Description

Title: METHOD FOR VERIFYING THE DISPLAY OF A CONTENT ITEM BY A DIGITAL DISPLAY DEVICE, AND DIGITAL DISPLAY SYSTEM

Technical field

[0001] The present description relates to methods for verifying the display of a content item by a digital display device and to digital display systems.

Prior art

[0002] Document WO03052734 describes a method for transmitting a coded message using a digital display device, in order to verify the content item displayed by the display device. The message is representative of the displayed content item.

Summary

[0002a] In an aspect, the present disclosure refers to a method for verifying the display of a content item by at least one digital display device,

said digital display device comprising a central unit and a digital screen controlled by the central unit,

the method comprising at least the following steps:

(a) using said central unit to display the content item on the digital screen,

(b) capturing at least one snapshot of at least one portion of the content item during at least one predetermined timeslot while said content item is displayed by said digital screen,

(c) automatically calculating, using a local processor, at least one first signature of the snapshot captured during said at least one predetermined timeslot,

(d) transmitting content authentication data dependent on said at least one first signature, with a timestamp, to at least one remote server,

(e) comparing at least one content authentication signature, dependent on the content authentication data, with at least one content reference signature that is calculated in the same way as the content authentication signature but based on a scheduled content item expected to be displayed on said digital screen during said at least one predetermined timeslot,

(f) if said content authentication signature corresponds to the content reference signature of said scheduled content item, generating at least one authentication token authenticating the displayed content item.

[0002b] In an aspect, the present disclosure refers to a digital display system having:

- a digital display device comprising a central unit and a digital screen controlled by the central unit,
- at least one remote server,

said central unit of the digital display device being configured so as to:

(a) display the content item on the digital screen,

(b) capture at least one snapshot of at least one portion of the content item during at least one predetermined timeslot during at least one predetermined timeslot while said content item is displayed by said digital screen,

(d) transmit content authentication data dependent on at least one first signature, with a timestamp, to said at least one remote server, said first signature being calculated automatically by a local processor based on a light signal captured during said at least one predetermined timeslot,

said at least one remote server being configured so as to compare at least one content authentication signature, dependent on the content authentication data, with at least one content reference signature that is calculated in the same way as the content authentication signature but based on a scheduled content item expected to be displayed on said digital screen during said at least one predetermined timeslot,

and said at least one remote server being configured so as, if said content authentication signature corresponds to the content reference signature of said scheduled content item, to generate at least one authentication token authenticating the displayed content item.

[0003] The present description aims in particular to propose a method for verifying the display of a content item by a digital display device, which provides solid proof that the content item has effectively been displayed.

[0004] To this end, the present description proposes, in an example, a method for verifying the display of a content item by at least one digital display device,

said digital display device comprising a central unit, a digital screen controlled by the central unit,

the method comprising at least the following steps:

(a) using said central unit to display the content item on the digital screen,

(b) capturing at least one snapshot of at least one portion of the content item during at least one predetermined timeslot while said content item is displayed by said digital screen,

(c) automatically calculating, using a local processor close to the digital screen, at least one first signature (encryption function) of the snapshot captured during said at least one predetermined timeslot,

(d) transmitting content authentication data dependent on said at least one first signature, with a timestamp, to at least one remote server,

(e) comparing at least one content authentication signature, dependent on the content authentication data, with at least one content reference signature that is calculated in the same way as the content authentication signature but based on a scheduled content item expected to be displayed on said digital screen during said at least one predetermined timeslot,

(f) and, if said content authentication signature corresponds to the content reference signature of said scheduled content item, generating at least one authentication token authenticating the displayed content item.

[0005] By virtue of these provisions, as the signature is calculated automatically and as close as possible to the display, it is very difficult to forge said signature, such that the method provides strong proof, created at the source and not able to be forged thereafter, of the effective display of the scheduled content item. In addition, as the signature represents a low volume of data, the method consumes little bandwidth when transmitting the authentication data to the remote server. As the signature is calculated simply on one or more snapshots, calculation thereof is moreover lightweight and fast.

[0006] The method moreover does not require modifying the content item by adding coded portions thereto or masking a portion of the content item by way of any optical sensors in order to capture the snapshot or snapshots. In the case of using optical sensors, the method is robust to any image distortions or any introduction of noise into the captured signals.

[0007] In various examples of the method, there is furthermore the potential to adopt one and/or another of the following provisions (on their own or in any of their mutual combinations):

[0008] - said at least one timeslot corresponds to a total content duration of between 500 ms and 5 s;

[0024] - said at least one optical sensor is designed to take at least one image of the content item displayed by the digital screen, and said captured signal is said at least one image;

[0025] - before calculating the first signature, aberrations and degradations of the light signal are corrected by a local processor close to the digital screen (the processor that calculates the first signature or another local processor);

[0026] - said optical sensor is configured so as to take a series of images of the content item displayed by the digital screen, and said captured signal is formed by said series of images;

[0027] - said at least one optical sensor comprises a camera;

[0028] - each timeslot has a duration of less than 10 s, for example of between 5 s and 10 s;

[0029] - in step (d), additional data relating for example to a broadcast quality of said digital screen and/or to external conditions and/or to audience criteria are transmitted to said at least one remote server and, in step (e), an authentication token is calculated with a value depending both on the authentication data and on the additional data;

[0030] - the value of the authentication token is representative of a monetary value.

[0031] Moreover, in an example, the present description also relates to a digital display system having:

- a digital display device comprising a central unit and a digital screen controlled by the central unit,
- at least one remote server,

said central unit of the digital display device being configured so as to:

(a) display the content item on the digital screen,

(b) capture at least one snapshot of at least one portion of the content item during at least one predetermined timeslot while said content item is displayed by said digital screen,

(d) transmit content authentication data dependent on at least one first signature, with a timestamp, to said at least one remote server, said first signature being calculated automatically by a local processor close to the digital screen based on a light signal captured by said at least one optical sensor during said at least one predetermined timeslot,

said at least one remote server being configured so as to compare at least one content authentication signature, dependent on the content authentication data, with at least one content reference signature that is calculated in the same way as the content authentication signature but based on a scheduled content item expected to be displayed on said digital screen during said at least one predetermined timeslot,

and said at least one remote server being configured so as, if said content authentication signature corresponds to the content reference signature of said scheduled content item, to generate at least one authentication token authenticating the displayed content item.

[0032] In various examples of the system, there is furthermore the potential to adopt one and/or another of the following provisions (on their own or in any of their mutual combinations):

[0033] - said at least one server is configured so as to store said authentication token in a cryptographically secure blockchain;

[0034] - said at least one timeslot corresponds to a total content duration of between 500 ms and 5 s;

[0035] - the digital display device furthermore comprises at least one optical sensor designed to detect a light signal emitted by at least one portion of the digital screen,

said central unit of the digital display device being configured so as to: