

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

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
20 February 2003 (20.02.2003)

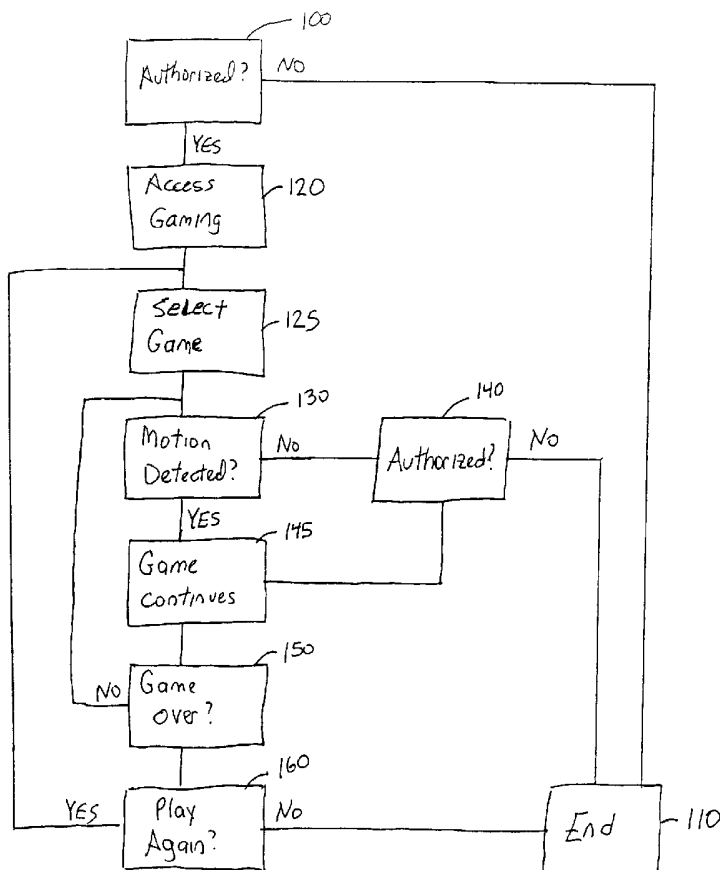
PCT

(10) International Publication Number
WO 03/015428 A1

- (51) International Patent Classification⁷: **H04Q 7/20**
- (21) International Application Number: PCT/US02/26977
- (22) International Filing Date: 8 August 2002 (08.08.2002)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
60/311,189 8 August 2001 (08.08.2001) US
- (71) Applicant (for all designated States except US): **BUCH-BINDER, Sam** [US/US]; 500 Skokie Blvd., Suite 200, Northbrook, IL 60062 (US).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): **MAGES, Ken** [US/US]; 1671 Strath Erin, Highland Park, IL 60035 (US).
- (74) Agent: **SHAFTAL, Max**; Patzik, Frank & Samotny, Ltd., 150 South Wacker Drive, Suite 900, Chicago, IL 60606 (US).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK,

[Continued on next page]

(54) Title: PREVENTING UNAUTHORIZED USE OF A WIRELESS OR WIRED DEVICE



(57) Abstract: A system and method for determining whether an authorized user (Fig. 7) has retained possession of a device (12) for participating in gaming activities. The system includes a wireless or wired remote device (12) that is fitted with a kill switch (80) that will disable use of the device (12) until the authorized user resubmits the necessary verification. The kill switch (80) may be activated by the lack of movement of the device (12), thermal sensors, capacity sensors, contact switches, dead-man switches or the like.

WO 03/015428 A1



TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *with international search report*

PREVENTING UNAUTHORIZED USE OF A WIRELESS OR WIRED DEVICE

10

This application claims priority based upon U.S. Provisional Patent Application Serial No. 60/311,189 filed August 8, 2001.

15

TECHNICAL FIELD

This invention relates in general to gaming activities, and more particularly to a system and method for providing security for wireless or wired remote gaming activities, and still more particularly to a system and method for providing security for wireless or wired remote gaming activities that includes a kill switch to prevent the unauthorized use of the wireless device if left unattended or taken from the authorized user.

20

BACKGROUND ART

Casinos provide a venue for people to participate in gaming activities. Recently, there has been a push for casinos to provide services to enable their patrons to remotely participate in gaming activities. Therefore, instead of having to physically sit down at a table or machine, the patron may participate in gaming activities from other locations such as in a shopping mall or on a golf course.

25

In addition to verifying the correct time and location of a user on the casino property to ensure that the activity is legally transacted, it is also imperative that the use of the device be limited to the authorized user to prevent unauthorized gaming activities from taking place.

5 Heretofore, it has been known to use passwords in connection with a wireless device to restrict access to on-line transactions to individuals with knowledge of the requisite password. Other devices have included means for recording, storing and verifying biometric information of the user so that access will be denied if the biometric information of the individual seeking access does not match the stored
10 biometric information of the user.

 While biometric, password-protected or other conventional security devices can perhaps prevent an unauthorized user from powering on a wireless device and initially gaining access to on-line transactions through the wireless device, they may not prevent on-line transactions by unauthorized users. In particular, the known
15 security devices do not protect against an unauthorized user using the wireless device-
-if the wireless device is put down or set aside after the authorized user activates the device. For example, if the authorized user leaves the unit powered on and inadvertently leaves it unattended while in the middle of an on-line gaming session, an unauthorized user may carry on a number of substantial losing wagers, which
20 would be automatically charged to the authorized user.

 If the authorized user challenges any losses on the basis that he or she did not authorize the wagers that led to the subsequent losses, then the casino would be put in the uncomfortable position of choosing between: (1) enforcing such losses and offending a potentially profitable guest, who may instead frequent a different casino
25 or hotel in the future; or (2) absorbing the financial loss by not enforcing such losses.

It has also been known to have the device shut off after the failure to detect gaming activity for a pre-determined amount of time. However, problems have arisen during the use of such security measures because of the pre-determined amount of time before shut-down. For instance, if a smaller time limit such as one minute is set for the device to shut off due to a lack of gaming activity, the device may shut off before the user has had the opportunity to complete the transaction. Conversely, if the interval before the device powers off is set at a large time limit, an unauthorized user may acquire an inadvertently unattended device and run up huge gaming losses during that interval. The losses would then be charged to the registered or authorized user as opposed to the actual user.

Therefore, there is a need to produce a wireless or wired remote device that protects against unauthorized use without interfering or interrupting the authorized use of the device.

DISCLOSURE OF THE INVENTION

The present invention is an improvement over the prior security systems used to prohibit unauthorized use of a wireless or wired remote device for gaming activities. In particular, the security system of the present invention includes a wireless or wired remote device that may be connected to the Internet, casino server or the like to participate in gaming activities. The device includes an internal or external kill switch that automatically disables the device when the authorized user sets the device down to prevent any unauthorized uses of the device. One embodiment of a kill switch is an internal motion switch that includes a positively-charged central thin foil sheet having a free end located between the arms of a negatively-charged U-shaped member. Movement of the device causes the free end of the foil sheet to contact the arms of the U-shaped member to complete the circuit

and allow for the device to continue to be used. If the completion of the circuit is not detected within a set amount of time, the wireless or wired remote device is disabled until proper authorization is verified.

It is therefore an object of the present invention to provide a new and
5 improved security device for a wireless or wired remote device that prevents unauthorized transactions.

A further object of the present invention is to provide a security system for a wireless or wired remote device that does not interfere or interrupt the authorized use and enjoyment of the device.

10 Another object of the present invention is to provide a kill switch for a wireless or wired remote device that will automatically shut down an unattended device after a certain interval of inactivity, movement or contact.

A still further object of the present invention is to provide a security system for a wireless or wired remote device that is easy and economical to manufacture.

15 Other objects, features and advantages of the invention will be apparent from the following detailed disclosure, taken in conjunction with the accompanying sheets of drawings, wherein like reference numerals refer to like parts.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram illustrating a device operably connected to the
20 Internet to provide gaming activities and a plurality of transmitters which in turn are operably connected to a CDMA server within a building and a GPS base station and associated GPS antenna outside the building.

Fig. 2 is a schematic view of an embodiment of a wireless device of the present invention.

Fig. 3 is a vertical plan view of an embodiment of a wireless device of the present invention.

Fig. 4 is a vertical plan view of the back side of a wireless device showing a biometric thumb print scanner.

5 Fig. 5 is a simplified vertical plan view of an embodiment of a motion switch of the present invention.

Fig. 6 is a perspective view of a wireless device having a pressure sensitive band around its periphery.

Fig. 7 is a simplified flow chart illustrating the steps involved in ensuring that
10 a wireless transaction is authorized.

DETAILED DESCRIPTION OF THE INVENTION

While this invention is susceptible of embodiment in many different forms, there is shown in the drawings and will herein be described in detail several specific embodiments, with the understanding that the present disclosure is to be considered
15 merely an exemplification of the principles of the invention and the application is limited only to the appended claims.

Referring now to the drawings, and particularly to FIG. 1, there is shown an example of an assisted global positioning system (hereinafter "AGPS") that may be used with the present invention to provide wireless or wired gaming activities. The
20 AGPS, generally designated by the number 10, is shown as having a device 12 operably connected to a plurality of transmitters 14 located throughout the inside of a building 16 to accurately determine the location of the device 12. Information collected from the device may then be transmitted to a microbase transceiver station 17, which in turn transmits the information to a GPS base station 18 having GPS base
25 station circuitry and a GPS antenna 20 for transmitting and/or receiving the

information or other transmissions to or from one of a plurality of GPS satellites 21 orbiting the earth. While GPS is referred to herein as the method for locating the user, other location methods or triangulation-based technology should be considered as being capable of being used with the present invention. The device is connected to the Internet 15 or a server associated with a casino to enable the device to offer gaming activities. While the transmitters are shown as being located within the interior of a building, it is appreciated that they also may be located outside the building as well, so as to assist in determining the location of the device outside. It is also appreciated that the transmitters may transmit the information directly to the device, which in turn transmits the information to the GPS base station.

Referring now to FIGS. 2 and 3, a wireless device for use in the present invention is shown. As shown in FIG. 2, the wireless device 12 may include a GPS chipset 22 for providing time and geographic position data to a microprocessor 23, means for providing hardware encryption and decryption of all information sent or received 24 from the wireless device 12, and a wireless modem 25 or other means for connecting to the Internet 15, remote server or the like. The wireless device 12 is also provided with memory 26, a RF or IR receiver/transmitter 27, a keypad 28 for manually inputting data and a display screen 30.

Alternatively, the display screen 30 can be a touch screen that serves as both the keypad for inputting information and the display screen. The keypad 28 can also be a peripheral device such as an external keyboard or a series of buttons 46 and a multi-directional thumb pad 44. Likewise, hardware encryption/decryption can be provided by the GPS chipset 22. Also provided are an external GPS antenna 39 and a receiver/transmitter antenna 38. The GPS chipset 22, kill switch 80, keypad 28, contact switch 90, screen display 30, biometric device 40, ram module slot 95,

memory 26, external power 32 and battery 31 and RF receiver/transmitter are all connected to the microprocessor 23. It also is appreciated that the wireless or wired remote device may include any other components known in the art to allow a wireless or wired remote device to send, retrieve and display information to participate in
5 wireless or wired remote gaming activities.

The example of the wireless device 12 shown and disclosed is sized so that it may be readily transported throughout the casino building 16. A smart or swipe card reader 50 having a unique identification number is preferably used in conjunction with the wireless device to allow the wireless device to be selectively activated and
10 used on different occasions. For example, the smart card may be inserted into a smart card reader 50 on the side of the wireless device in a known way to allow the wireless device to access the information on the smart card to verify and determine identity and account information. Once a smart card is issued and inserted into the wireless device 12, the wireless device communicates with the Internet 15 to allow for secure,
15 legal wagers to be placed from within the casino or on the casino grounds. While a modular wireless device is shown, it is appreciated that the device may be a cellular phone, a wireless device having cellular phone capabilities, other wireless devices such as PDAs and the like, or a wired gaming device. Similarly, while a device for participating in gaming activities is shown and disclosed, it is appreciated that the
20 device may be used for any secure transactions, such as on-line shopping, financial transactions or the like.

As shown in FIG. 2, the wireless device 12 includes the viewing or display screen 30, such as an LCD screen, for displaying information; one or more speakers 42 for providing voice or sound in conjunction with the selections or results; and a
25 multi-directional thumb pad 44 and a series of button 46 on the face 48 of the wireless

device 12 for selecting and playing the various gaming activities or games associated with the wireless device.

The kill switch 80 of the wireless device may be any kind of switch that is capable of detecting when the wireless device has been set aside, placed down or otherwise left unattended. One such embodiment of a kill switch is one or more conventional internal or external motion switches 80 of the type generally known in the prior art for opening or closing a circuit upon a predetermined degree of movement being applied thereto. Referring to Fig. 5, one such motion switch would have a positively-charged central thin, foil sheet 82 having a free end 84 surrounded by a pair of arms 88 of a negatively-charged U-shaped member 86. In operation, virtually any slight movement of the device 12 would cause the free end 84 of the foil sheet 82 to make momentary contact with either of the oppositely charged arms 88 of the U-shaped member 86 located on either side of the foil sheet 82, thereby closing a circuit and sending a signal to the microprocessor 23. The device can be programmed so that if no such motion is detected within a predetermined amount of time, on-line usage is terminated and a new thumbprint or other verification means from the authorized user would be needed before the device would resume on-line usage. While a U-shaped member with a foil sheet is shown, it is appreciated that other types of motion sensors, such as the Tilt-Actuated Switch of US Pat. No. 5,153,394, should be considered as being within the scope of this invention.

It is also appreciated that multiple contact switches of the type generally known in the prior art can also be provided on the top and bottom of the device for opening or closing a circuit when pressure is applied to the contact switch, such as by placing the wireless device down on a surface. While one contact switch may be employed, it is preferred that multiple contact switches be used, for example, near the

corners of the top and bottom of the device. Such switches may be spring-biased outwardly so that when the device is placed down on a surface, such as a table, one or more of the switches would close, thereby opening or breaking a circuit to discontinue the gaming activities or otherwise sending a signal to the microprocessor that the
5 device has been placed down by the user. The switches are sensitive enough to be activated if placed down on a couch, chair or carpeted floor. Once placed down, use of the wireless device to participate in gaming activities would be suspended and the entry of another verified thumbprint would be needed before use could be resumed.

Alternatively, the device could include a conventional "dead man's switch" of
10 the type generally known in the prior art, wherein in order to maintain continued on-line access, the user would have to continuously activate a switch located on the outside of the device in order to keep the circuit closed. For example, as shown in Fig. 6, the wireless device may include a pressure-sensitive band 92 that surrounds the outer circumference of the wireless device 12, where the wireless device 12 would
15 normally be held. Holding the device pushes the pressure sensitive band against the wireless device to close the circuit and supply power to the wireless device. Upon release of the dead man's switch (e.g., the device is placed on a table or the like), the circuit is opened and the wireless device would terminate the on-line connection. The switch is preferably spring-loaded and biased into the open position, so that the
20 removal of the pressure from the pressure sensitive band results in opening of the circuit. Release of the wireless device for any purpose would thereby suspend use and require the entry of another verified thumbprint or some other form of identification verification before use is resumed.

Other types of kill switches may include, but are not limited to, thermal sensor
25 switches and capacitor sensors that allow continued use of the device so long as

thermal or electrical sensors detect human activity within a preset range. The foregoing kill switch features could be similarly applied to a wired device, such as one that has a wired power, Internet or network connection. Additionally, the foregoing kill switch features can also be applicable to those devices that do not have
5 GPS or other location identification capabilities.

As indicated in the simplified flow diagram of FIG. 7, the device 12, when started will request verification of an authorized use in step 100. Verification of an authorized use of the wireless device may be accomplished through the use of a biometric device 40 such as a thumbprint or retinal scanner, or any other known
10 means. Examples of a thumbprint scanner are U-Match Biolink® or ThumbTrax® devices embedded in the exterior of the device. Alternatively, biometric device 40 can be an external peripheral device such as a mouse or Compact Flash Card. If the proper verification is not inputted or received, then the wireless device will not permit access to the gaming activities and the use of the wireless device will end in step 110
15 until proper verification is submitted. On the other hand, if verification in the form of the proper thumbprint or otherwise is inputted and confirmed, then the wireless device 12 is connected to the Internet 15, casino server or the like to permit the authorized gaming activities to commence in step 120. Once the gaming activities commence, a particular game may be selected in step 125.

20 If during use of the wireless device, the motion sensor kill switch 80 fails to sense motion for a predetermined amount of time in step 130, use of the wireless device will be suspended by the microprocessor 23 in step 110 unless verification of an authorized use is completed in step 140. If the verification step is completed, gaming activities may again be engaged in through the use of the wireless device.
25 Likewise, if during use of the wireless device, the dead man's switch detects that the

wireless device is no longer being held or has been placed down on a couch or table, then use of the wireless device to participate in gaming activities will be suspended unless and until identity verification is provided. If the proper identification information is not inputted into the wireless device, then the gaming activities will
5 end in step 110.

Alternatively, if the motion sensor kill switch detects motion within the preset amount of time in step 130, the wireless device will allow for the gaming activities to continue in step 145. The motion sensor kill switch will *continue to monitor whether* the wireless device moves within the prescribed time period until the particular
10 gaming activity is completed in step 150. Thus, if the motion sensor kill switch fails to detect motion before the transaction is completed, then the wireless device will disconnect the wireless device from the Internet, network or casino server in step 110 until proper authorization is once again inputted in step 100 or step 140.

Upon completion of the gaming activity in step 150, the wireless device will
15 display a message in step 160 inquiring whether it is desired to play another game. If another game is desired, the game may be selected and played in step 125. Otherwise, the wireless device may shut down if no further gaming activities are desired in step 110.

While a device connected by wire or wirelessly to the Internet, network or
20 casino server is described in the foregoing examples, the aforementioned kill switches of the present invention would be applicable to a stand-alone, handheld or portable device, as well.

It will be understood that modifications and variations may be effected without departing from the scope of the *novel concepts of the present invention*, but it
25 is understood that this application is limited only by the scope of the appended claims.

5

Claims

- 10 1. A system for preventing the unauthorized use of a device (12)
 comprising:
 a device (12) for performing one or more transactions;
 means (80) to detect when the device (12) is left unattended; and
 means to prevent performance of the transactions when it is determined that
15 the device (12) has been left unattended.
2. A system for preventing unauthorized remote gaming activities
 comprising:
 a device (12) for allowing an authorized user to participate in gaming
20 activities;
 means (12,15) to provide gaming activities;
 means (80) to detect when the device (12) is left unattended; and
 means to cease the gaming activities when it is determined that the device (12)
 has been left unattended.
- 25 3. The system of claim 2 wherein the device (12) is a wireless device.

4. The system of claim 3 wherein the detection means (80) comprises a motion sensor.

5. The system of claim 4 wherein the motion sensor (80) comprises a positively-charged thin foil strip (82) located between a pair of arms (88) of a negatively-charged U-shaped member (86), wherein movement of the wireless device (12) causes the thin foil strip (82) to contact one of the arms (88) of the U-shaped member (86) to complete a circuit.

6. The system of claim 5 wherein the means to cease gaming activities comprises means to determine if the circuit is completed within a predetermined amount of time.

7. The system of claim 3 wherein the detecting means (80) comprises a dead man's switch.

8. The system of claim 7 wherein the dead man's switch comprises a pressure-sensitive band (92) located around the wireless device.

9. The system of claim 3 wherein the detecting means (80) comprises a contact switch.

10. The system of claim 3 wherein the detecting means (80) comprises a thermal sensor.

11. The system of claim 3 wherein the detecting means (80) comprises a capacitor sensor.

12. The system of claim 3 which further comprises means (40, 50) to
5 verify identity of the authorized user.

13. The system of claim 12 wherein the identifying means (40) comprises a biometric scanning device.

10 14. The system of claim 13 wherein the identifying means comprises a password.

15 15. A method for preventing the unauthorized use of a device (12) comprising the steps of:
providing a device (12) to an authorized user for performing one or more transactions;
providing means to activate the device (12);
detecting (130) whether the authorized user has retained possession of the device (12); and
20 selectively (145) allowing the performance of the transactions depending on whether the authorized user has retained possession of the device (12).

16. A method for preventing unauthorized remote gaming activities comprising the steps of:
25 providing a device (12) to an authorized user for performing gaming activities;

providing means to activate the device (12);
detecting (130) whether the authorized user has retained possession of the
device (12);
selectively (145) allowing the gaming activities to proceed depending on
5 whether the authorized user has retained possession of the device (12).

17. The method of claim 16 wherein the device (12) is a wireless device.

18. The method of claim 17 wherein the step of detecting (130) whether
10 the authorized user has retained possession of the wireless device (12) comprises
means (80) to determine whether the wireless device (12) has been moved within a
predetermined time period.

19. The method of claim 18 wherein the step of detecting (130) whether
15 the authorized user has retained possession of the wireless device (12) comprises
using a motion sensor.

20. The method of claim 19 wherein the motion sensor comprises a
positively-charged thin foil strip (82) located between a pair of arms (88) of a
20 negatively-charged U-shaped member (86), wherein movement of the wireless device
(12) causes the thin foil strip (82) to contact one of the arms (88) of the U-shaped
member (86) to complete a circuit.

21. The method of claim 20 wherein the step of detecting (130) whether
25 the authorized user has retained possession of the wireless device (12) further

comprises means to determine if the circuit is completed within a predetermined amount of time.

22. The method of claim 17 wherein the step of detecting (130) whether
5 the authorized user has retained possession of the wireless device (12) comprises using a dead man's switch.

23. The method of claim 22 wherein the contact switch comprises a pressure-sensitive band (92) located around the wireless device (12).

10

24. The method of claim 17 wherein the step of detecting (130) whether the authorized user has retained possession of the wireless device (12) comprises using a contact switch.

15 25. The method of claim 17 wherein the step of detecting (130) whether the authorized user has retained possession of the wireless device (12) comprises using a thermal sensor.

26. The method of claim 17 wherein the step of detecting (130) whether
20 the authorized user has retained possession of the wireless device (12) comprises using a capacity sensor.

27. The method of claim 17 wherein the step of detecting (130) whether the authorized user has retained possession of the wireless device (12) comprises
25 means to determine whether the wireless device (12) has been placed on a surface.

28. The method of claim 17 which further comprises the step of verifying (100,140) the authorized use of the wireless device (12) after the wireless device (12) is shut down.

5

29. The method of claim 28 wherein the step of verifying (100,140) the authorized use comprises using a biometric scanner (40).

30. The method of claim 28 wherein the step of verifying (100,140) the
10 authorized user comprises inputting a password.

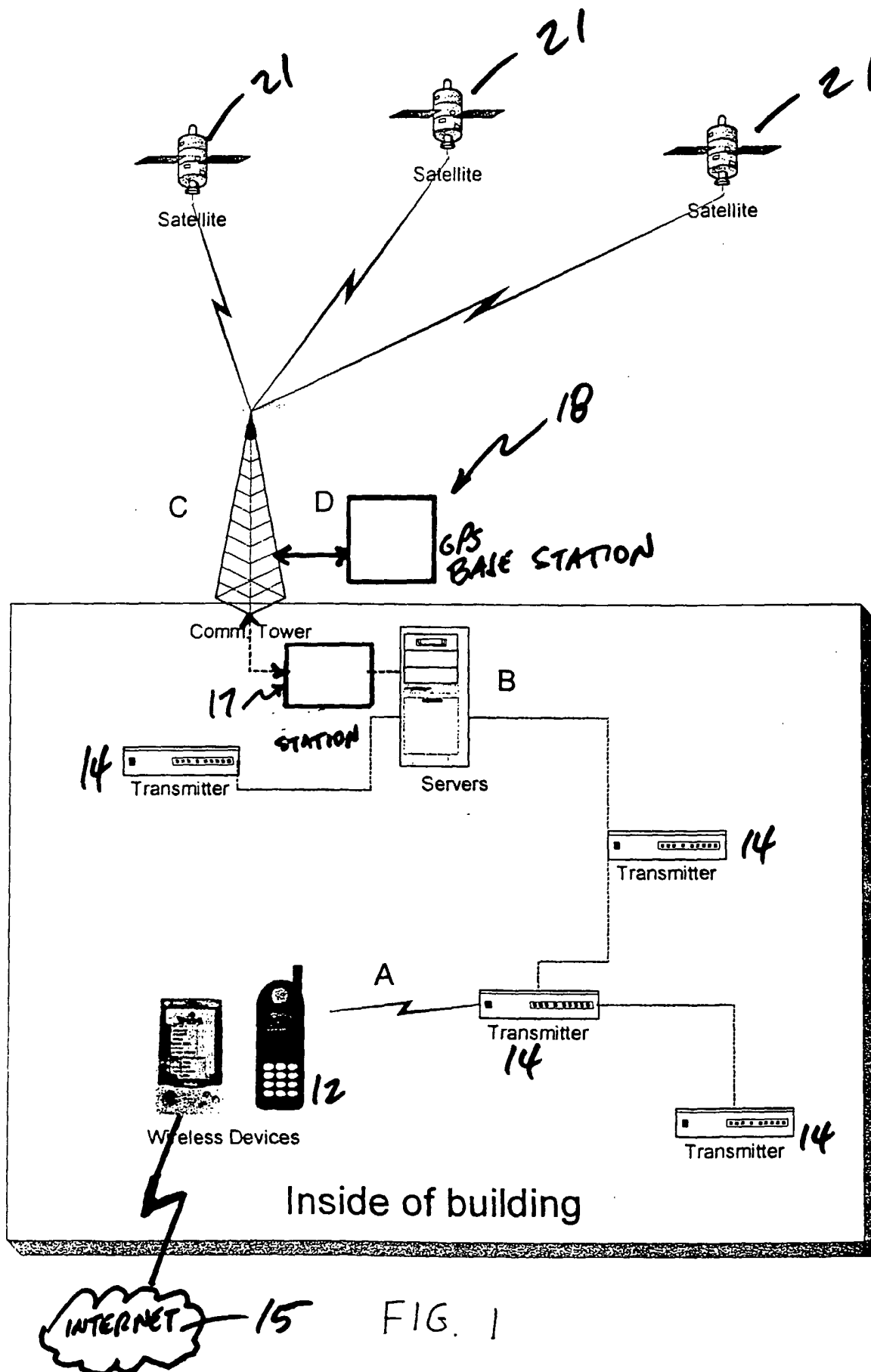
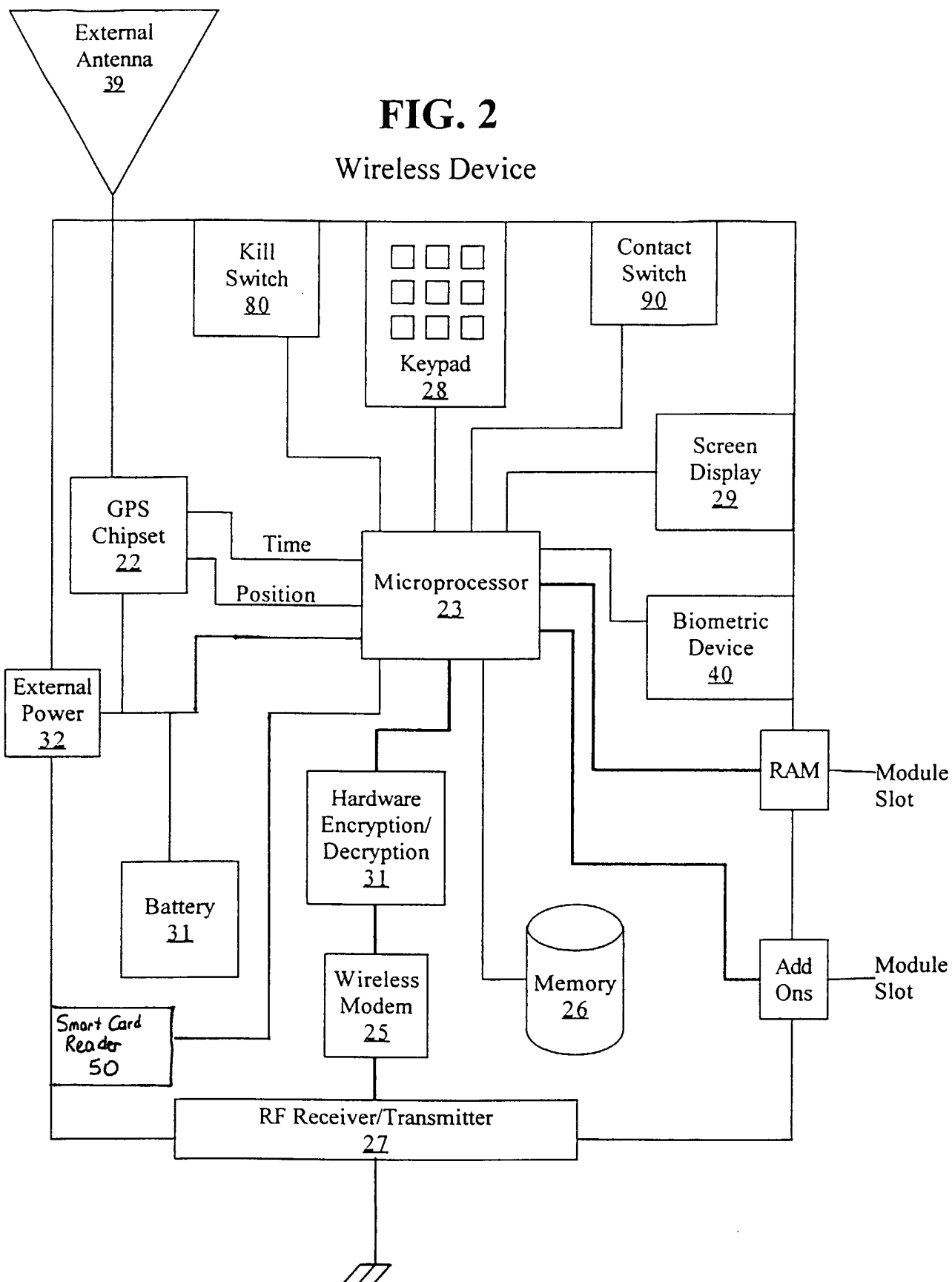


FIG. 1



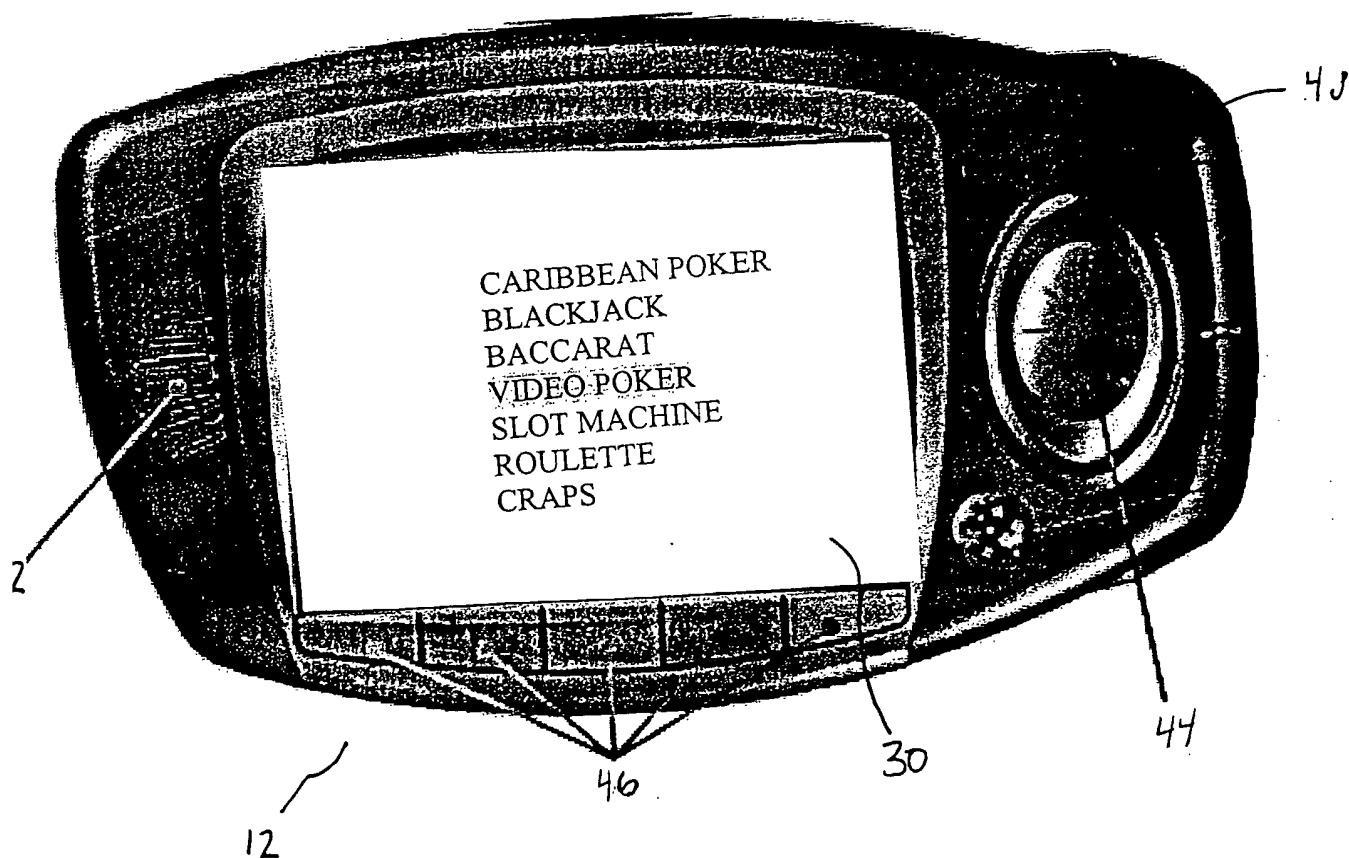


FIG. 3.

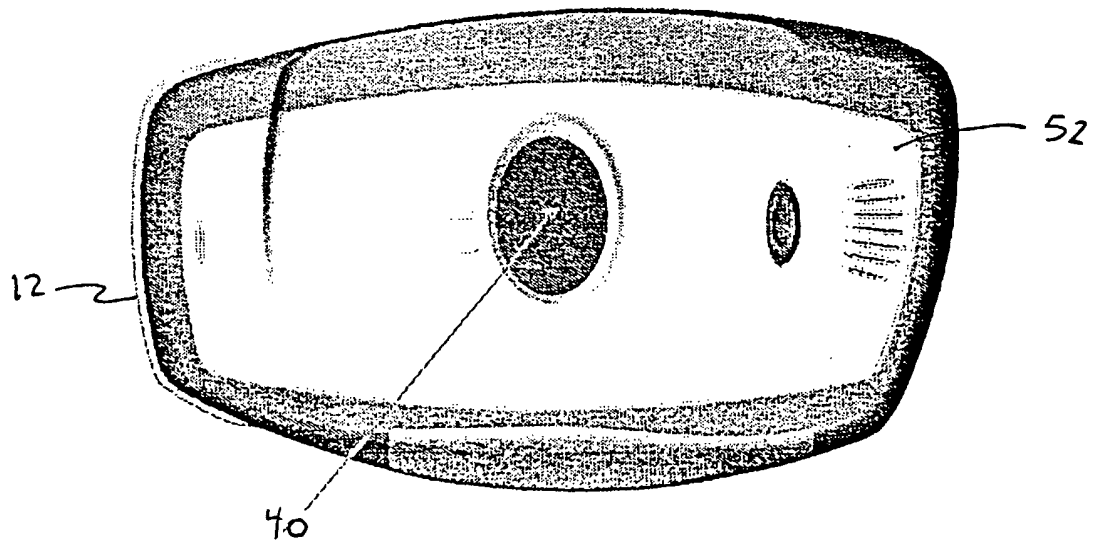


Fig. 4

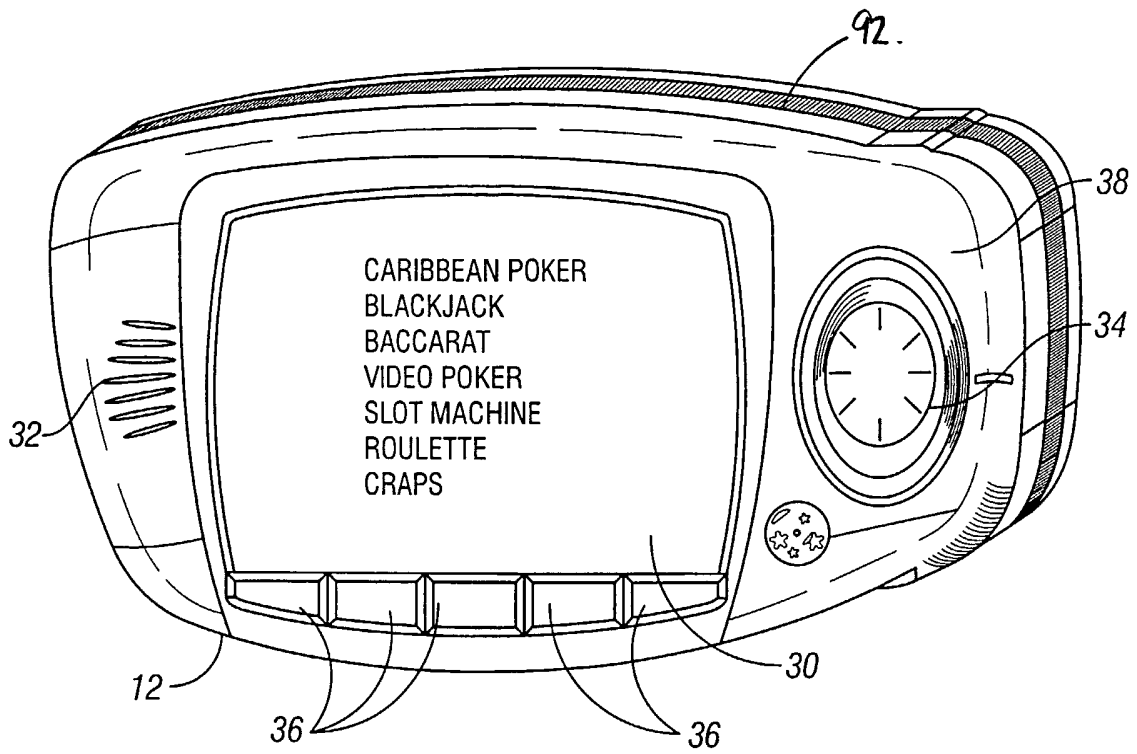


FIG. 6

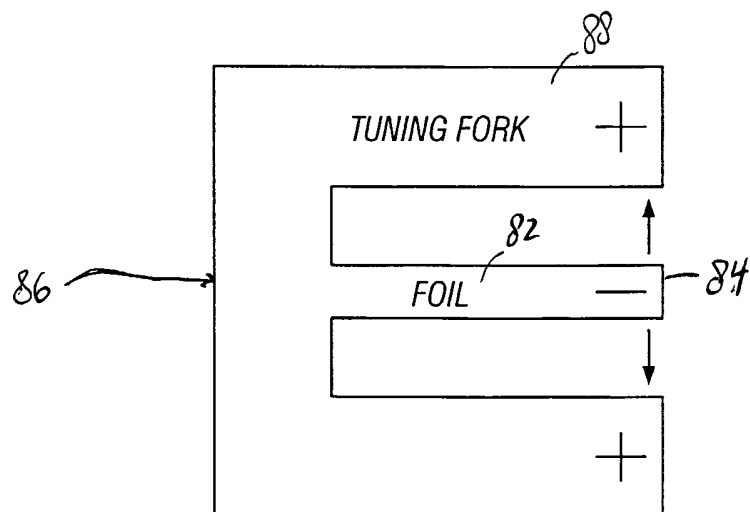


FIG. 5

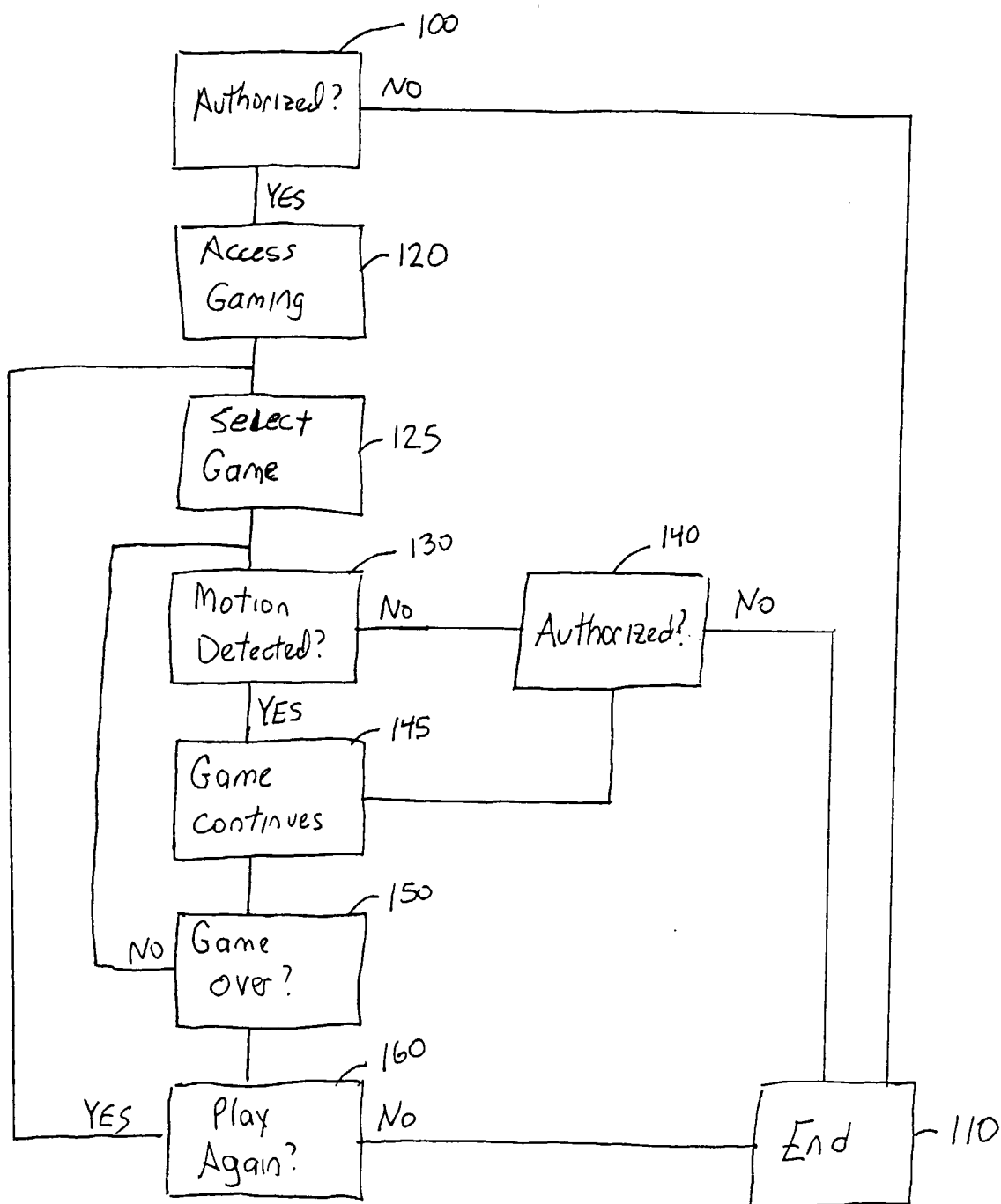


FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/26977

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04Q 7/20

US CL : 455/90, 410, 411, 412, 550, 575; 709/201, 203, 218, 225

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)

U.S. : 455/90, 410, 411, 412, 550, 575; 709/201, 203, 218, 225

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 practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,145,083 A (SHAFFER et al) 07 November 2000, cols. 1, 4 and 5.	1, 15
---		-----
Y		2-4, 9, 12-14, 16-19, 24, and 28-30
Y	US 6,009,458 A (HAWKINS et al) 28 December 1999, cols. 2-4.	2-4, 9, 12-14, 16-19, 24 and 28-30
A	US 5,999,808 A (LADUE) 07 December 1999, see entire reference.	1-30



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 application or patent 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

20 October 2002 (20.10.2002)

Date of mailing of the international search report

03 DEC 2002

Name and mailing address of the ISA/US

Commissioner of Patents and Trademarks

Box PCT

Washington, D.C. 20231

Facsimile No. (703)305-3230

Authorized officer

Nay A. Maungt

Telephone No. 703-308-7745