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

(19) **World Intellectual Property Organization**
International Bureau

(43) **International Publication Date**
23 September 2010 (23.09.2010)

PCT

(10) **International Publication Number**
WO 2010/106518 A1

(51) **International Patent Classification**:
H04N 7/16 (2006.01) ***H04N 7/167*** (2006.01)

(21) **International Application Number**:
PCT/IB2010/051185

(22) **International Filing Date**:
18 March 2010 (18.03.2010)

(25) **Filing Language**: English

(26) **Publication Language**: English

(30) **Priority Data**:
2009/01905 18 March 2009 (18.03.2009) ZA

(71) **Applicant** *(for all designated States except US)*: **AL-TECH UEC (PTY) LIMITED** [ZA/ZA]; UEC House, 1 Montgomery Drive, 4302 Mount Edgecombe (ZA).

(72) **Inventor; and**
(75) **Inventor/Applicant** *(for US only)*: **SIMMS, Grant Peter** [ZA/ZA]; Unit 37 Strawberry Fields, 144 Wattle Grove Sherwood, 4091 Durban (ZA).

(74) **Agent**: **DM KISCH INC.**; P O Box 781218, 2146 Sandton (ZA).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, 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, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

[Continued on next page]

(54) **Title**: METHOD AND SYSTEM FOR CONTROLLING DISTRIBUTED SET TOP BOXES

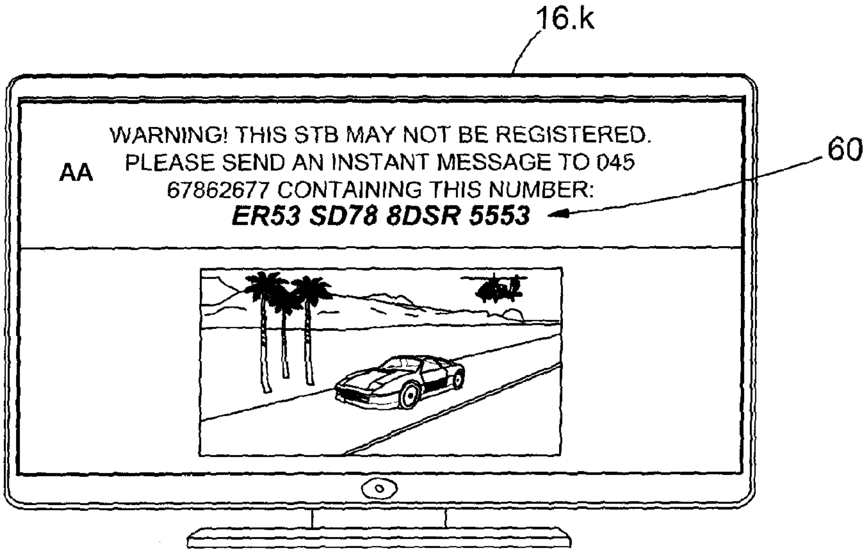

16.k
60
AA
WARNING! THIS STB MAY NOT BE REGISTERED.
PLEASE SEND AN INSTANT MESSAGE TO 045
67862677 CONTAINING THIS NUMBER:
ER53 SD78 8DSR 5553

FIGURE 6(b)

(57) **Abstract**: A method of controlling at least one of a plurality of distributed receiving devices for encrypted broadcast services comprising the steps of broadcasting to the at least one device (12.1 to 12.n) an application module 22 comprising an application code part, a business rules part and an application data part. The module is sequentially mutated 22', 22" by changing at least one of the application code part, the business rules part and the application data part. The mutated application modules 22, 22' 22"... are sequentially executed by the device and the device is caused to operate in accordance with the mutated application modules.

WO 2010/106518 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

METHOD AND SYSTEM FOR CONTROLLING DISTRIBUTED SET TOP BOXES

INTRODUCTION AND BACKGROUND

This invention relates to a method and system for controlling a receiving device for encrypted broadcast services at a user station. More particularly, the invention relates to a method and system for controlling a set-top box connected to a television monitor at a user station.

It is well known that smart cards for set-top boxes or the like intended to be connected to television (TV) sets and to decode encrypted services broadcasted from one or more head-ends, are cloned by unauthorized parties and the cloned cards are sold to customers. These cloned smart cards may then be used with genuine boxes by pirate viewers. These viewers are then in a position to receive and view the services without paying a subscription or paying a discounted subscription to the unauthorized parties. It will be appreciated that these unauthorized parties and pirate viewers cause serious damage for, amongst others, the service broadcasters.

OBJECT OF THE INVENTION

Accordingly, it is an object of the present invention to provide a method and system with which the applicant believes the aforementioned disadvantages may at least be alleviated or which may provide a useful alternative to known methods and systems for controlling receiving devices for encrypted broadcast services.

SUMMARY OF THE INVENTION

A method of controlling at least one of a plurality of distributed receiving devices for encrypted broadcast services, the method comprising the steps of:

- broadcasting to the at least one device an application module comprising an application code part, a business rules part and an application data part;
- sequentially mutating the application module by changing at least one of the application code part, the business rules part and the application data part;
- causing the mutated application modules sequentially to be executed by the at the at least one device; and
- causing the at least one device to operate in accordance with the mutated application modules.

The receiving device may comprise a wireless receiver, which may be a satellite receiver or terrestrial receiver.

The receiving device may comprise at least one decoder and a respective key token, such as a smart card, for decoding encrypted service data broadcasted by a broadcasting head-end.

In one form of the method, the application module is broadcasted to n devices and a first mutation of the application module is executed by m devices selected from the n devices and wherein m < n.

The first mutation may be generated in response to response data received from the selected devices, or users of the selected devices.

The first mutation may comprise an application data part which is different from the application data part of the application module.

The first mutation may comprise a business rules part which is different from the business rules part of the application module.

The response data from each selected device may comprise data relating to a unique address associated with the device.

Also included within the scope of the present invention is a system for controlling at least one of a plurality of distributed receiving devices for encrypted broadcast services, the system comprising:

- a broadcast head-end comprising a server, a database and a transmitter;
- an application module mutating tool connected to the head-end, the tool being configured to generate an application module comprising an application code part, an application data part and a business rule part and the tool further being configured to mutate the application module by changing at least one of the application code part, the application data part and the business rules part;
- the head end being configured sequentially to broadcast the application module and at least part of the mutated application modules; and
- the plurality of receiving devices being configured to receive the application module and a processor of each device being configured sequentially to execute the application module and at least one mutated application module and to cause the device to operate in accordance with the application module and the at least one mutated application module.

BRIEF DESCRIPTION OF THE ACCOMPANYING DIAGRAMS

The invention will now further be described, by way of example only, with reference to the accompanying diagrams wherein:

figure 1 is a diagrammatic representation of a broadcasting system comprising a plurality of distributed receiving devices for encrypted broadcast services;

figure 2 is a diagrammatic representation of relevant parts of the receiving device and an application module hosted on the device;

figure 3 is a diagrammatic representation of relevant parts of a mutating application which in use is intermittently mutated and broadcasted to the receiving devices;

figure 4 is a similar diagram of the module in compiled form;

figures 5(a) to (c) are diagrammatic representations of the application module communicating with a hardware platform of the receiving device via an operating system running on the hardware platform;

figures 6(a) and (b) are diagrammatic representations of a display on a screen associated with the receiving device and which is controlled in accordance with the application module;

figures 7(a) and (b) are similar representations of a display on the screen and which is controlled in accordance with a mutation of the application module; and

figure 8 is a diagrammatic view of relevant parts of a system.

DESCRIPTION OF A PREFERRED EMBODIMENT OF THE INVENTION

A broadcasting system for broadcasting encoded services to a plurality of distributed receiving devices is generally designated by the reference numeral 10 in figure1.

The system comprises a plurality of distributed receiving devices 12.1 to 12.n for encrypted broadcast services. Each receiving device comprises a wireless receiver connected to a suitable antenna. In the embodiment shown, the receiver is connected to a satellite dish antenna 14.1 to 14.n. Each receiving device 12.1 to 12.n is connected to a respective screen or monitor such as a television screen 16.1 to 16.n. Each receiving device comprises at least one decoder and associated smart card 17.1 to 17.n for decoding encrypted broadcast services which are broadcasted to be received by the receiving devices. Only registered receiving devices registered at an upstream database 36 are normally enabled to decrypt the encrypted services and to cause the services to be played out on the monitor. A return path, such as return path 19.1, may be provided from at least some of the receiving devices. The return path may comprise a modem (not shown) which is connectable to the head-end 30 or may at least in part comprise part of a cellular telephone infrastructure, including a cellular phone 21.1 at the user station 23.1

Further, and as shown in figure 2, each receiving device 12.1 comprises a hardware platform 18 comprising a processor. The platform also comprises so-called secure silicon in that a unique ID code for chips or chip sets, forming part of the platform, is embedded in the chips or chip sets upon fabrication thereof. An operating system 20 runs on the platform. Application modules 22 are receivable by the receiving devices and are configured to execute on the hardware in conjunction with the operating system.

Each receiving device 12.1 to 12.n is also associated with a unique electronic address which enables a selected device to be addressed individually from the broadcast head-end 30, or as part of a group of a larger population of devices 12.1 to 12.n or as part of the whole population. The addresses may fall in a range comprising m, typically four, bytes each capable of holding 256 numbers (ranging from 0 to 255). If zero is ignored for the purpose hereinafter described, the remaining 255 numbers allow $(255)^4$ = 4,228,250,625 devices to be addressed either separately or in groups. The range is hence 0.0.0.0 to 255.255.255.255. The number 0 may not be bound and may be used to blanket address all devices falling in an address range. For example, if the address 255.255.0.0 is used, all devices with addresses in the range 255.255.1.1 to 255.255.255.255 (that is 64516 devices) would be addressed. On the other hand electronic address 192.168.10.100 would address a single device in the population 12.1 to 12.n

The electronic addresses and aforementioned embedded hardware codes may be related. The electronic addresses are generated and stored in the devices at manufacturing of the devices. The electronic address and hardware code as well as a smart card number associated with a respective smart card may be stored in the database 36 (shown in figure1).

For each device 12.1 to 12.n a processor on the smart card 17.1 and the processor of the device 12.1 may cooperate and on an instruction from a back-end processor and under guidance of the back-end processor, generate and store on the smart card and/or on the device a unique code or "biometric code" which is derived from data relating to the device on the one hand and data relating to the smart card on the other. Since this generation is performed under control or guidance of the back-end processor, the biometric codes for each back-end registered smart card and device combination, would be known to the back-end processor.

Referring to figures 3 and 4, the application module 22 comprises an application execution engine part 24 comprising the application code, an application data part 26 and a business rules part 28. The engine 24 is configured to interoperate the application data part 26. The business rules part 28 dictates how the application module behaves on a hosting receiving device 12.1 to 12.n. The module is compiled at a head-end 30 (shown in figure 1) utilizing a special tool 32.

Referring to figure 1, a method of controlling the receiving devices 12.1 to 12.n comprises the steps of broadcasting from the head-end 30 via a satellite communication path 34 to the distributed devices 12.1 to 12.n, the application module 22 comprising the application code part 24, the application data part 26 and the business rules part 28. The application 22 is sequentially mutated 22', 22'', 22'''....by changing at least one of the application code part, the business rules part and the application data part. The application module 22 and mutated application modules 22′, 22″, 22‴....are sequentially executed by the at least one device and the at least one device is caused to operate in accordance with the application module 22 and mutated application modules 22′, 22″..... More particularly, the application module 22 and the mutated application modules 22′, 22″, 22‴...., in conjunction with the operating system 20 and the hardware platform 18, cause the receiving devices 12.1 to 12.n to operate in a predetermined manner.

For example and referring to figures 5(a) to 5(b), the application module 22 interrogates the hardware platform 18 via the operating system 20 regarding the embedded code. If the module 22 determines that the embedded code is not a code registered in the aforementioned upstream database, the business rules part causes the receiving device, as shown in figure 5(c), to operate in a predetermined manner.

In one form of the method and in order to determine whether unregistered smart cards or cloned smart cards 17.k are used to decode broadcast services, a first application module 22 is broadcast to all or a group of devices 12.1 to 12.n. The application module 22, when hosted on the devices, is configured to read the aforementioned unique code or biometric code and to compare on the device the code read and the code, which according to the back-end processor, should be the code for a particular combination of device and associated smart card. If the compared codes of a device 12.k do not match, a first version of the business rules part 28 of the application module 22 is configured to cause the device 12.k to display on the associated monitor 16.k a message, such as that shown in figure 6(b). The message comprises an encrypted number 60 comprising the aforementioned electronic address of the device 12.k. Genuine and properly registered devices, such as device 12.1 connected to screen 16.1 shown in figure 6(a), continues to operate normally.

The aforementioned displayed message requests the user to return via return path 19.k, the encrypted number 60. The returned number is processed at the back-end to update a list of electronic addresses associated with unregistered smart cards hosted in the database 36. The user may be given an opportunity, within a specified time window, to register the unregistered card. If done, the services may not be interrupted.

However, if the device or smart card is not registered within the time window, data relating to a first mutation 22′ of the application module may be broadcasted from the head-end 30. The first mutation comprises the electronic address of the unregistered device 12.k, typically as part of the application data part 26. Therefore at least the application data part 26 of the first mutation 22' is different from the application data part of the original application module 22. The business rules part 28 of the first mutation 22' may also differ from the first version of the business rules part of original application module 22. The business rules part in the first mutation 22' may dictate that device 12.k be switched from the normal operating state as shown in figure 7(a) to a stand-by or disabled state, wherein the device 12.k is disabled from playing out the content on the screen 16.k.

As in the case of the example hereabove, the generation of mutations of the application module 22 may be triggered by a response comprising response data received from a selected device or devices, or, from users of such devices. In a preferred form of the invention, at least one of the application data part 26 and the business rules part 28 is changed. The entire mutated module 22' may be broadcasted from the head end and in other forms, only the changed parts may be so broadcasted.

In still other forms of the method, the mutations are automatically generated intermittently, to stay ahead of hackers, imitators and copiers. At least one mutation application module 22′ is generated and executed, but it will be appreciated that any suitable number of mutation modules 22″, 22‴ may sequentially be generated and executed.

A system 100 comprising backend server 132 and a client or user devices 112.1 is shown in figure 8.

A suite of software algorithms (ε1, ε2, ε3 and ε4) for the compression and manipulation of digital interactive information is executed by the system 100. The suite of software algorithms is used for the interactive synchronization and management of broadcast data for digital program content. The result output of the system gives a user of the device 112.1 a two-way interactive perception on the user play-out device 112.1, although the transmission/broadcast may only one-way, from back-end 132 to device 112.1.

The backend server 132 executes several algorithms and software modules that produce compressed interactive epsilon (ε) binary flow code that may either be broadcast directly to client devices 112.1 (Set

Top Boxes, kiosks, mobile phones etc) or further interpreted for play-out to third party devices using specific proprietary applications.

These modules provide several tool sets that allow the integration of interactive menus and special objects called "gadgets" for the enhanced user experience of viewing and interacting with broadcast or streamed digital content.

The content management system comprises the following main modules Epsilon Designer, Epsilon Broadcast Automation, Epsilon Synchronisation and Epsilon Debug.

Epsilon Designer is a Rapid Interactive TV Application Development (RAD) tool for developing application for several different output devices such as Set Top Box's (STBs) and kiosks.

The automation engine allows system critical data flow processes for interactive applications. It enables real-time data updates to be multicast with intrinsic binary data.

The synchronization engine allows the interactive play-out of interactive content with program and advertising information.

Interactive application play-out allows targeted advertising for interactive view of products.

Referring again to the diagram, the first algorithm ε1 interprets any vector graphic input into an efficient and compressed data block.

The data is further processed through a special interactive engine that allows the integration of interactive objects with the vector produced data. These may include dialogue boxes, buttons, action items, triggers and events. The algorithm then takes this data block and using a second encoding algorithm ε3 to produce an efficient and compressed Extensible Mark-up Language (XML) file with embedded content and interactive objects, called gadgets. These objects and gadgets may be encrypted and encapsulated with a unique algorithm.

The XML file is a generic output of the first set of unique algorithms that may then be further encoded for a specific target device. The target device may run software (middleware).

The resultant output of the third encoding ε3 is a binary source flow file that may be played using the Epsilon broadcast server and synchronisation engine to the target devices.

The Epsilon client application ε4 that resides in each user device 14 is agnostic to the mechanism used to play-out the source binary file to the device. For example, the source binary file may be streamed by the broadcaster or it may be streamed using any TCP/IP or broadband connectivity.

On reception of the source binary file, the Epsilon client module ε4 interprets the received binary source file and places the necessary objects and gadgets on the receiving device screen. The algorithm used in the client module ε4 offers the intelligence required to interpret the interactive reactions of each unique user to the gadgets and objects displayed on the screen, offering a seamless interactive experience.

The epsilon playback on the receiving device 112.1 may be used for several applications for interactive advertising, games, education programs and even a form of unique mutating conditional access.

The system according to the invention may also be used selectively to disable or switch off remote devices 112.1 as hereinbefore described.

CLAIMS

1. A method of controlling at least one of a plurality of distributed receiving devices for encrypted broadcast services, the method comprising the steps of:

   - broadcasting to the at least one device an application module comprising an application code part, a business rules part and an application data part;
   - mutating the application module at least once by changing at least one of the application code part, the business rules part and the application data part;
   - causing the application module and the mutated application module sequentially to be executed by the at the at least one device; and
   - causing the at least one device to operate in accordance with the application module and the mutated application module.

2. A method as claimed in claim 1 wherein the application module is broadcasted to n devices and wherein a first mutation of the application module is executed by m devices selected from the n devices and wherein m < n.

3. A method as claimed in claim 2 wherein the first mutation is generated in response to response data received from the selected devices, or users of the selected devices.

4. A method as claimed in any one of claims 2 and 3 wherein the first mutation comprises an application data part which is different from the application data part of the application module.

5. A method as claimed in any one of claims 2 to 4 wherein the first mutation comprises a business rules part which is different from the business rules part of the application module.

6. A method as claimed in any one of claims 3 to 5 wherein the response data from each selected device comprises data relating to a unique address associated with the device.

7. A system for controlling at least one of a plurality of distributed receiving devices for encrypted broadcast services, the system comprising:

- a broadcast head-end comprising a server, a database and a transmitter;

- an application module mutating tool connected to the head-end, the tool being configured to generate an application module comprising an application code part, an application data part and a business rule part and the tool further being configured to mutate the application module by changing at least one of the application code part, the application data part and the business rules part;
- the head end being configured sequentially to broadcast the application module and at least part of the mutated application modules; and
- the plurality of receiving devices being configured to receive the application module and a processor of each device being configured sequentially to execute the application module and at least one mutated application module and to cause the device to operate in accordance with the application module and the at least one mutated application module.

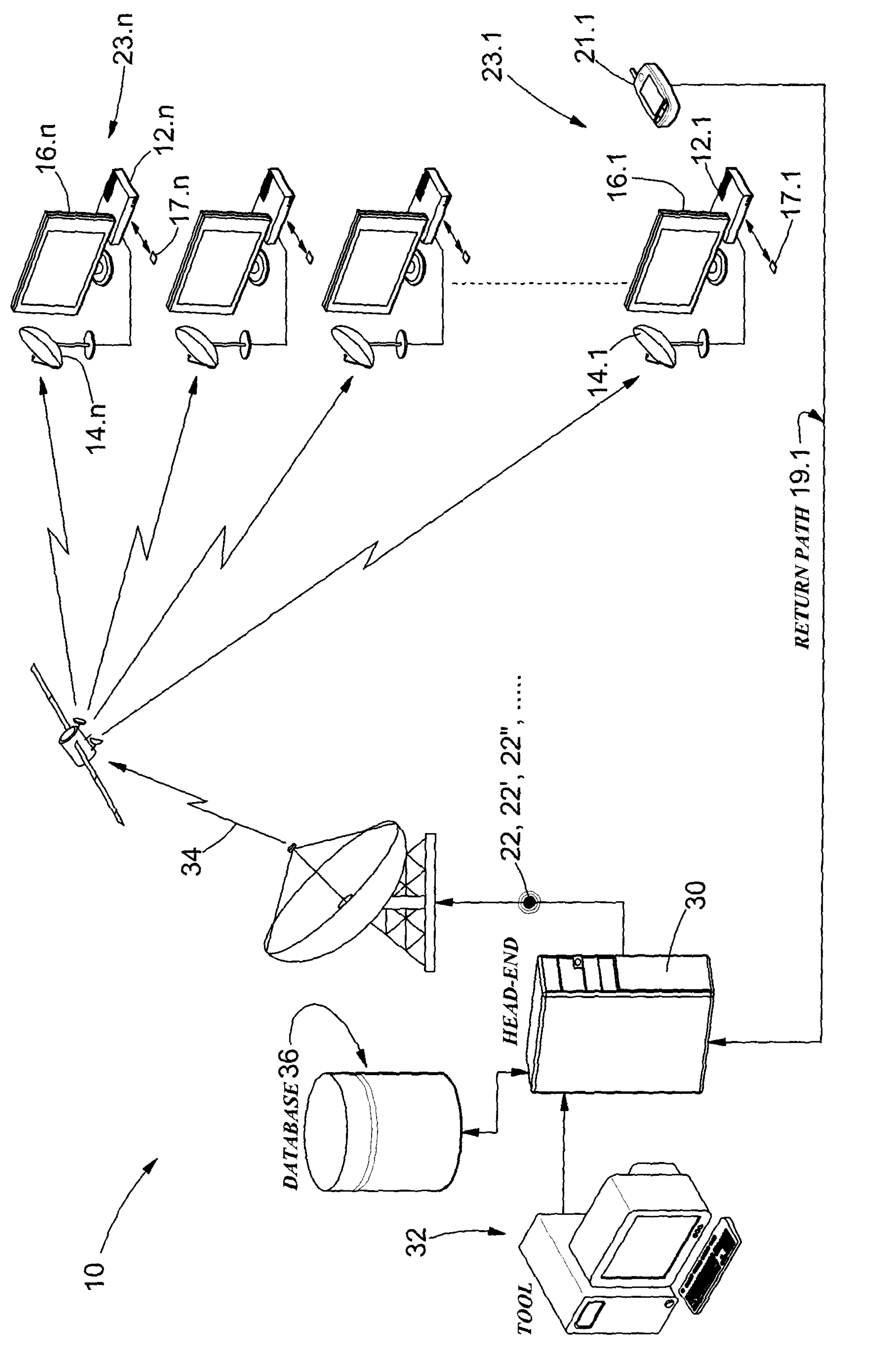

10
32
TOOL
DATABASE 36
HEAD-END
30
22, 22', 22", ...
34
14.n
16.n
12.n
23.n
17.n
23.1
21.1
16.1
12.1
17.1
14.1
RETURN PATH 19.1

FIGURE 1

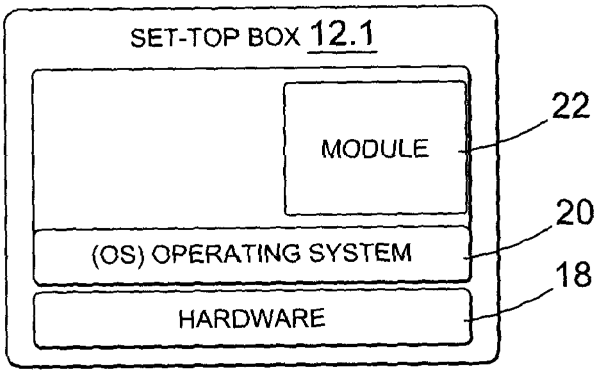


FIGURE 2

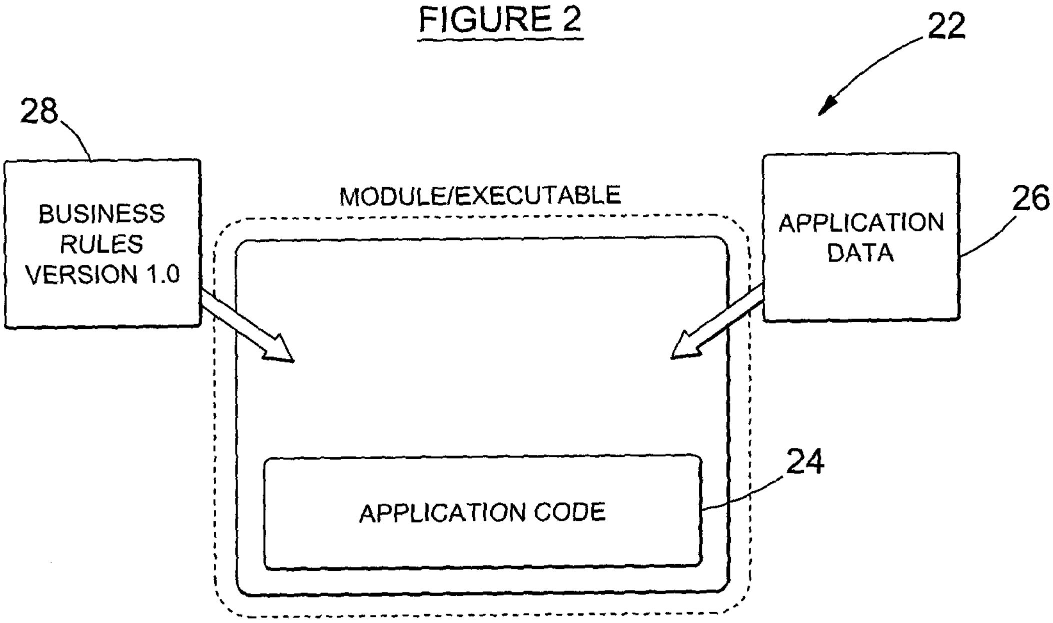


FIGURE 3

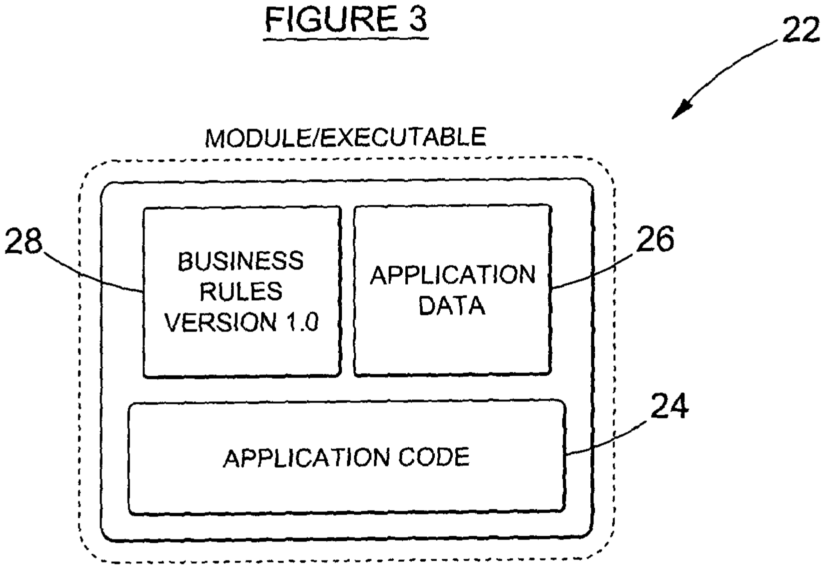


FIGURE 4

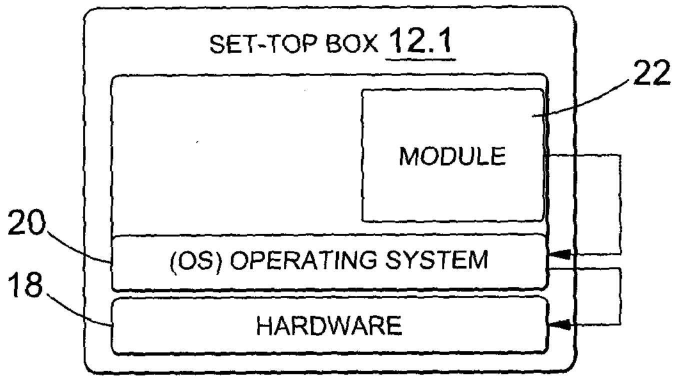


FIGURE 5(a)

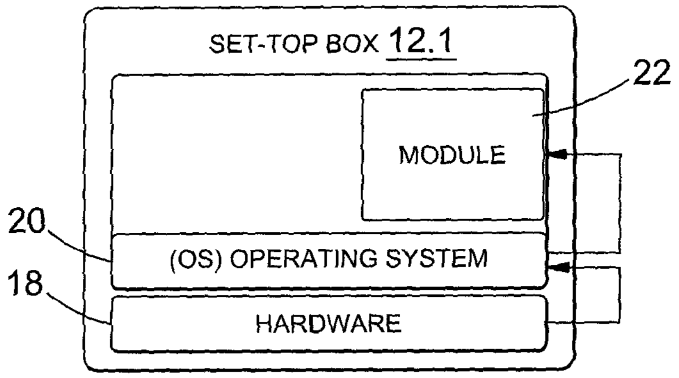


FIGURE 5(b)

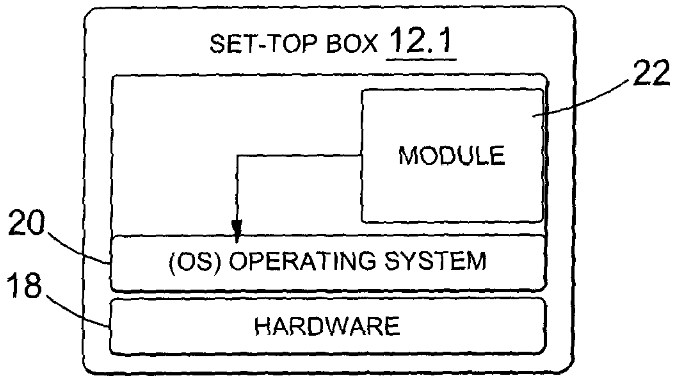


FIGURE 5(c)

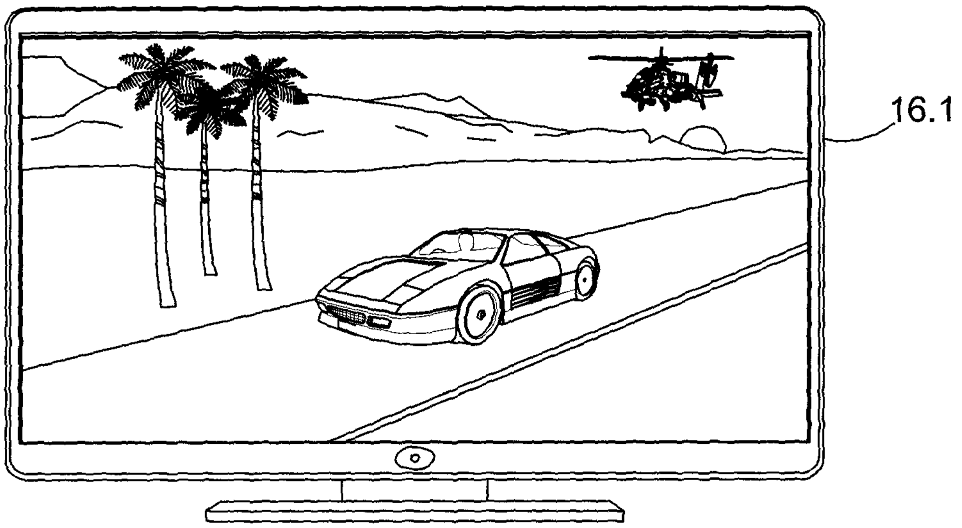
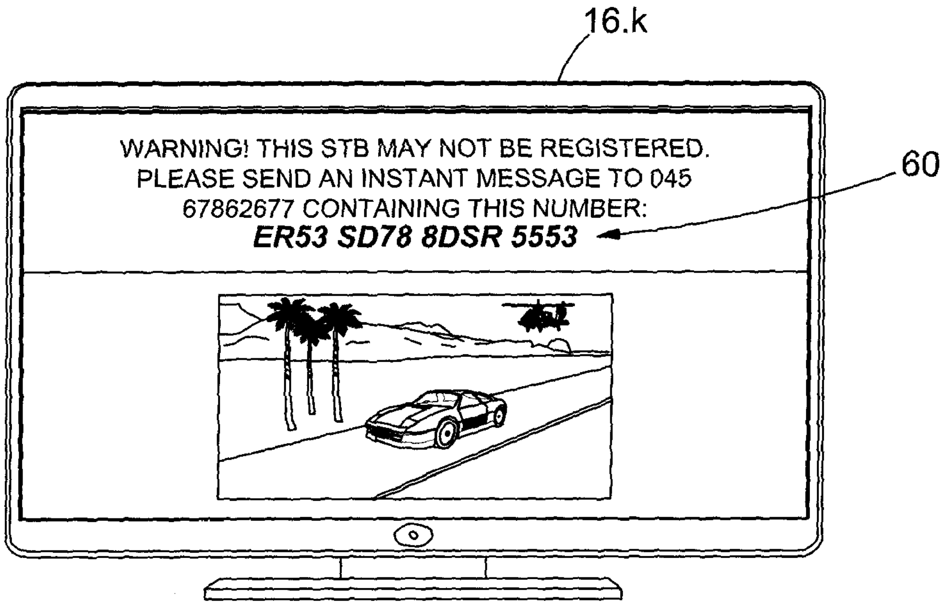


FIGURE 6(a)



WARNING! THIS STB MAY NOT BE REGISTERED.
PLEASE SEND AN INSTANT MESSAGE TO 045
67862677 CONTAINING THIS NUMBER:
ER53 SD78 8DSR 5553

FIGURE 6(b)

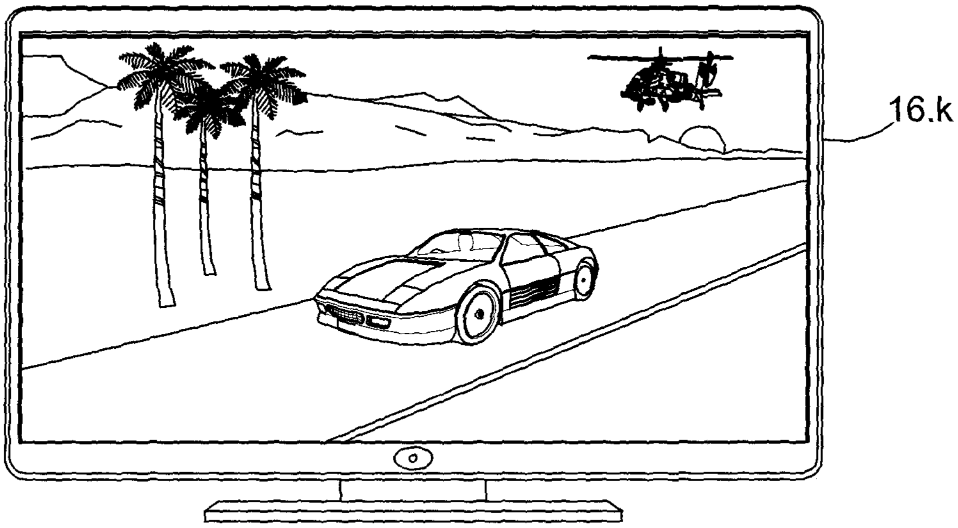


FIGURE 7(a)

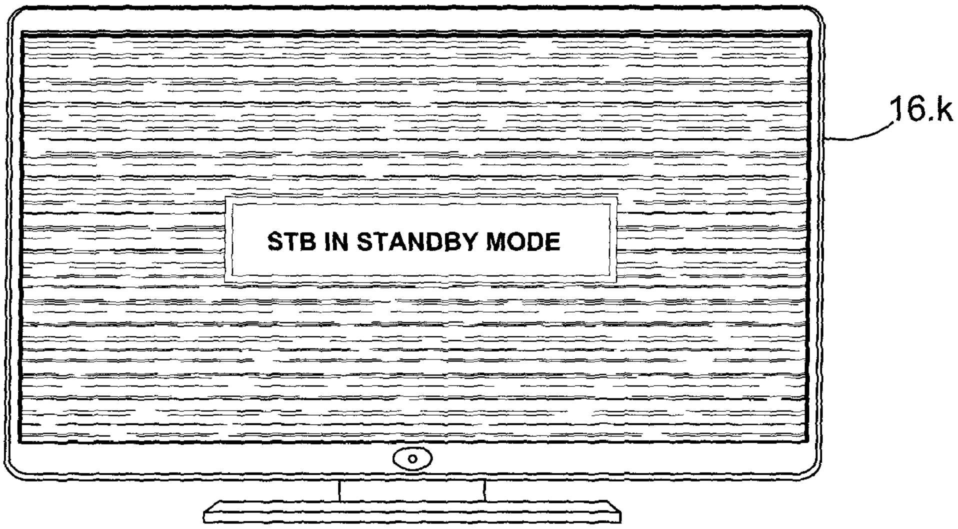


FIGURE 7(b)

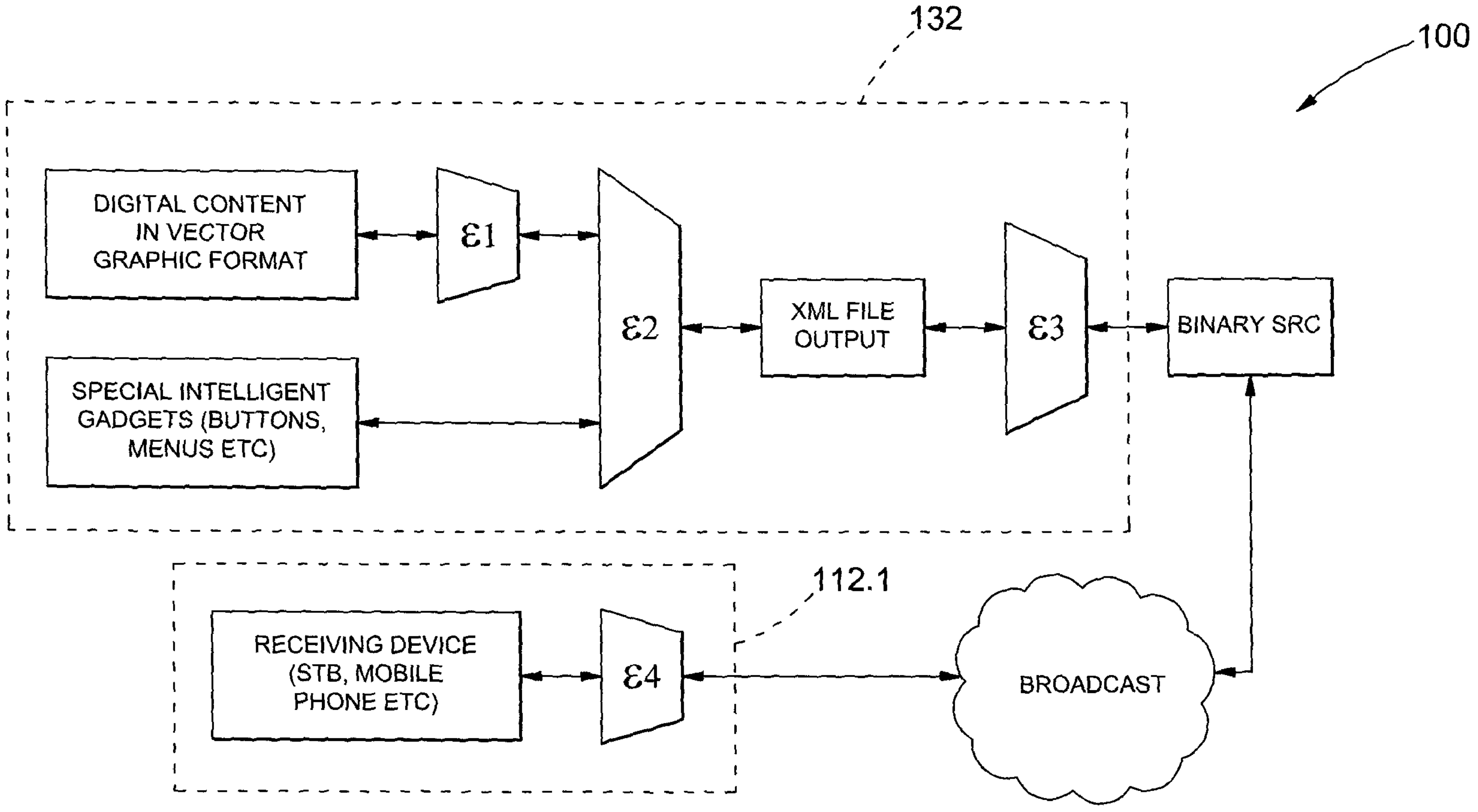

132
100
DIGITAL CONTENT IN VECTOR GRAPHIC FORMAT
ε1
ε2
XML FILE OUTPUT
ε3
BINARY SRC
SPECIAL INTELLIGENT GADGETS (BUTTONS, MENUS ETC)
112.1
RECEIVING DEVICE (STB, MOBILE PHONE ETC)
ε4
BROADCAST

FIGURE 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2010/051185

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04N7/16 H04N7/167
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008/008321 A1 (GAGNON GREGORY J [US] ET AL) 10 January 2008 (2008-01-10) paragraphs [0050] - [0087]; figure 4	1-7
X	US 6 550 008 B1 (ZHANG MINDA [US] ET AL) 15 April 2003 (2003-04-15) column 6, lines 35-46; figures 1-3	1-7
X	US 2002/031224 A1 (BASAWAPATNA GANESH [US] ET AL) 14 March 2002 (2002-03-14) paragraphs [0069] - [0072]	1-7
X	FR 2 865 592 A1 (VOGT NOEL [FR]) 29 July 2005 (2005-07-29) the whole document	1-7

□ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 14 June 2010	Date of mailing of the international search report 12/07/2010
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Marzal-Abarca, X

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2010/051185

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 2008008321	A1	10-01-2008	NONE	
US 6550008	B1	15-04-2003	NONE	
US 2002031224	A1	14-03-2002	NONE	
FR 2865592	A1	29-07-2005	NONE	