(19) World Intellectual Property Organization

(43) International Publication Date
25 July 2013 (25.07.2013)

(51) International Patent Classification:
H04N 21/20 (201.01)

(21) International Application Number:
PCT/EP2013/050569

(22) International Filing Date:
14 January 2013 (14.01.2013)

(25) Filing Language:
English

(26) Publication Language:
English

(30) Priority Data:
12305073.4 20 January 2012 (20.01.2012) EP
12165599.7 26 April 2012 (26.04.2012) EP

(71) Applicant: THOMSON LICENSING [FR/F]; 1-5 rue Jeanne d’Arc, F-92130 Issy-les-Moulineaux (FR).

(72) Inventor: DIEHL, Eric; c/o Technicolor, 975, avenue des Champs Blancs, ZAC des Champs Blancs, CS 176 16, F-35576 Cesson Sevigne (FR).


(54) Title: IN-FLIGHT ENTERTAINMENT SYSTEM

(40) to the user player device (170). Also provided is a content rendering method.

(57) Abstract: A content delivery system (100) comprising a content database (150) storing a content item (10) and a content license (20); a video server (140) configured to retrieve the content item (10) and the content license (20) from the content database (150) and to send them to a player device (170, 180); a registration server (120) configured to receive credentials from a user player device (170), to generate user information from the credentials, to forward the user information to an application server (110); an application server (110) configured to generate a personalized player application (30) for the user player device (170); and a license server (130) configured to receive a content license (20) and a user identity from the user player device, to check with the registration server (120) that a user corresponding to the user identity is authorized to access the content item (10), to decrypt the content license (20) using a system license key and re-encrypt the decrypted content license (20) using a user license key to obtain a user license (40), and to send the user license (40) to the user player device (170). Also provided is a content rendering method.

Figure 1
Declarations under Rule 4.17:
— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(H))

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 (Rule 48.2(g))
TECHNICAL FIELD

The present invention relates to protection of digital content and finds particular use in In-Flight Entertainment (IFE) systems.

BACKGROUND

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

In current IFE systems, a server on the airplane provides a plurality of different films to a plurality of users. Usually, each user is able to watch a film independently of all the other users. To achieve this, the user requests a desired content that then is streamed by the server.

Current IFE systems have two main characteristics:

- Content in the system is unprotected except for the intermittent addition of a visible, often semi-transparent, watermark that identifies the airline company. This can prove insufficient to deter theft, in particular in view of the hospitality release window, i.e., airlines receive films close to their theatrical release dates.

- The system only renders content on screens associated with the seats in the airplane, e.g., inserted in the back of the seat just in front or in the armrest of the seat.

It is assumed that the development goes towards providing High Definition (HD) content, which makes the IFE systems good targets for piracy.
attempts, and towards the ability for passengers to stream the content to their own devices, such as for example tablets and computers.

Current IFE systems are not suited for these developments and it will thus be appreciated that there is a need for a solution that provides an improved IFE system. The present application provides such a solution.

SUMMARY OF INVENTION

In a first aspect, the invention is directed to a method of rendering a content item. A device having a processor executes a player and renders the content item. At at least one point of time during execution of the method, the device verifies the presence of a proximity server; and stops the rendering of the content item in case the proximity server is not present.

In a first preferred embodiment, the device has a user identity and the player has been personalised to comprise the user identity and a user license key for the device. The device sends a content license for the content item and the user identity to a license server; obtains a user license for the content item from the license server; decrypts the user license using the user license key to obtain a scrambling key and descrambles the content item using the scrambling key.

It is advantageous that the device further watermarks the content between descrambling and rendering, the watermark in particular being a user watermark identity.

It is also advantageous that the device sends user credentials to a registration server and receives the player.

It is also advantageous that the device obtains the content item and the content license.

It is also advantageous that the user license has been generated from the content license.
In a second aspect, the invention is directed to a content delivery system comprising a content database configured to store at least one content item and a corresponding content license; a video server configured to retrieve a content item and a corresponding content license from the content database and to send the retrieved content item and corresponding content license to a player device; an application server configured to receive user information from the registration server, to generate a personalised player application for the user player device and to deliver the personalised player application to the user player device; a license server configured to receive a content license and a user identity from the user player device, to check with the registration server that a user corresponding to the user identity is authorized to access the content item, to decrypt the content license using a system license key and re-encrypt the decrypted content license using a user license key to obtain a user license, and to send the user license to the user player device; and a proximity server configured to participate in a challenge-response protocol with the user player device.

In a first preferred embodiment, the content delivery system further comprises a registration server configured to receive credentials from a user player device, to generate the user information from the credentials, to forward the user information to an application server.

In a second preferred embodiment the content delivery system further comprises a system player device comprising the system license key, the system player device being configured to receive the content item and the corresponding content license, to decrypt the content license using the system license key to obtain a scrambling key, to descramble the content item using the scrambling key, and to render the descrambled content item.

In a third preferred embodiment, the system player device is further configured to embed a watermark in the descrambled content item before rendering.
BRIEF DESCRIPTION OF DRAWINGS

Preferred features of the present invention will now be described, by way of non-limiting example, with reference to the accompanying drawings, in which

Figure 1 illustrates an In-Flight Entertainment system according to a preferred embodiment of the present invention;
Figure 2 illustrates a method for accessing content by a fixed player according to a preferred embodiment of the present invention; and
Figure 3 illustrates a method for accessing content by a mobile player according to a preferred embodiment of the present invention.

DESCRIPTION OF EMBODIMENTS

Figure 1 illustrates an In-Flight Entertainment system (IFE) according to a preferred embodiment of the present invention. The IFE is advantageously implemented onboard a vehicle, in particular an airplane that will be used as a non-limitative example hereinafter.

The IFE 100 comprises a head-end 105 and at least one player. The player may be a fixed player 180 that is managed by the system and, usually, fixed to the airplane; an example is a screen attached to the back of the seat of the row in front. The player may also be a mobile player 170, e.g. a tablet or a computer, that is not managed by the IFE, but by a user. This is to say that the IFE head-end 105 controls the software and so on of the fixed player 180, but not of the mobile player 170. It is assumed that the mobile player 170 is capable of downloading and executing software applications.

The IFE head-end 105 preferably comprises:

- A video content database 150 configured to store content and licenses for the content.
- A video server 140 configured to retrieve a content item 10 and the associated content license 20 from the video database 150 and to send the content license 20 to a player 170, 180 and also to stream the content 10 to the player.
• A license server 130.
• A registration server 120.
• An application server 110.
• A proximity server 160.

The skilled person will appreciate that the features are logical features that may be implemented as separate devices or grouped together in any possible manner.

Each device in the system comprises the necessary hardware and software needed for performing its functions, such as memory, at least one processor, at least one interface for interaction with other devices and a user interface.

The content 10 is preferably scrambled using at least one scrambling key that is held by the content license 20. The scrambling key may be unique for each content item 10, but it may also be common to more than one content item 10, possibly all the content items 10 in the video database 150. In case the scrambling key is the same for all the content items 10, then a single, generic content license is sufficient. Each content license 20 is encrypted using a license key (that preferably is the same for all the content licenses, but that may also be different).

It is preferred to send the same content 10 and content license 20 to a player, regardless of whether the player is a fixed player 180 or a mobile player 170.

It is further preferred that each fixed player 180 executes the same player software with (generally) the same parameters. The skilled person will appreciate that it is also possible for e.g. different groups of fixed players to execute different player software; an example is that players having different screen sizes or capabilities (such as 3D capability) execute different player software or at least use different parameters.
However, each mobile player 170 receives a specific personalised secure player 30 that has been generated by the application server 110. This secure player 30 preferably comprises:

- A dedicated secret used to receive user licenses 40.
- A unique payload to be used for insertion of forensics watermarks.
- A secret unique to the proximity server 160. During execution, the personalised secure player regularly checks the presence of this proximity server 160. If the proximity server 160 is not in the presence of the mobile player 170 (which may be checked using any suitable prior art protocols - there are many), the personalised secure player stops working.

Figure 2 illustrates a method for accessing content by a fixed player according to a preferred embodiment of the present invention.

First the fixed player 180 executes S21 an embedded software player that holds the license key common to all fixed players of the airplane (or at least to a group of fixed players). The fixed player 180 obtains S22 content 10 and a content license 20 from the video server 140. The fixed player 180 then attempts to decrypt S23 the content license 20 using the license key to obtain the scrambling key. It will be appreciated that the operation normally is successful. The fixed player 180 then uses the scrambling key to descramble S24 the scrambled content 10. Then an invisible (and possibly a visible watermark) is embedded S25 in the content 10. The skilled person will appreciate that the watermark can allow tracing of leaked content. The payload of the watermark may comprise features from the following non-exhaustive list: an identifier of the airline company, an identifier of the plane, an identifier of the flight, an identifier of the screen (i.e. the seat) and the current time. The watermarked content is then rendered S26.

It will be appreciated that in a variant embodiment, the content 10 in the video database 150 is watermarked with for example the identity of the plane.
In this case, there may be no need for the fixed player 180 to watermark the content.

The skilled person will note that this is a rather conventional method. The security assumption is that the "screen" (or "seat") is rather secure.

Figure 3 illustrates a method for accessing content by a mobile player according to a preferred embodiment of the present invention.

For a mobile player 170 to access content, it has first to obtain a personalised secure player 30 from the application server 110. For that purpose:

· The mobile player 170 executes a web browser and relays information 50 between a user and the registration server 120. The information 50 comprises credentials that will identify the user.

· The registration server 120 analyses the credentials and then decides whether the user is granted access to at least one of the services of the IFE head-end, notably access to the content 10 in the video database 150. It will be appreciated that how the decision is made is beyond the scope of the present invention. In case of a positive decision, i.e. if access is granted, then the registration server 120 registers the user.

· The registration server 120 preferably defines three parameters for the user:
  o a unique user identity,
  o a unique user license key, and
  o a unique user watermark identity.

· The registration server 120 forwards the parameters to the application server 110 that builds the personalised secure player 30 for the mobile player 170. The personalised secure player 30 is preferably obfuscated and securely embeds the user license key, the user watermark identity, and an address of the presence proxy 160.
• The mobile player 170 is then notified, preferably by the registration server 120 or the application server 110, that the personalised secure player 30 may be downloaded, but the personalised secure player 30 may also be pushed to the mobile player 170.

5 • The mobile player 170 then executes S31 the personalised secure player 30.

Once the mobile player 170 executes the personalised secure player 30, it may access content 10 by:

10 • Obtaining S32 content 10 and the content license 20 from the video server 140.

• Sending S33 the content license 20 and its own user identity to the license server 130.

• At this point, the license server 130 checks with the registration server 120 that a mobile device 170 associated with the user identity is granted access to content. If so, the license server 130 builds a user license 40 that comprises the scrambling key and that is encrypted so that only the personalised secure player corresponding to the user identity can decrypt it using the user license key. The user license 40 is then returned to and received S34 by the personalised secure player 30.

• Decrypting S35 the user license 40 using the user license key and retrieving the scrambling key.

• Descrambling S36 the content 10 using the retrieved scrambling key.

25 • Embedding S37 an invisible watermark (and possibly also a visible watermark) that can allow tracing of leakage of the content 10. The payload of the watermark is preferably at least the user watermark identity, but other data such as a combination of one or more of the features used for the ‘fixed player’ watermark described hereinbefore may be used in addition.

• Rendering S38 the watermarked content 10.
During the rendering of the content 10, the mobile player 170 regularly (or at irregular intervals) at least once verifies S39 the presence of the proximity server 160. In case the mobile player 170 does not obtain an accepted response (i.e. if the proximity server 160 is not 'present'), the mobile player stops rendering the content 10. The response may be unacceptable on account of it being wrong or because the distance to the proximity server 160 is too great. It will be appreciated that this verification may also be made at a point before the rendering begins.

Typically, the mobile player 170 and the proximity server 160 perform a challenge-response protocol - many such suitable protocols are well known in the art, such as for example limiting the number of 'hops' (see e.g. EP 1926250) or by limiting the round-trip time. It is also possible to require the two to be connected by one, non-relayed, radio (e.g. WiFi) connection. It can thus be ensured that the proximity server 160 is 'local' to the mobile player 170, i.e. that they are located on the same plane or in the same building. The proximity server 160 can also be configured to not respond during e.g. take-off and landing so as to help inhibit the use of electronic devices then.

In a preferred embodiment:

- Content 10 is scrambled using AES-128. Thus, the scrambling key is a (random) 128-bit number.
- The content license 20 and the user license 40 are protected by RSA-1024. To that end, each fixed player 180 has a common RSA-1024 public key $K_{pub\_plane}$. The content license 20 is encrypted using the corresponding common private key $K_{pri\_plane}$. In addition, the license server 130 also possesses the common RSA-1024 public key $K_{pub\_plane}$.
- When registering a user, the registration server 120 creates a 128-bit random number as the user identity and a unique RSA-1024 key pair $\{K_{pub\_tablet}, K_{pri\_tablet}\}$. 
The registration server 120 logs the transaction with the provided credentials, the user identity, the flight number, and the date. The log is kept by the airline company and used in case of litigation.

The proximity server 160 has a unique AES 128 bit key $K_{proxy}$.

The personalization of the personalized secure player 30 is made by:

- Embedding an obfuscated AES using a key $K_{tabiet}$. The player 30 expects to find at specific locations the four parameters (user identity, user license key (i.e. $K_{pub,tabiet}$), user watermark identity (preferably the user identity), and $K_{proxy}$) encrypted using $K_{tabiet}$.
- Encrypting the four parameters with $K_{tabiet}$ and storing them in the proper memory locations. Then it packages the final personalized secure player 30.

When the license server 130 receives the content license 20 and the user identity, it forwards the user identity to the registration server 120. If the corresponding user is already registered, the registration server 120 returns the corresponding $K_{pri,tabiet}$. The license server 130 decrypts the content license 20 using $K_{pub,plane}$ and generates the user license 40 by encrypting the decrypted content license 20 with $K_{pri,tabiet}$. The user license 40 is then sent to the mobile player 170.

The mobile player 170 decrypts the user license 40 with $K_{pri,tabiet}$ and descrambles the content 10 using the scrambling key.

Every minute, the personalized secure player generates a random number $R$, encrypts $R$ using $K_{proxy}$ and sends it to the proximity server 160. The proximity server 160 returns $R+1$ encrypted with $K_{proxy}$. The personalized secure player checks whether the returned value was incremented. After two successive failures, the personalized secure player stops the playback of the content 10.
The skilled person will appreciate that the system of the invention can offer the following advantages:

• end-to-end security for highly valuable content,
• high traceability of content in case of leakage, and
• use of a user's personal device as rendering unit.

It will thus be appreciated that the present invention provides an improved IFE system. It will be understood that the present invention is not limited to IFE, but that it may also be used e.g. in a museum where the solution may be modified so that the 'fixed players' are the museum's owned mobile players.

Each feature disclosed in the description and (where appropriate) the claims and drawings may be provided independently or in any appropriate combination. Features described as being implemented in hardware may also be implemented in software, and vice versa. Reference numerals appearing in the claims are by way of illustration only and shall have no limiting effect on the scope of the claims.
CLAIMS

1. A method of rendering a content item (10), the method comprising the steps, in a device (170) having a processor executing a player (30), of:

- rendering (S38) the content item (10);

and, at at least one point of time during execution of the method:

- verifying (S39) the presence of a proximity server (160); and

- stopping the rendering of the content item (10) in case the proximity server is not present.

2. The method of claim 1, wherein the device (170) has a user identity and the player (30) has been personalised to comprise the user identity and a user license key for the device (170), the method further comprising the steps of:

- sending (S33) a content license (20) for the content item (10) and the user identity to a license server (130);

- obtaining (S34) a user license (40) for the content item (10) from the license server (130);

- decrypting (S35) the user license (40) using the user license key to obtain a scrambling key; and

- descrambling (S36) the content item (10) using the scrambling key.

3. The method of claim 2, further comprising the step, between the descrambling step (S36) and the rendering step (S38), of watermarking the content (10).

4. The method of claim 3, wherein the player (30) has further been personalised to comprise a user watermark identity and the content (10) is watermarked with the user watermark identity.

5. The method of claim 2, further comprising the prior steps of sending user credentials to a registration server (120) and of receiving the player (30).

6. The method of claim 2, further comprising the step of obtaining (S32) the content item (10) and the content license (20).
7. The method of claim 2, wherein user license (40) has been generated from the content license (20).

8. A content delivery system (100) comprising:
   - a content database (150) configured to store at least one content item (10) and a corresponding content license (20);
   - a video server (140) configured to retrieve a content item (10) and a corresponding content license (20) from the content database (150) and to send the retrieved content item (10) and corresponding content license (20) to a player device (170, 180);
   - an application server (110) configured to receive user information from the registration server (120), to generate a personalised player application (30) for the user player device (170) and to deliver the personalised player application (30) to the user player device (170);
   - a license server (130) configured to receive a content license (20) and a user identity from the user player device, to check with the registration server (120) that a user corresponding to the user identity is authorized to access the content item (10), to decrypt the content license (20) using a system license key and re-encrypt the decrypted content license (20) using a user license key to obtain a user license (40), and to send the user license (40) to the user player device (170); and
   - a proximity server (160) configured to participate in a challenge-response protocol with the user player device (170).

9. The content delivery system of claim 8, further comprising a registration server (120) configured to receive credentials from a user player device (170), to generate the user information from the credentials, to forward the user information to an application server (110).

10. The content delivery system of claim 8, further comprising a system player device (180) comprising the system license key, the system player device being configured to receive the content item (10) and the corresponding content license (20), to decrypt the content license (20) using the system license key.
license key to obtain a scrambling key, to descramble the content item (10) using the scrambling key, and to render the descrambled content item.

11. The content delivery system of claim 10, wherein the system player device (180) is further configured to embed a watermark in the descrambled content item before rendering.
Figure 1
S21: Execute embedded player

S22: Obtain content and content license

S23: Decrypt content license

S24: Descramble content

S25: Embed watermark

S26: Render watermarked content

Figure 2
S31: Execute personalised player

S32: Obtain content and content license

S33: Send content license and user ID to the license server

S34: Receive user license from the license server

S35: Decrypt content license

S36: Descramble content

S37: Embed watermark

S38: Render watermarked content

S39: Check presence of the presence proxy

Figure 3