2nd Floor Mariendahl House, Newlands on Main, Main Road, Newsland, 7700 Western Cape (ZA).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, 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, LV, LY, MA, MD, 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.

(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, HU, IE, IS, IT, LT, LU, LV, MC, NL, 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:**
— *without international search report and to be republished upon receipt of that report*

(54) **Title:** DIGITAL RIGHTS MANAGEMENT SYSTEM




(57) **Abstract:** A method of managing digital media and an associated method of doing business are provided, along with encryption (16) and player software (12) for the method. The method comprises encrypting the digital media, making the encrypted media available to be copied without limitation and allowing users to playing the encrypted media on players (14), loaded with the player software (12) that is distributed free of charge, but the players (12,14) retrieve advertisement media from a server (22) and plays the advertisement media along with the encrypted media. Revenue is generated from advertisers (24) and part of the revenue is used to pay media rights owners (18) for the digital media.

WO 2008/072022 A2

# DIGITAL RIGHTS MANAGEMENT SYSTEM

## FIELD OF THE INVENTION

This invention relates to digital rights management (DRM) to allow the distribution and playing of digital media and generation of income from the media.

## BACKGROUND TO THE INVENTION

Digital media such as sound recordings and feature films are freely available in digital format, e.g. as downloads via the internet and can be readily copied without the permission of persons who may own rights subsisting in the media, such as copyright or contractual rights, referred to in this specification as "media owners". The result is that unlawful or so-called "pirate" copies of these media are frequently made and distributed, thus satisfying the demands of potential purchasers of lawfully obtained copies and depriving the media owners of their profits from sales of lawful copies of the media.

Due to the high risk of copying, some media owners such as film and music recording studios have been reluctant to distribute their media via decentralised peer-to-peer methods on the internet, which severely limits the volumes of media copies from which such media owners can profit.

Other media owners choose to distribute their media via centralised servers on the internet, but employ DRM systems to restrict the usage of such media.

One example of such a DRM system allows users to purchase media in the form of music files online, to make an unlimited number of copies and transfer the music files to an unlimited number of media players that are specific to the media owner. The purchased music files are encoded in a format that can only be played on the specific media players that are also sold or licensed by the media owner. The media owner further reserves the right to alter its DRM restrictions on the music files a user has purchased, at any time, for example to restrict the number of times a user is allowed to copy a playlist of music files, to limit the number of players on which music files can be played at a time, to prevent users from editing or sampling the music files they purchased, etc. Despite these restrictions, this DRM system is often seen as lenient and can be easily bypassed by using freely available computer programs and/or can be stored on digital storage devices such as compact discs without restrictions on further copying, by using software provided by the media owner.

In another example of such a DRM system, a subscription based approach is used alongside permanent purchases. Users of a subscription service of the media owner can purchase an unlimited amount of encoded music online while subscribed to the service, but as soon as the user's subscription is defective, e.g. if a payment is missed, the service renders all

the downloaded music unplayable. The service also charges users an additional subscription if they wish to play the music on portable devices and requires users to pay an additional amount per music file copied to a digital storage device or to play the music file after the subscription has expired. Music files bought through the service can only be played on certain players, excluding players supplied by the media owner mentioned in the previous example, above.

Some academic institutions make arrangements with media owners selling music online, to provide access (typically DRM protected) to music files for their students, typically by paying subscriptions to the media owners. However, such DRM systems are typically configured so that the music files become unplayable when the students leave the academic institution, unless the student continues to pay subscriptions to the media owner, individually.

Almost all media owners who presently sell media online require client software of some sort to be downloaded and some also need plug-ins. They also require media to be provided from an owned or owner supported centralised server that is often country-specific.

Many of the various DRM systems that are currently in use are not interoperable, with the result that media purchased from one media owner may be unplayable on a player that is configured to be compatible with media supplied by another media owner.

The various DRM systems that are presently in use thus typically require payment before media are supplied to vendors and place restrictions on the use and copying of the media. It is thus tempting for users to opt for purchasing pirate copies of media, typically at lower cost and usually without the cumbersome restrictions imposed by lawful media owners.

The object of the present invention is to provide a DRM system that allows media owners to generate income from the media they own, without restricting copying of the media.

## BRIEF DESCRIPTION OF THE INVENTION

According to a first aspect of the present invention, there is provided a method of managing digital media, said method comprising:

encrypting the digital media;

making the encrypted media available to be copied without limitation; and

playing the encrypted media on a player;

wherein the player retrieves advertisement media from a server and plays the advertisement media along with the encrypted media.

The player may play the advertisement media at timed intervals, may stop playing the encrypted media while playing the advertisement media and may verify the status of the encrypted media before the media is played on the player.

A unique key may be assigned to the media when it is encrypted and the status of the encrypted media may be verified by comparing the key of the media with a list of valid media keys. The status of the encrypted media may be verified via the internet.

The key may comprise unique coding associated with software used during encryption and unique coding associated with the media and the key may be embedded in the encrypted media.

The encrypted media may include embedded codes and the advertising media may be played when such an embedded code is encountered in the player.

A unique key may be assigned to each media player and the key may be recorded by the server when the advertisement media is retrieved from the server. Further, the advertisement media that is retrieved from the server may be selected on the basis of the player's key and the unique key of the media being played on the player, may recorded by the server.

According to another aspect of the present invention, there is provided a method of managing digital media, said method comprising:

encrypting the digital media;

making the encrypted media available to be copied without limitation; and

playing the encrypted media on a player;

wherein the encrypted media include coding and only selected players include enabling coding, the player accessing the server according to the method of claim 1, and the server verifying the coding of the media and verifying the enabling coding of the player and permitting the player to play the media.

The present invention extends to encryption software configured to encrypt digital media and to player software configured to play digital media as set out herein above.

According to a further aspect of the present invention, there is provided a method of doing business, said method comprising:

receiving advertisement media from advertisers;

storing the advertisement media on a server; and

making the advertisement media available to be retrieved from the server and played along with the encrypted media as described herein above;

wherein the advertisers pay for the advertisement media to be played and at least part of said payment is applied to pay for the digital media.

The advertisement media may be intended to be played on targeted players, e.g. players in a predetermined geographical area.

The amounts paid by advertisers may be determined according to the popularity of the media along with which the advertisement media is

played and in a preferred embodiment of the invention, the amounts may be determined by extent of feedback between the advertisement media and the server.

The method may include making encryption software available against payment, for encrypting the digital media to be played along with the advertisement media, e.g. the encryption software may be sold or may be rented out or a service of encryption using the encryption software, may be provided against payment.

## BRIEF DESCRIPTION OF THE DRAWING

For a better understanding of the present invention and to show how the same may be carried into effect, reference will now be made, by way of non-limiting example, to the accompanying drawing which shows a schematic representation of a digital rights management system DRM in accordance with the present invention.

## DETAIL DESCRIPTION OF THE DRAWINGS

Referring to the drawing, a digital rights management (DRM) system in accordance with the present invention is generally indicated by reference numeral 10. The system 10 is configured to for the management of rights subsisting in digital media in the form of feature films or video recordings, by way of example, but those skilled in the art would appreciate that the system can be configured equally effectively for other forms of digital

media, such as music recordings. The word "film" is used to refer to digitised copies of feature films.

The system 10 includes player software 12 that is made available for free download on the internet and that is stored on a video player hardware 14 (which could be part of a computer), encryption software 16 that is used by media owners who in the illustrated example are film recording studios 18 and a set of codes in the form of break codes and/or override or VIP codes, that are embedded in encrypted media files in the form of digital films and that trigger the player 12,14 to download advertisement media files 20 from a server 22 via the internet 30.

Commercial DVD-quality films are encrypted by the studios 18 or other lawful owners of rights in the films, using the encryption software 16, to a special format including the break codes and/or VIP codes (see below). The films in this special encrypted format are made available for free download from any standard internet point, such as via peer-to-peer file sharing networks or from the film studios' own websites. The encrypted films could also be made available on DVDs that can be freely copied by the public. The break codes and/or VIP codes are embedded in the encrypted films at predetermined interval, e.g. every 15 minutes and the codes are configured to cause the video player 14 on which the film is being played, to do the following:

pause the film and blank the player window in which the film was being played;

disable the fast forward, rewind, play and quit controls of the player 12,14, while the pause control is left active;

play high quality full motion advertisements in the player window.

resume playing the film at the end of the advertisement; and

re-enable the player controls.

The advertisements are preferably actual television commercials that have been digitised to be played on the players 12,14, as opposed to simply creating standard web adverts. In addition, the software nature of the player software 12 allows click-able overlays to be created for these advertisements, for interactivity and online purchases.

The fast forward, rewind, play and quit controls of the player 12,14 are disabled and are re-enabled in order to allow users to stop playing a film and to continue again by fast forwarding to a desired place in the film, e.g. the place where the user stopped, or to rewind to a place in the film the user may want to re-play. However, the user will not be able to pause, or fast forward through the advertisements. If a user attempts this, the player 12,14 will immediately stop at the first break code it encounters and begin playing advertisements.

The advertisement files 20 are provided by advertisers 24 to an operator 26 of the system 10, who uses encoding software 28 to encode the advertisement files and saves them to the server 22. The operator 26 collects payment from the advertisers 24 in exchange for the exposure their

advertisements get on the players 12,14 and part of the payment is paid to the studios 18 as payment for the films they make available. The advertising thus generates payment for all the contributing parties involved, so that the films can be made available to the users free of charge.

These advertisements are encoded by the operator 26 to be specific to predetermined geographic target regions and the advertisement files are automatically downloaded by the players 12,14 via the internet 30 from a series of central servers 22 while the film is playing on the player and they are buffered, ready to play when a break code is encountered in the film file being played.

The film files do not contain any built-in advertisements, but only the break codes necessary to retrieve the advertisement files 20 that are specific to the users' region. This is in contrast to existing adware products that rely on a player downloading a fixed set of (typically web/html based) advertisements from a server, rather than requesting high quality television advertisement files 20 that are specific to the user's geographic location, or even, in a preferred embodiment described below, advertisement files that are selected to target users based on the films they play.

When the player software 12 is installed, a security code or key is generated in the same way as the ones generated when commercially available software packages are activated. The key generated is unique and is associated with the particular player software 12 and the player hardware

14 on which it has been installed and to which it is paired. The key is also used to create a unique account code automatically on the server 22 through a process of product activation of the player software 12.

The key contains no information that could be used to identify a user, player hardware 14 or system information, but does include an indication of the country in which the player hardware 14 is located so that the correct advertisement files 20 are loaded to the player and the key creates an account on the server that maintains a list of the films that have been played on the player, the frequency with which films are played on the player, as well as which advertisements have been played on the player and the frequency of the advertisements.

If the underlying system, i.e. the player hardware 14, associated with the player software 12 changes, a new key is generated. In this way, the account on the advert server is "keyed" to a specific software/hardware combination.

The reason why the unique keys are generated for each player is to allow for statistics to be compiled of which films are most popular in which countries. This information can be used by the operator 26 on the server 22 to create a sliding-scale price structure for the sale of advertising, based on popularity of the films during which the advertisements will be showed – advertisements shown during more popular or most watched films commanding higher rates because they will have higher exposure. Initially,

when a film is first released and has no popularity track record, a base advertising rate is charged for advertisements shown during playing of such films.

The system 10 monitors the frequency with which advertisements 20 are being downloaded, to keep a record for the benefit of the advertisers 24 and to be used as groundwork statistics for future advertisement sales.

The advertisements can contain clickable hyperlinks to advertised websites, possibly even with hotspots.

When the encryption software 16 is installed, it creates a unique key that is based on the serial number of the software and an activation code that is automatically generated when the software is registered. This key is also based on the hardware on which the encryption software 16 is installed, possibly with an additional "user-generated" key as a further indication of the origin of an individual film encrypted on the installed software.

When a film is encrypted with the software 16, the break codes are tagged with the unique key of the encryption software, along with an additional key that is assigned to the encrypted film. This double-key is uploaded to the central servers 22 when the encrypted film is registered on the server and is saved on a list 32.

The player software 12 is configured to allow the player 14 only to play films that have keys that match the keys on list 32. The result is that if the encryption software 16 is copied unlawfully and is used to encrypt films in a custom, non-studio sanctioned manner, e.g. without break codes, the encrypted film will not have the requisite double key saved on the list 32 and the player software will prevent the player 12,14 from playing the film.

It is to be noted that anyone can copy a film that has already been encrypted and they can do so quite lawfully. This is because the film already contains all the break codes and unique encryption program and film keys.

This also means that if a studio 18 would like to release a new version of a film, they can quickly and easily disable an existing film (no matter how many copies are in circulation) by issuing a simple instruction to the server 22 to remove the existing key code for this particular film from its list 32, so that no player 14 will play the film. Instead a message will be displayed on the player 14 such as "This film has been deactivated by the studio. Please download a new copy", or "This film does not have a correct encryption key. Please delete it and download a new copy HERE" (with a hyperlink to the new, properly encrypted and lawful version).

The encryption software 16 also allows a film to be encrypted with a special set of codes, referred to in this specification as "VIP codes", throughout the film, instead of break codes. These VIP codes are useful when

a studio 18 wants to create a special release version of a film for a select audience such as Academy Awards pre-screenings.

The player application software 12 is installed on the player hardware 14 of a user qualifying for VIP status. As always, a unique key is generated for this player software 12. The VIP takes note of his unique key and sends it to the encrypting film studio 18 or awards body. This key is then added to a list on the computer or encrypter on which the encryption software 16 is installed. When ready to encrypt the film, the studio selects VIP-mode on the encrypter and adds the list of unique keys of the VIP's players to the encrypter. The encrypter then creates a set of VIP codes that will only allow the particular film to be played in a player 12,14 whose key matches that of one of those on the VIP key list. In this way, it doesn't matter if the film is copied without permission or "leaked", since it can only be played on one of the players 12,14 of the VIPs selected by the studio 18. The present invention thus holds the advantage that no special player software is needed for VIP screenings of films (without advertisements) and there is no need to protect the actual film files, as all the protection is done in the encryption.

The player software 12 can be downloaded and installed on a computer or other suitable hardware 14 that can play digital film files, but in one embodiment of the present invention, the software 12 can be incorporated into the internal hardware of a specialized media player unit 14. This hardware player unit 14 is a set-top box that will offer internet connectivity so that films can be downloaded, a hard drive so that they can be stored and integrated

player software 12 so that the films can be played. Such a player unit 14 can have all the usual connections that a DVD player would typically have, e.g. fibre-optic, SVGA, multi-channel surround sound out, etc.

Such a player unit 14 is not the same as a Digital Video Recorder (DVR) service or device. Those services still rely on a central broadcaster and only offer the ability to record or pause live programming content. By contrast, the player unit 14 offers the ability to download and keep indefinitely, encrypted commercial films for free, while maintaining the rights of the copyright holders or studios 18 and generating income for the studios.

Some of the advantages of the present invention have been described above, but in particular, the invention holds the advantages that it allows the public to watch films for free and to keep the free film files to play them at their leisure. The film industry (studios 18) generates income on these films through the sale of advertising and as the uptake of the system 10 increases, the production and distribution costs for providing encrypted films is expected to reduce. The system 10 is complimentary to existing theatre sales and DVD sales. The advertisements that are displayed to the users can be up to date, can be targeted at certain groupings of users and can be appropriately priced in relation to the popularity of the films during which they are shown.

It is expected that the distribution of pirated films will decrease with the implementation of the system 10 as the public is offered a lawful way of getting free films to keep on their computers from any of their usual distribution points, not to mention being able to copy these films lawfully, e.g. by writing them to DVDs and sharing them with others or making them available via peer-to-peer networks.

The function of the operator 26 is to run the advertising content server 22 and sell the advertising that will be embedded in the films, in exchange for a percentage of the revenue generated through advertising sales – the rest of the revenue going to the film studios 18. In addition to this, the operator 26 encodes the films for a per-film charge or alternatively provides the encryption software 16 to the film studios 18 for rental or for a fixed-price lump sum purchase. It is envisaged that larger studios 18 may want to purchase the encryption software 16, while smaller studios may prefer either to rent it or to pay a once-off fee to get their films encoded and sent out to the major distribution points.

Further, in the drawing, only one advertiser 24, one operator 26, one server 22, one studio 18 and one player 14 are shown. However, those skilled in the art will appreciate that the system 10 can include one, but will typically include many of each of these features.

CLAIMS

1. A method of managing digital media, said method comprising:

encrypting the digital media;

making the encrypted media available to be copied without limitation; and

playing the encrypted media on a player;

wherein the player retrieves advertisement media from a server and plays the advertisement media along with the encrypted media.

2. A method as claimed in claim 1, wherein the player plays the advertisement media at timed intervals.

3. A method as claimed in claim 2, wherein the player stops playing the encrypted media while playing the advertisement media.

4. A method as claimed in claim1, wherein the player verifies the status of the encrypted media before the media is played on the player.

5. A method as claimed in claim 4, wherein a unique key is assigned to the media when it is encrypted and wherein the status of the encrypted media is verified by comparing said key of the media with a list of valid media keys.

6. A method as claimed in claim 4, wherein the status of the encrypted media is verified via the internet.

7. A method as claimed in claim 5, wherein the key comprises unique coding associated with software used during encryption and unique coding associated with the media.

8. A method as claimed in claim 5, wherein said key is embedded in the encrypted media.

9. A method as claimed in claim 2, wherein the encrypted media includes embedded codes and the advertising media is played when such an embedded code is encountered in the player.

10. A method as claimed in claim 1, wherein a unique key is assigned to each media player and the key is recorded by the server when the advertisement media is retrieved from the server.

11. A method as claimed in claim 10, wherein the advertisement media that is retrieved from the server is selected on the basis of the player's key.

12. A method as claimed in claim 10, wherein a unique key is assigned to the media when it is encrypted and the key of the media being played on the player, is recorded by the server.

13. A method of managing digital media, said method comprising:

encrypting the digital media;

making the encrypted media available to be copied without limitation; and

playing the encrypted media on a player;

wherein the encrypted media include coding and only selected players include enabling coding, the player accessing the server according to the method of claim 1, and the server verifying the coding of the media and verifying the enabling coding of the player and permitting the player to play the media.

14. Encryption software configured to encrypt digital media according to claim 1.

15. Player software configured to play digital media according to claim 1.

16. A method of doing business, said method comprising:

receiving advertisement media from advertisers;

storing the advertisement media on a server; and

making the advertisement media available to be retrieved from the server and played along with the encrypted media according to claim 1;

wherein the advertisers pay for the advertisement media to be played and at least part of said payment is applied to pay for the digital media.

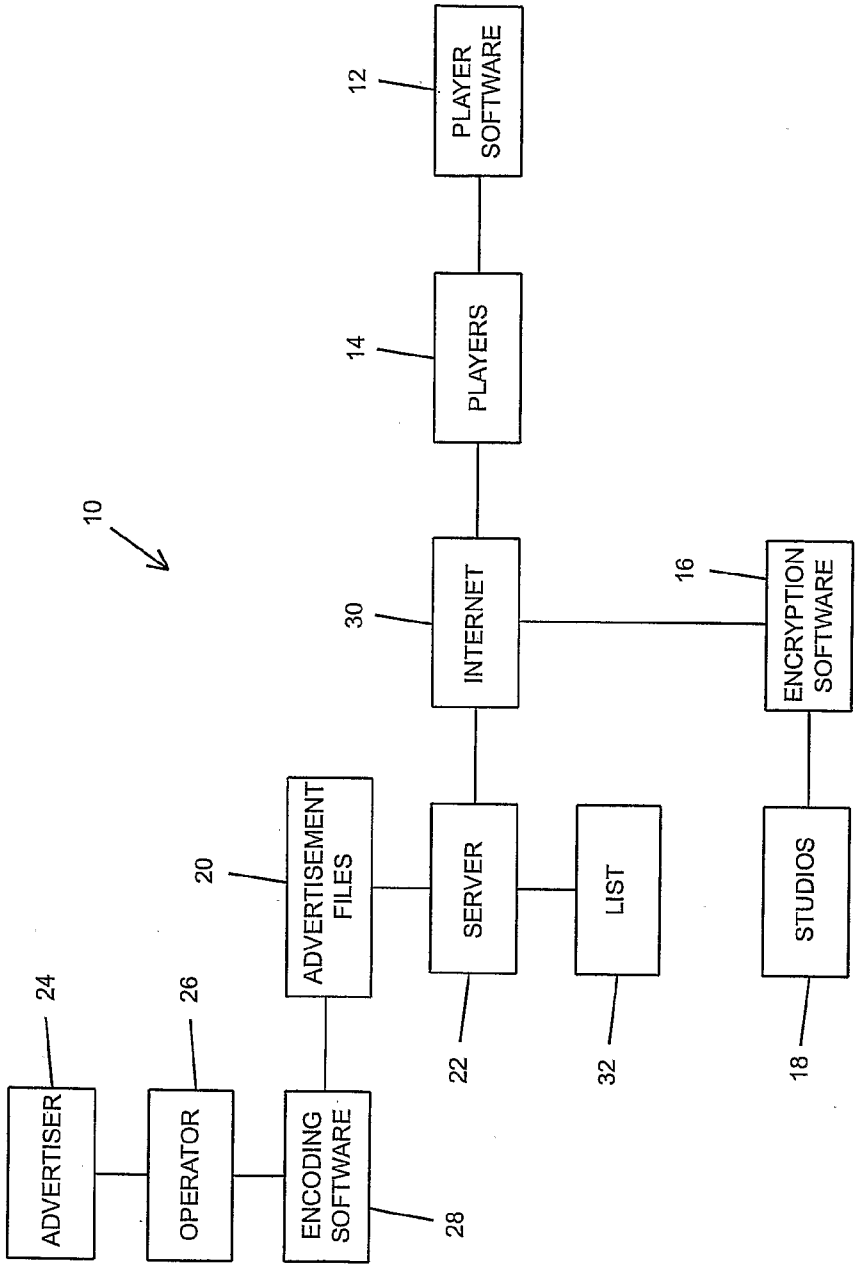
17. A method as claimed in claim 16, wherein the amounts paid by advertisers are determined according to the popularity of the media along with which the advertisement media is played.

18. A method as claimed in claim 16, which includes making encryption software available against payment, for encrypting the digital media to be played along with the advertisement media.

19. A method as claimed in claim 18, wherein the encryption software is sold.

20. A method as claimed in claim 18, wherein the encryption software is rented out.

21. A method as claimed in claim 18, wherein a service of encryption using the encryption software, is provided against payment.


10
12
PLAYER SOFTWARE
14
PLAYERS
30
INTERNET
16
ENCRYPTION SOFTWARE
20
ADVERTISEMENT FILES
SERVER
LIST
STUDIOS
22
32
18
24
26
ADVERTISER
OPERATOR
ENCODING SOFTWARE
28