ADAM K. YOWELL
Nevada Bar No. 11748
Adam.yowell@fisherbroyles.com
FISHERBROYLES, LLP
59 Damonte Ranch Pkwy
Ste B # 508
Reno, NV 89521
Telephone: (775) 230-7364
Counsel for Plaintiff

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

NEXRF Corp., a Nevada Corporation

Plaintiff,

v.

Playtika Ltd., an Israel Corporation, Playtika Holding Corp., a Delaware Corporation, and Caesars Interactive Entertainment LLC, a Delaware LLC,

Defendants.

Case No.: 3:20-cv-603

COMPLAINT FOR PATENT INFRINGEMENT

DEMAND FOR JURY TRIAL

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff NEXRF Corp. ("NEXRF"), a Nevada Limited Liability Company ("Plaintiff") files this Complaint for damages, injunctive relief and demand for a jury trial against Playtika Ltd., Playtika Holding Corp. (collectively "Playtika"), and Caesars Interactive Entertainment, LLC ("CIE"), (collectively "Defendants"), and alleges as follows:

NATURE OF THE CASE

1. NEXRF brings this action against Defendants for infringement of U.S. Patent Nos. 8,747,229 (the '229 patent), 8,506,406 (the '406 patent), 9,646,454 (the '454 patent), 8,506,407 (the '407 patent), and 9,373,116 (the '116 patent) (collectively, the "patents in suit").

BACKGROUND

2. The casino gaming industry has sought to create and encourage new ways for patrons to gamble on casino games. While many patrons enjoyed the experience of playing a real slot machine in front of them, many potential gaming patrons were underserved.

3. One area of interest to the casino industry was remote gaming, where a patron could play a casino game while not physically sitting in front of and interacting with a typical casino gaming device. Examples of prior art devices included systems where a patron would use a handheld device to "play" a casino game by causing a remotely located but otherwise typical slot machine to spin, and the information about the game outcome and the winnings would be communicated to the player through the handheld device. These devices were flawed. For example, they did not have a strict correlation between the actual game outcome and what the player was shown, and additionally required the operation of a physical slot machine as an input.

4. The patents in suit disclose various systems and methods for embodiments of a fully remote, multiplayer capable, secure, and engaging casino-style gaming system. This novel design departed from prior art systems in that it, among other advancements, provided for streamlined media delivery for increased engagement with less resources, increased security to reduce unauthorized use, multiplayer extensibility with improved scaling and reliability, and a flexible infrastructure that could accommodate gambling or social gaming and different types of games.

5. The inventive concepts of the patents in suit were unconventional. At the time of the patents in suit, it was not well-understood, conventional, or routine to have, among other distinctions: 1) a central gaming server that determined game outcome, associated that game outcome with an image ID, and transmitted that image/video and game outcome to a remote device; 2) a verification server coupled with a central gaming server to control access to gaming activities; and, 3) an image and/or video delivery component that included relatively fast memory to store and communicate media associated with recently generated game outcomes. These unconventional centralized server-based elements allowed for a stable, secure, flexible, engaging multiplayer-compatible online gaming experience for the user while minimizing the hardware, storage, and network burdens and requirements on the user's device. This combination of desirable qualities was absent in prior art gaming systems, and providing popular features such as progressive jackpots was made simpler and more flexible by the system of the patents in suit.

6. The '229 patent contains the additional unconventional element of a paytable module associated with the centralized gaming server, which allowed further advantages such as

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

the ability to change game outcome distributions and rewards for all connected devices with any software updates on the device.

7. The '407 patent contains the additional unconventional element of a transactional system that credited funds from winning game outcomes to a user's financial account, which increases security of the system and reduced the amount of processing and network activity required of the user's device and its associated software.

8. The '116 patent contains the additional unconventional elements of location tracking of the user and providing rewards to the user for their historical play, which increase the security of play and engagement of the user with the game.

9. These are just exemplary reasons why the claimed inventions of the patents in suit were not well-understood, routine, or conventional.

10. The value and unconventional nature of the claimed inventions of the patents in suit are further demonstrated by the fact that, despite being described nearly twenty years ago, it is only in the last few years that online mobile gambling and social casino gaming have become wide-spread. In those short recent years, however, both mobile casino gambling and social casino gaming have become massive, multi-billion dollar industries.

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

PARTIES

11. NEXRF Corp. is a Nevada corporation with a principal place of business at 9190 Double Diamond Pkwy, Reno, NV 89521.

12. Defendant Playtika Ltd. is a limited company incorporated and existing under the laws of Israel, with its principal place of business at 8 HaChoshlim Street, Herzliya 4672408, Israel. Playtika Ltd. conducts business throughout Nevada and the United States.

13. Defendant Playtika Holding Corp. is a corporation incorporated and existing under the laws of Delaware, with its principal place of business at 2225 Village Walk Drive #240, Henderson, Nevada 89052. Playtika Holding Corp. conducts business throughout Nevada and the United States.

14. Defendant Caesars Interactive Entertainment, LLC is a limited liability company organized and existing under the laws of Delaware, with its principal place of business at One

Caesars Palace Drive, Las Vegas, Nevada 89109. Caesars Interactive conducts business throughout Nevada and the United States.

JURISDICTION AND VENUE

15. This is a civil action seeking damages and injunctive relief for patent infringement under the patent laws of the United States, Title 35 of the United States Code. This Court has exclusive subject matter jurisdiction over this Complaint pursuant to 28 U.S.C. Sections 1331 and 1338(a).

16. This Court has personal jurisdiction over Playtika Ltd. Playtika Ltd. directly and through its agents regularly does, solicits, and transacts business in the State of Nevada, including making available the Accused Games (defined below) and related conduct and transactions with co-defendants Playtika Holding Corp. and CIE. Those acts have caused and continue to cause injury to NEXRF.

17. This Court has personal jurisdiction over defendants Playtika Holding Corp. and CIE. Each of these entities has its principal place of business in Nevada, and directly and through its agents regularly does, solicits, and transacts business in the State of Nevada. Those acts have caused injury to NEXRF.

18. Venue is proper in this District under 28 U.S.C. Sections 1391 and 1400(b). Playtika Ltd. is a foreign corporation, and both Playtika Holding Corp and CIE have regular and established places of business in this District. Playtika Holding Corp. has its principal place of business at 2225 Village Walk Drive #240, Henderson, Nevada 89052. CIE has its principal place of business at One Caesars Palace Drive, Las Vegas, Nevada 89109. Defendants have also committed acts of infringement in this district by selling, using, and/or offering for sale the Accused Games in this District.

JOINDER

19. In 2011, CIE purchased Playtika Ltd.,[1] and owned and operated Playtika Ltd. for several years until it sold Playtika Ltd. to a Chinese entity, Giant Interactive Group.[2] The 2016

[1] *Caesars Acquires Israel's Playtika*, Global Gaming Business, https://ggbmagazine.com/article/caesars-acquires-israels-playtika/ (last visited 10/20/2020).

[2] *China's Giant leads consortium to buy Playtika for $4.4 billion*, Game Beat,

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

sale of Playtika did not include the World Series of Poker game or the real-money online gaming business.[3]

20. Playtika has continued to operate CIE-branded games, such as Caesars Casino.[4] The Caesars Rewards program is still associated with other Playtika games, such as Slotomania and Bingo Blitz.[5]

21. Playtika and CIE's ongoing relationship relating to many of the Accused Games means that the use of those same games amounts to a single transaction or occurrence as between Defendants. Defendants have been and are acting in concert, and are liable jointly, severally, or otherwise for a right to relief related to or arising out of the same transaction, occurrence, or series of transactions or occurrences related to the making, using, importing into the United States, offering for sale or selling the infringing products in this District. This action involves questions of law and fact that are common to all Defendants.

22. Joinder of all Defendants is proper under 35 U.S.C. Section 299(a)(1) & (2).

DEFENDANTS' INFRINGEMENT OF NEXRF'S INTELLECTUAL PROPERTY

23. The recent ubiquity of internet-connected personal devices combined with the unprecedented consequences of the current global pandemic have created a perfect storm for online real-money gambling and social free-to-play gaming.

24. Online real-money gaming was recently legalized in a few states, and allows users to wager real money in an online environment similar to a real casino. Online real-money games are associated with a real casino and provide the closest virtual alternative to the physical play of a slot machine in a casino. In the second quarter of 2020 alone, the online casino gambling games market in the US generated over $400 million in revenue.[6]

25. Despite the name, "free-to-play" social casino games are enormously lucrative.

---

https://venturebeat.com/2016/07/30/chinas-giant-leads-consortium-to-buy-playtika-for-4-4-billion/ (last visited 10/20/2020).

[3] *Id.*

[4] *Google Play Store page for Caesars Casino: Free Slots Games*, https://play.google.com/store/apps/details?id=com.playtika.caesarscasino&hl=en_US (last visited 10/20/2020).

[5] *Caesars Play Online*, https://www.caesars.com/play (last visited 10/20/2020).

[6] *Online poker and casino games have tripled their revenue from last year as real-world casinos shut their doors*, Business Insider, https://www.businessinsider.com/online-poker-casino-games-business-triple-as-casinos-close-2020-8 (last visited 10/20/2020).

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

While the download of the game is free, thousands of "in-app" items range in price from a few cents to hundreds of dollars. These in-app purchases are often subject to heavy discounts in flash sales and are constantly presented to the player. Defendant Playtika alone generated $425 million in revenue in the first quarter of 2020.[7] Total revenue for the social casino market are projected to be approximately $6 billion in 2020. *Id.*

26. Defendants provided games in both the real-money and social categories. In the real money category, Defendants have at least the Caesars Casino and Sports App. The Caesars Casino and Sports App is made available to the public at least through the iOS App Store[8] and the Caesars Casino website.[9] The Caesars Casino website includes instructions for the download, installation, and account creation steps for the user.[10]

27. The use, operation, and distribution of the Caesars Casino and Sports App is representative of Defendants' real money online slot games, which are collectively referred to as the "Accused Gambling Games." "Accused Gambling Games" includes the game application and the infrastructure necessary to operate the game, such as game servers.

28. In the social casino games category, Defendants are some of the leading game publishers. Playtika claims over 280,000,000 installations of its Social Casino Games.[11] CIE also claims to be a "leading provider of social slots games for players on iOS and Android devices."[12] Exemplary social casino games from Defendants include Slotomania, Caesars Casino: Free Slots Games, and Vegas Downtown Slots – Slot Machines & Word Games. The use, operation, and distribution of these exemplar apps is representative of Defendants' social casino slot games, which are collectively referred to as the "Accused Social Games." "Accused Social Games" includes the game application and the infrastructure necessary to operate the game, such as game servers. The Accused Gambling Games and the Accused Social Games are, collectively, the

[7] *No slots, no problem: Social gaming steps in to fill the empty space*, CDC Gaming Reports, https://www.cdcgamingreports.com/commentaries/no-slots-no-problem-social-gaming-steps-in-to-fill-the-empty-space/ (last visited 10/20/2020).
[8] https://apps.apple.com/us/app/caesars-casino-sportsbook-nj/id876336616 (last visited 10/20/2020).
[9] https://www.caesarscasino.com/ (last visited 10/20/2020).
[10] https://www.caesarscasino.com/p/mobile-casino/ (last visited 10/20/2020).
[11] https://play.google.com/store/apps/dev?id=8370476508159322879&hl=en&gl=US (last visited 10/20/2020).
[12] https://www.caesarsgames.com/2018/08/30/can-you-win-real-money-on-slot-apps/ (last visited 10/20/2020).

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

"Accused Games."

COUNT I – INFRINGEMENT OF U.S. PATENT NO. 8,747,229

(Against all Defendants)

29. Paragraphs 1 through 28 are incorporated herein by reference.

30. U.S. Patent No. 8,747,229, titled "Gaming System Network and Method for Delivering Gaming Media," was duly and lawfully issued by the United States Patent and Trademark Office on June 10, 2014. A true and correct copy of the '229 patent is attached as Exhibit 1.

31. NEXRF is the owner by assignment of all rights, title, and interest in the '229 patent, including the right to bring this suit for past and future damages and/or injunctive relief.

32. The '229 patent is valid and enforceable.

33. Defendants infringe one or more claims of the '229 patent, including but not limited to claim 1, directly and/or indirectly via induced infringement and/or contributory infringement. Defendants infringe the asserted claims of the '229 patent by making, using, importing, selling for importation, and/or selling after importation into the United States at least the Accused Games in violation of 35 U.S.C. Section 271(a)-(b). The Accused Games satisfy all limitations of the asserted claims of the '229 patent at least when the respective game is made available for download and play by a user, or after being installed by a user, or after being installed and played by a user.

34. Defendants had actual knowledge of the '229 patent or were willfully blind to its existence and their infringement no later than the filing of this action. Defendants' ongoing infringement is willful and deliberate, entitling NEXRF to enhanced damages.

35. Defendants directly infringe the asserted claims of the '229 patent by making, using, offering to sell, or selling the Accused Games in the United States in violation of 35 U.S.C. Section 271(a). Claim 1 of the '229 patent is exemplary and recites:

> 1. A gaming server system configured to communicate with at least one network access device communicatively coupled to a network, the gaming server system comprising:
>
> a verification system configured to access a registration database having a plurality of registration data associated with each registered user;
>
> a memory module configured to store a plurality of images corresponding to at least one game outcome that are communicated to the at least one network access device;

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

a centralized gaming server communicatively coupled to each of the at least one network access device, the centralized gaming server configured to generate at least one random game outcome by random generation at the centralized gaming server;

a paytable module associated with the centralized gaming server, the paytable module configured to determine one or more prizes associated with a game outcome; and

the centralized gaming server configured to access the memory module and communicate the plurality of images corresponding to the at least one random game outcome to the at least one network access device.

36. Defendants infringe claim 1 for at least the following reasons:

37. To the extent the preamble is limiting, the Accused Games comprise a gaming server system configured to communicate with at least one network access device communicatively coupled to a network.

38. On information and belief, the Accused Games include a verification system configured to access a registration database having a plurality of registration data associated with each registered user. The Accused Games allow and/or require a user to register for a user account, which includes the transmission of registration that may include the player's name, user name, password, Facebook account, and/or other registration data. The Accused Gambling Games also require more substantive registration data to comply with online gambling regulations. The user registration data is stored in a database in a verification system such that the registration data is associated with the registered user.

39. On information and belief, the Accused Games include a memory configured to store a plurality of images corresponding to at least one game outcome that are communicated to the at least one network access device. For example, the Accused Games display celebration graphics and text and/or the display of the slot machine reels when the player achieves certain winning outcomes, such as a winning slot machine spin. At least some of those images are transmitted to the user device over normal internet protocols after the particular game is installed.

40. On information and belief, the Accused Games include a centralized gaming server communicatively coupled to each of the at least one network access device, the centralized gaming server configured to generate at least one random game outcome by random generation at the centralized gaming server. For example, the Accused Games include one or more servers that players connect to in order to play the games, and which generate at least some game outcomes

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

for players playing the game. These game outcomes are generated using a random number generator ("RNG"). For the Accused Gambling Games, the RNG game outcome determination is required by regulations to be conducted at a centralized server.

41. On information and belief, the Accused Games include a paytable module associated with the centralized gaming server, the paytable module configured to determine one or more prizes associated with a game outcome. For example, each slot skin playable on an Accused Game has a paytable, and those paytables can often be displayed to the user if the user performs certain commands. These paytables comprise a matrix of game outcomes, such as slot reel positions, and the resulting prize, such as a multiple of a bet, a jackpot, free spins, a bonus game, or nothing.

42. On information and belief, the centralized gaming server(s) of the Accused Games are configured to access the memory module and communicate the plurality of images corresponding to the at least one random game outcome to the at least one network access device. For example, the mobile application for the particular Accused Game is first downloaded from the appropriate mobile application store, such as the Apple App Store or Google Play. However, after the mobile app is downloaded and installed, additional graphical assets are downloaded for display to the player, including some that are downloaded contemporaneously with play. At least some of these post-install graphical assets are communicated to the user device from the centralized gaming server(s).NEXRF has and continues to be damaged by the Defendants' infringement of the '229 patent.

COUNT II – INFRINGEMENT OF U.S. PATENT NO. 8,506,406

(Against all Defendants)

43. Paragraphs 1 through 42 are incorporated herein by reference.

44. U.S. Patent No. 8,506,406, titled "Network Access Device and Method to Run a Game Application," was duly and lawfully issued by the United States Patent and Trademark Office on August 13, 2013. A true and correct copy of the '406 patent is attached as Exhibit 2.

45. NEXRF is the owner by assignment of all rights, title, and interest in the '406 patent, including the right to bring this suit for past and future damages and/or injunctive relief.

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

46. The '406 patent is valid and enforceable.

47. Defendants infringe one or more claims of the '406 patent, including but not limited to claim 1, directly and/or indirectly via induced infringement and/or contributory infringement. Defendants infringe the asserted claims of the '406 patent by making, using, importing, selling for importation, and/or selling after importation into the United States at least the Accused Games in violation of 35 U.S.C. Section 271(a)-(b). The Accused Games satisfy all limitations of the asserted claims of the '406 patent at least when the respective game is made available for download and play by a user, or after being installed by a user, or after being installed and played by a user.

48. Defendants had actual knowledge of the '406 patent or were willfully blind to its existence and their infringement no later than the filing of this action. Defendants' ongoing infringement is willful and deliberate, entitling NEXRF to enhanced damages.

49. Defendants directly infringe the asserted claims of the '406 patent by making, using, offering to sell, or selling the Accused Games in the United States in violation of 35 U.S.C. Section 271(a). Defendants directly infringe the asserted claims of the '406 patent, at minimum, through use of the system for testing. Claim 1 of the '406 patent is exemplary and recites:

> 1. A system to run a gaming application on a network access device, comprising:
> the network access device; and
> a remote gaming system including a verification system;
> the network access device configured to transmit user identification information and security information to the verification system;
> the network access device configured to receive an acknowledgement from the verification system indicating that the user identification information and security information are valid;
> the network access device configured to receive a game input from a user of the network access device and transmit the game input to the remote gaming system;
> the remote gaming system configured to receive the game input and generate a random game output, the remote gaming system further configured to associate an image ID with the random game output and select one or more images associated with the image ID for encoding and broadcasting to the network access device;
> the network access device configured to receive a plurality of broadcast images generated by the remote gaming system.

50. Defendants infringe claim 1 for at least the following reasons:

51. To the extent the preamble is limiting, the Accused Games as operated include a system to run a gaming application on a network access device.

52. On information and belief, the Accused Games, in operation, include a network access device such as a phone or laptop.

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

53. On information and belief, the Accused Games include a remote gaming system including a verification system. For example, the Accused Games allow and/or require a user to register for a user account and log into a central gaming server system in order to play the games.

54. On information and belief, the Accused Games include that the network access device is configured to transmit user identification information and security information to the verification system. For example, the Accused Games when operated on a user device collect and transmit registration data that may include the player's name, user name, password, and other registration data to the verification system.

55. On information and belief, the Accused Games include that the network access device is configured to receive an acknowledgement from the verification system indicating that the user identification information and security information are valid. For example, the verification system of the central gaming server system sends a message to the Accused Game application running on a user device that the login information is verified, and the login is allowed to complete and the user to play the game.

56. On information and belief, the Accused Games include that the network access device is configured to receive a game input from the user and transmit the game input to the remote gaming system. For example, an Accused Game on a user device will receive an input, such as a touch input, of a user selecting an action, such as touching or clicking the spin button in the game. This input is then transmitted by the Accused Game application to the remote gaming server system and the inputted command is executed, such as by initiating the play of the game.

57. On information and belief, the Accused Games include that the remote gaming system is configured to receive the game input and generate a random game output, the remote gaming system further configured to associate an image ID with the random game output and select one or more images associated with the image ID for encoding and broadcasting to the network access device. For example, the Accused Games include one or more servers that players connect to in order to play the games, and which generate at least some game outcomes for players playing the game. These game outcomes will be generated after the player initiates play, which is communicated to the gaming server from the Accused Game application running on the user

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

device. These game outcomes are generated using a RNG. For the Accused Gambling Games, the RNG game outcome determination is required by regulations to be conducted at a centralized server. The central gaming server system further associates the generated game outcome with an image ID, such as a celebratory graphic for a winning spin, or the icons on the virtual slot reels. These images are then encoded and transmitted to the user device over the internet.

58. On information and belief, the Accused Games include that the network access device is configured to receive a plurality of broadcast images generated by the remote gaming system. The Accused Game application running on the user device includes instructions sufficient for the user device to be configured to receive the broadcast images from the central gaming server system and display one or more of those images to the user.

59. Defendants directly infringe the asserted claims of the '406 patent because they use the system as a whole and put it into service. Defendants or their agents supply every component of the system except the user device, to the extent that is a required element of an asserted claim. Further, Defendants' applications on a user device control all claimed components, configurations, functions, and processes, which constitutes sufficient control over the user device.

60. In addition, Defendants are vicariously liable for the actions of its customers because the only action required of a user is to play the Accused Game. Defendants condition the benefits of playing the game upon the act of the player to actually play the game. In other words, the player can never win if they do not play. Further, Defendants exercise the requisite control over the manner and/or timing of the user's actions as it relates to the user's network access device. Specifically, the player cannot play the game without running Defendants' application, and further restrictions exist such as the requirement of an internet connection to Defendants' servers, logging in to a user account, and other restrictions. This is particularly apparent for the Accused Gambling Games, as gaming regulations require additional controls such as geofencing.

61. Additionally or alternatively, Defendants indirectly infringe the asserted claims of the '406 patent through its users' actions. Defendants contributorily infringe the asserted claims of the '406 patent by making available for use the Accused Games, knowing the same to be especially made or especially adapted for use in infringing the '406 patent, and not a staple article

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

or commodity of commerce suitable for substantial noninfringing use. The play of the Accused Game is an act of infringement, and so the Accused Games are not staple articles of commerce or otherwise capable of substantial noninfringing use.

62. Additionally or alternatively, Defendants actively, knowingly, and intentionally induce the infringement of the asserted claims of the '406 patent by actively encouraging its users to use the Accused Games by playing them. Defendants know, at least as of the date of this Complaint, that their actions will induce users of the Accused Games to directly infringe the asserted claims of the '406 patent. Those users then directly infringe the asserted claims of the '406 patent. For example, Defendants provide instructions to users on how to access the Accused Games and play the Accused Games and otherwise instructing and encouraging players to play the Accused Games, an act which directly infringes the asserted claims of the '406 patent.[13]

63. NEXRF has and continues to be damaged by the Defendants' infringement of the '406 patent.

COUNT III – INFRINGEMENT OF U.S. PATENT NO. 9,646,454

(Against all Defendants)

64. Paragraphs 1 through 63 are incorporated herein by reference.

65. U.S. Patent No. 9,646,454, titled "Networked Gaming System and Method," was duly and lawfully issued by the United States Patent and Trademark Office on May 9, 2017. A true and correct copy of the '454 patent is attached as Exhibit 3.

66. NEXRF is the owner by assignment of all rights, title, and interest in the '454 patent, including the right to bring this suit for past and future damages and/or injunctive relief.

67. The '454 patent is valid and enforceable.

68. Defendants infringe one or more claims of the '454 patent, including but not limited to claim 1, directly and/or indirectly via induced infringement and/or contributory infringement. Defendants infringe the asserted claims of the '454 patent by making, using, importing, selling for importation, and/or selling after importation into the United States at least the Accused Games in

[13] *See, e.g., Guide for How to Play Free Slots Online*, https://www.caesarsgames.com/free-slot-games/ (last visited 10/20/2020), attached as Exhibit 6; *Slotomania: How to Play Slots* https://www.slotomania.com/how-to-play/ (last visited 10/20/2020), attached as Exhibit 7.

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

violation of 35 U.S.C. Section 271(a)-(b). The Accused Games satisfy all limitations of the asserted claims of the '454 patent at least when the respective game is made available for download and play by a user, or after being installed by a user, or after being installed and played by a user.

69. Defendants had actual knowledge of the '454 patent or were willfully blind to its existence and their infringement no later than the filing of this action. Defendants' ongoing infringement is willful and deliberate, entitling NEXRF to enhanced damages.

70. Defendants directly infringe the asserted claims of the '454 patent by making, using, offering to sell, or selling the Accused Games in the United States in violation of 35 U.S.C. Section 271(a). Claim 1 of the '454 patent is exemplary and recites:

> 1. A networked gaming system comprising:
>
> a user identification received by at least one network access device that is compared with registration data in a registration database, wherein a player is provided access to a game when the user identification matches the registered player data;
>
> a transactional component that charges the registered player at least one credit for a game outcome;
>
> a centralized networked gaming module that performs game operations and generates at least one random game output by random generation at the networked gaming module;
>
> the networked gaming module associates the at least one random game output with an image ID; and
>
> the networked gaming module communicates one or more images corresponding to the image ID to the network access device.

71. Defendants infringe claim 1 for at least the following reasons:

72. To the extent the preamble is limiting, the Accused Games comprise a networked gaming system.

73. On information and belief, the Accused Games include a user identification received by at least one network access device that is compared with registration data in a registration database, wherein a player is provided access to a game when the user identification matches the registered player data. For example, the Accused Games allow or require a user to log onto the game by providing a username and password, a Facebook account, or similar. This constitutes user identification information that is compared by the game system to the database of registered users, and when an appropriate match is found the player is allowed to log in and access the game.

74. On information and belief, the Accused Games include a transactional component

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

that charges the registered player at least one credit for a game outcome. For example, the Accused Games that include a slot embodiment require a credit wager of some amount, which is often selectable within a range by the player. These credits may represent actual currency or not, depending on the particular game. Once the slot machine reel is spun and so the game initiated, the initial wager of credit(s) is deducted from the player's store of credits.

75. On information and belief, the Accused Games include a centralized networked gaming module that performs game operations and generates at least one random game output by random generation at the networked gaming module. For example, the Accused Games include one or more servers that players connect to in order to play the games, and which generate at least some game outcomes for players playing the game. These game outcomes are generated using a RNG. For the Accused Gambling Games, the RNG game outcome determination is required by regulations to be conducted at a centralized server.

76. On information and belief, the Accused Games' centralized networked gaming module further associates the at least one random game output with an image ID. For example, in the Accused Games a winning game outcome will have celebratory graphic media for display to the player. The appropriate celebratory graphic media is associated to the game outcome by the centralized gaming server of the Accused Games.

77. On information and belief, the Accused Games' networked gaming module communicates one or more images corresponding to the image ID to the network access device. For example, the Accused Games transmit the appropriate celebratory graphic media for the particular game outcome to the player's device over normal internet protocols.

78. Defendants directly infringe the asserted claims of the '454 patent because they use the system as a whole and put it into service. Defendants or their agents supply every component of the system except the user device, to the extent that is a required element of an asserted claim. Further, Defendants' applications on a user device control all claimed components, configurations, functions, and processes, which constitutes sufficient control over the user device.

79. In addition, Defendants are vicariously liable for the actions of its customers because the only action required of a user is to play the Accused Game. Defendants condition the

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

benefits of playing the game upon the act of the player to actually play the game. In other words, the player can never win if they do not play. Further, Defendants exercise the requisite control over the manner and/or timing of the user's actions as it relates to the user's network access device. Specifically, the player cannot play the game without running Defendants' application, and further restrictions exist such as the requirement of an internet connection to Defendants' servers, logging in to a user account, and other restrictions. This is particularly apparent for the Accused Gambling Games, as gaming regulations require additional controls such as geofencing.

80. Additionally or alternatively, Defendants indirectly infringe the asserted claims of the '454 patent through its users' actions. Defendants contributorily infringe the asserted claims of the '454 patent by making available for use the Accused Games, knowing the same to be especially made or especially adapted for use in infringing the '454 patent, and not a staple article or commodity of commerce suitable for substantial noninfringing use. The play of the Accused Game is an act of infringement, and so the Accused Games are not staple articles of commerce or otherwise capable of substantial noninfringing use.

81. Additionally or alternatively, Defendants actively, knowingly, and intentionally induce the infringement of the asserted claims of the '454 patent by actively encouraging its users to use the Accused Games by playing them. Defendants know, at least as of the date of this Complaint, that their actions will induce users of the Accused Games to directly infringe the asserted claims of the '454 patent. Those users then directly infringe the asserted claims of the '454 patent. For example, Defendants provide instructions to users on how to access the Accused Games and play the Accused Games and otherwise instructing and encouraging players to play the Accused Games, an act which directly infringes the asserted claims of the '454 patent.[14]

82. NEXRF has and continues to be damaged by the Defendants' infringement of the '454 patent.

COUNT IV – INFRINGEMENT OF U.S. PATENT NO. 8,506,407

(Against all Defendants)

83. Paragraphs 1 through 82 are incorporated herein by reference.

[14] Ex. 6; Ex. 7.

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

84. U.S. Patent No. 8,506,407, titled "Gaming System Network and Method for Delivering Gaming Media," was duly and lawfully issued by the United States Patent and Trademark Office on August 13, 2013. A true and correct copy of the '407 patent is attached as Exhibit 4.

85. NEXRF is the owner by assignment of all rights, title, and interest in the '407 patent, including the right to bring this suit for past and future damages and/or injunctive relief.

86. The '407 patent is valid and enforceable.

87. Defendants infringe one or more claims of the '407 patent, including but not limited to claim 1, directly and/or indirectly via induced infringement and/or contributory infringement. Defendants infringe the asserted claims of the '407 patent by making, using, importing, selling for importation, and/or selling after importation into the United States at least the Accused Gambling Games in violation of 35 U.S.C. Section 271(a)-(b). The Accused Gambling Games satisfy all limitations of the asserted claims of the '407 patent at least when the respective game is made available for download and play by a user, or after being installed by a user, or after being installed and played by a user.

88. Defendants had actual knowledge of the '407 patent or were willfully blind to its existence and their infringement no later than the filing of this action. Defendants' ongoing infringement is willful and deliberate, entitling NEXRF to enhanced damages.

89. Defendants directly infringe the asserted claims of the '407 patent by making, using, offering to sell, or selling the Accused Gambling Games in the United States in violation of 35 U.S.C. Section 271(a). Claim 1 of the '407 patent is exemplary and recites:

> 1. A gaming system network, comprising:
>
> a verification system configured to verify that a user attempting to access the gaming system network is a registered player, the user operating a network access device communicating with the gaming system network;
>
> a gaming system configured to generate at least one random game output, the gaming system configured to associate an image ID with the at least one random game output;
>
> a video server configured to store a plurality of images corresponding to at least one game, the video server configured to retrieve one or more images associated with the image ID, wherein the one or more images are representative of a game output, the video server configured to communicate the one or more images to the network access device; and
>
> a transactional system configured to credit monetary funds to a financial account of the user based on the at least one random game output.

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

90. Defendants infringe claim 1 for at least the following reasons:

91. To the extent the preamble is limiting, the Accused Gambling Games comprise a gaming system network.

92. On information and belief, the Accused Gambling Games include a verification system configured to verify that a user attempting to access the gaming system network is a registered player, the user operating a network access device communicating with the gaming system network. For example, the Accused Gambling Games require a player to create an account and register with the system. In order to play the games, the user must enter verification information on their user device, such as a smartphone, which the Accused Gambling Games verify before allowing play.

93. On information and belief, the Accused Gambling Games include a gaming system configured to generate at least one random game output, the gaming system configured to associate an image ID with the at least one random game output. For example, the Accused Gambling Games include one or more servers that players connect to in order to play the games. These game outcomes are generated using a RNG. The RNG game outcome determination is required by regulations to be conducted at a centralized server for real money gaming applications such as the Accused Gambling Games. Further in the Accused Gambling Games a winning game outcome will have celebratory graphic media for display to the player. The appropriate celebratory graphic media is associated to the game outcome by the centralized gaming server of the Accused Games.

94. On information and belief, the Accused Gambling Games include a video server configured to store a plurality of images corresponding to at least one game, the video server configured to retrieve one or more images associated with the image ID, wherein the one or more images are representative of a game output, the video server configured to communicate the one or more images to the network access device. For example, the Accused Gambling Games' server system includes a component that transmits images and/or video to the player device. These graphics are associated with particular game outcomes, such as a winning spin, a jackpot win, and the like. The Accused Gambling Games' server system is further configured to determine a graphic that is associated with a particular game outcome, retrieve it, prepare it for transmission to

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

the user device, and transmit it to the user device according to normal internet communication protocols.

95. On information and belief, the Accused Gambling Games further include a transactional system configured to credit monetary funds to a financial account of the user based on the at least one random game output. For example, in order to play the games the user first needs a source of funds, which could include linking a credit card or bank account to the user's account. If, during play, the user wins a game and therefore some amount of credits representing monetary value, those monetary funds are then transferred back to the user's financial account, which could be the user's game account, a bank account, or similar, upon cashing out.

96. NEXRF has and continues to be damaged by the Defendants' infringement of the '407 patent.

COUNT V – INFRINGEMENT OF U.S. PATENT NO. 9,373,116

(Against all Defendants)

97. Paragraphs 1 through 96 are incorporated herein by reference.

98. U.S. Patent No. 9,373,116, titled "Player Tracking Using a Wireless Device for a Casino Property," was duly and lawfully issued by the United States Patent and Trademark Office on January 1, 2016. A true and correct copy of the '116 patent is attached as Exhibit 5.

99. NEXRF is the owner by assignment of all rights, title, and interest in the '116 patent, including the right to bring this suit for past and future damages and/or injunctive relief.

100. The '116 patent is valid and enforceable.

101. Defendants infringe one or more claims of the '116 patent, including but not limited to claim 1, directly and/or indirectly via induced infringement and/or contributory infringement. Defendants infringe the asserted claims of the '116 patent by making, using, importing, selling for importation, and/or selling after importation into the United States at least the Accused Gambling Games in violation of 35 U.S.C. Section 271(a)-(b). The Accused Gambling Games satisfy all limitations of the asserted claims of the '116 patent at least when the respective game is made available for download and play by a user, or after being installed by a user, or after being installed and played by a user.

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

102. Defendants had actual knowledge of the '116 patent or were willfully blind to its existence and their infringement no later than the filing of this action. Defendants' ongoing infringement is willful and deliberate, entitling NEXRF to enhanced damages.

103. Defendants directly infringe the asserted claims of the '116 patent by making, using, offering to sell, or selling the Accused Gambling Games in the United States in violation of 35 U.S.C. Section 271(a). Claim 1 of the '116 patent is exemplary and recites:

> 1. An interactive gaming system for a casino property, the interactive gaming system comprising:
>
> a wireless device associated with a registered user, wherein the wireless device is used to determine a location of the registered user and the wireless device communicates with a network using at least one wireless networking protocol;
>
> a verification system that accesses a registration database having registration data associated with each registered user;
>
> a centralized gaming server communicatively coupled to the wireless device, the centralized gaming server generates at least one random game outcome;
>
> a memory module that stores a plurality of images corresponding to the at least one game outcome that are communicated to the wireless device;
>
> the centralized gaming server accesses the memory module and communicates the plurality of images corresponding to the random game outcome to the wireless device; and
>
> a casino player tracking system that includes,
>
> a registered user profile that further includes a plurality of user preferences,
>
> a record of a plurality of accumulated points associated with a betting activity of the registered user, wherein the betting activity is associated with the random outcomes generated by the centralized gaming server,
>
> at least one complimentary good or service corresponding to the accumulated points associated with the registered user; and
>
> a plurality of messages generated by the casino player tracking system for the wireless device regarding the complementary goods or services.

104. Defendants infringe claim 1 for at least the following reasons:

105. To the extent the preamble is limiting, the Accused Gambling Games comprise an interactive gaming system for a casino property.

106. On information and belief, the Accused Gambling Games in operation include a wireless device associated with a registered user, wherein the wireless device is used to determine a location of the registered user and the wireless device communicates with a network using at least one wireless networking protocol. For example, the Accused Gambling Games can be played by a user on their smartphone. Pursuant to regulation, the user device must be able to have its location determined to be within a gaming jurisdiction via geofencing. The user's wireless device communicates with the Accused Gambling Games' server wirelessly, using a standard wireless networking protocol, such as Wi-Fi.

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

107. On information and belief, the Accused Gambling Games include a verification system that accesses a registration database having registration data associated with each registered user. For example, the Accused Gambling Games require a player to create an account and register with the system. In order to play the games, the user must enter verification information on their user device, such as a smartphone, which the Accused Gambling Games verify before allowing play.

108. On information and belief, the Accused Gambling Games include a centralized gaming server communicatively coupled to the wireless device, the centralized gaming server generates at least one random game outcome. For example, the Accused Gambling Games include one or more servers that players connect to via the internet in order to play the games. These game outcomes are generated using a RNG. The RNG game outcome determination is required by regulations to be conducted at a centralized server for real money gaming applications such as the Accused Gambling Games.

109. On information and belief, the Accused Gambling Games' server system includes a memory module that stores a plurality of images corresponding to the at least one game outcome that are communicated to the wireless device. For example, the Accused Gambling Games' server system includes a component that transmits images and/or video to the player device over normal internet protocols. These graphics are stored in the server system's memory module and associated with particular game outcomes, such as a winning spin, a jackpot win, and the like. The Accused Gambling Games' server system is further configured to determine a graphic that is associated with a particular game outcome, retrieve it, prepare it for transmission to the user device, and transmit it to the user device according to normal internet protocols.

110. On information and belief, the Accused Gambling Games' centralized server system accesses the memory module and communicates the plurality of images corresponding to the random game outcomes to the wireless devices. For example, the Accused Gambling Games' server system is configured to determine a graphic that is associated with a particular game outcome, access it at the memory module, prepare it for transmission to the user device, and transmit it to the wireless user device according to normal internet protocols.

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

111. On information and belief, the Accused Gambling Games include a player tracking system. For example, the Caesars Rewards component of the Accused Gambling Games track player activities.

112. On information and belief, the Accused Gambling Games' player tracking system includes a registered user profile that includes a plurality of user preferences. For example, in the Caesars Rewards program user preferences could include payment options, credit lines, links to local casino accounts, reward point swaps, price alerts, and similar.

113. On information and belief, the Accused Gambling Games' player tracking system includes a record of a plurality of accumulated points associated with a betting activity of the registered user, where the betting activity is associated with the random outcomes generated by the centralized gaming server. For example, the Caesars Rewards program tracks player play that includes betting activity in the Accused Gambling Games and assigns reward points based upon that play.

114. On information and belief, the Accused Gambling Games' player tracking system includes providing at least one complimentary good or service corresponding to the accumulated points associated with the registered user. For example, some Caesars Rewards benefits include free hotel stays, a free night in Las Vegas or Atlantic City, a free dinner, free valet parking, and free casino game play. These rewards are associated with various levels of player reward points that the player has accumulated.

115. On information and belief, the Accused Gambling Games' player tracking system includes a plurality of messages generated by the casino player tracking system for the wireless device regarding the complementary goods or services. For example, these messages may include emails, texts, phone notifications, browser notifications, and in-app notifications to the user when a reward is available or redeemed.

116. Defendants directly infringe the asserted claims of the '116 patent because they use the system as a whole and put it into service. Defendants or their agents supply every component of the system except the user device, to the extent that is a required element of an asserted claim. Further, Defendants' applications on a user device control all claimed components, configurations,

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

functions, and processes, which constitutes sufficient control over the user device.

117. In addition, Defendants are vicariously liable for the actions of its customers because the only action required of a user is to play the Accused Gambling Game. Defendants condition the benefits of playing the game upon the act of the player to actually play the game. In other words, the player can never win if they do not play. Further, Defendants exercise the requisite control over the manner and/or timing of the user's actions as it relates to the user's network access device. Specifically, the player cannot play the game without running Defendants' application, and further restrictions exist such as the requirement of an internet connection to Defendants' servers, logging in to a user account, and other restrictions such as geofencing.

118. Additionally or alternatively, Defendants indirectly infringe the asserted claims of the '116 patent through its users' actions. Defendants contributorily infringe the asserted claims of the '116 patent by making available for use the Accused Gambling Games, knowing the same to be especially made or especially adapted for use in infringing the '116 patent, and not a staple article or commodity of commerce suitable for substantial noninfringing use. The play of the Accused Gambling Game is an act of infringement, and so the Accused Gambling Games are not staple articles of commerce or otherwise capable of substantial noninfringing use.

119. Additionally or alternatively, Defendants actively, knowingly, and intentionally induce the infringement of the asserted claims of the '116 patent by actively encouraging its users to use the Accused Games by playing them. Defendants know, at least as of the date of this Complaint, that their actions will induce users of the Accused Gambling Games to directly infringe the asserted claims of the '116 patent. Those users then directly infringe the asserted claims of the '116 patent. For example, Defendants provide instructions to users on how to access the Accused Games and play the Accused Gambling Games and otherwise instructing and encouraging players to play the Accused Gambling Games, an act which directly infringes the asserted claims of the '116 patent.[15]

120. NEXRF has and continues to be damaged by the Defendants' infringement of the '116 patent.

[15] Ex. 6; Ex. 7.

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

PRAYER FOR RELIEF

WHEREFORE, Plaintiff seeks the following relief:

A. Judgment in NEXRF's favor and against Defendants on all causes of action alleged herein;

B. Damages in an amount to be determined at trial, including trebling of all post-filing damages awarded with respect to infringement of the patents in suit;

C. Judgment that this is an exceptional case;

D. Costs of suit incurred herein;

E. Prejudgment interest;

F. Attorneys' fees and costs; and

G. Such other and further relief as the Court may deem to be just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, NEXRF respectfully demands a trial by jury on all issues triable by Jury.

DATED this 26th day of October 2020.

Respectfully submitted,

FISHERBROYLES, LLP

/s/ Adam Yowell

ADAM YOWELL
Nevada Bar No. 11748
59 Damonte Ranch Pkwy
Ste B # 508
Reno, NV 89521
Telephone: (775) 230-7364
Counsel for Plaintiff

FISHERBROYLES, LLP
530 Lytton Avenue, Second Floor
Palo Alto, CA 94301
Telephone: (775) 230-7364

US008747229B2

(12) **United States Patent**
Kerr

(10) **Patent No.: US 8,747,229 B2**
(45) **Date of Patent: *Jun. 10, 2014**

(54) **GAMING SYSTEM NETWORK AND METHOD FOR DELIVERING GAMING MEDIA**

(75) Inventor: **Michael A. Kerr**, Reno, NV (US)

(73) Assignee: **NEXRF, Corp.**, Reno, NV (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 145 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **12/981,403**

(22) Filed: **Dec. 29, 2010**

(65) **Prior Publication Data**

US 2011/0159952 A1 Jun. 30, 2011

Related U.S. Application Data

(63) Continuation of application No. 10/681,034, filed on Oct. 8, 2003, now Pat. No. 8,403,755, which is a continuation of application No. 09/899,559, filed on Jul. 5, 2001, now abandoned.

(60) Provisional application No. 60/266,956, filed on Feb. 6, 2001.

(51) **Int. Cl.**
A63F 9/24 (2006.01)
G07F 17/00 (2006.01)

(52) **U.S. Cl.**
USPC **463/42**; 463/16; 463/25

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,339,798	A	7/1982	Hedges et al.
4,856,787	A	8/1989	Itkis
5,586,937	A	12/1996	Menashe
5,594,491	A	1/1997	Hodge et al.
5,630,757	A	5/1997	Gagin et al.
5,643,086	A	7/1997	Alcorn et al.
5,738,583	A	4/1998	Comas et al.
5,761,416	A	6/1998	Mandal et al.
5,762,552	A	6/1998	Vuong et al.
5,768,382	A	6/1998	Schneier et al.
5,779,545	A	7/1998	Berg et al.
5,800,268	A	9/1998	Molnick

(Continued)

OTHER PUBLICATIONS

"Internet Industry Interacting Gambling Code: A Code for Industry Co-Regulation in the Area of Internet Gambling Content Pursuant to the Requirements of the Interactive Gaming Act of 2001". Internet Industry Association. Dec. 2001.

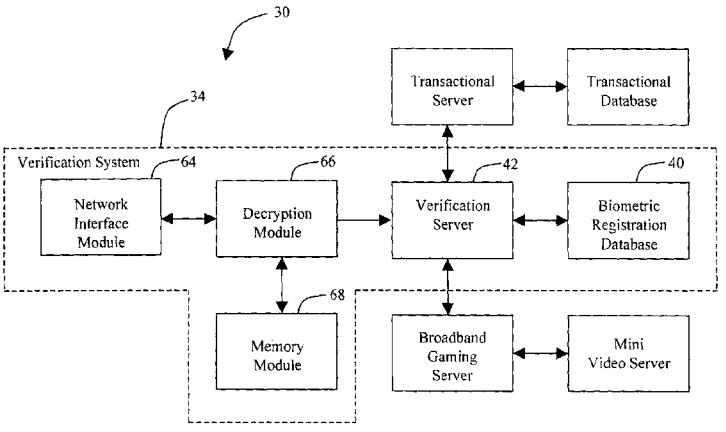
(Continued)

Primary Examiner — Paul A D'Agostino
(74) *Attorney, Agent, or Firm* — Michael A. Kerr; Kerr IP Group, LLC

(57) **ABSTRACT**

A gaming server system is described, the gaming server system including a verification system, a memory module, a centralized gaming server, and a paytable module. The verification system is configured to access a registration database having registration data for registered users. The memory module is configured to store images corresponding to at least one game outcome, with the images communicated to the network access devices. The paytable module is associated with the centralized gaming server, and it is configured to determine one or more prizes associated with a game outcome. The centralized gaming server is configured to generate at least one random game outcome by random generation at the centralized gaming server, and configured to access the memory module and communicate the images corresponding to the random game outcome to the network access devices.

24 Claims, 9 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

5,851,149	A		12/1998	Xidos et al.
5,871,398	A		2/1999	Schneier et al.
5,902,983	A		5/1999	Crevalt et al.
5,971,849	A	*	10/1999	Falciglia 463/16
6,001,016	A	*	12/1999	Walker et al. 463/42
6,010,404	A		1/2000	Walker et al.
6,106,396	A		8/2000	Alcorn et al.
6,142,876	A		11/2000	Cumbers
6,178,510	B1		1/2001	O'Connor et al.
6,409,602	B1		6/2002	Wiltshire et al.
6,500,068	B2		12/2002	Walker et al.
6,508,709	B1	*	1/2003	Karmarkar 463/42
6,508,710	B1		1/2003	Paravia et al.
6,527,638	B1		3/2003	Walker et al.
6,575,834	B1		6/2003	Lindo
6,612,928	B1		9/2003	Bradford et al.
6,628,939	B2		9/2003	Paulsen
6,676,522	B2		1/2004	Rowe
6,682,421	B1		1/2004	Rowe et al.
6,709,333	B1		3/2004	Bradford et al.
6,709,631	B2		3/2004	Mori et al.
6,719,631	B1		4/2004	Tulley et al.
6,749,512	B2		6/2004	MacGregor et al.
6,875,110	B1		4/2005	Crumby
6,884,162	B2		4/2005	Raverdy et al.
6,942,574	B1		9/2005	LeMay et al.
7,107,245	B1	*	9/2006	Kowalick 705/44
7,338,372	B2		3/2008	Morrow et al.
7,341,522	B2		3/2008	Yamagishi
7,534,169	B2		5/2009	Amaitis et al.
7,611,407	B1		11/2009	Itkis et al.
8,029,349	B2		10/2011	Lind
2001/0004768	A1		6/2001	Hodge et al.
2001/0005908	A1		6/2001	Hodge et al.
2002/0002073	A1		1/2002	Montgomery et al.
2002/0007494	A1		1/2002	Hodge
2002/0056125	A1		5/2002	Hodge et al.
2002/0056143	A1		5/2002	Hodge et al.
2002/0077167	A1		6/2002	Merari
2002/0142815	A1		10/2002	Candelore
2002/0142844	A1		10/2002	Kerr
2006/0189382	A1		8/2006	Muir et al.
2007/0087834	A1		4/2007	Moser et al.
2007/0270212	A1		11/2007	Cockerille et al.
2008/0026844	A1		1/2008	Wells
2008/0057894	A1		3/2008	Aleksic et al.
2008/0097858	A1		4/2008	Vucina et al.
2009/0325708	A9	*	12/2009	Kerr 463/42
2011/0159953	A1	*	6/2011	Kerr 463/29
2011/0165936	A1	*	7/2011	Kerr 463/25

OTHER PUBLICATIONS

Wirelss Network. Wikipedia.http://en.wikipedia.org/wiki/Wireless_network. Nov. 17, 2008.

"Tracking Cookie." Wikipedia.http://en.wikipedia.org/wiki/Tracking_cookie. May 24, 2009.

* cited by examiner

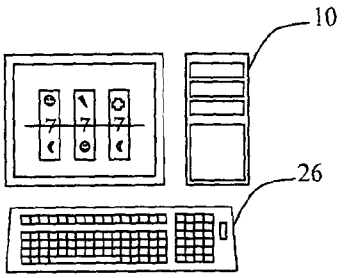


FIG. 1a

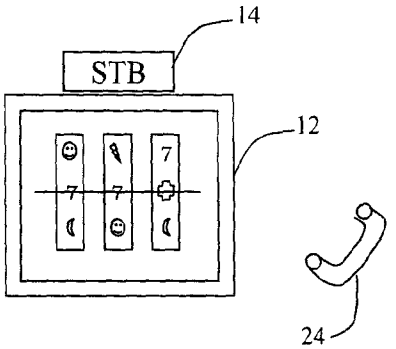


FIG. 1b

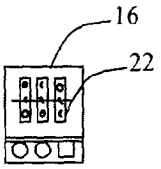


FIG. 1c

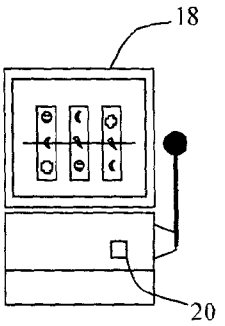
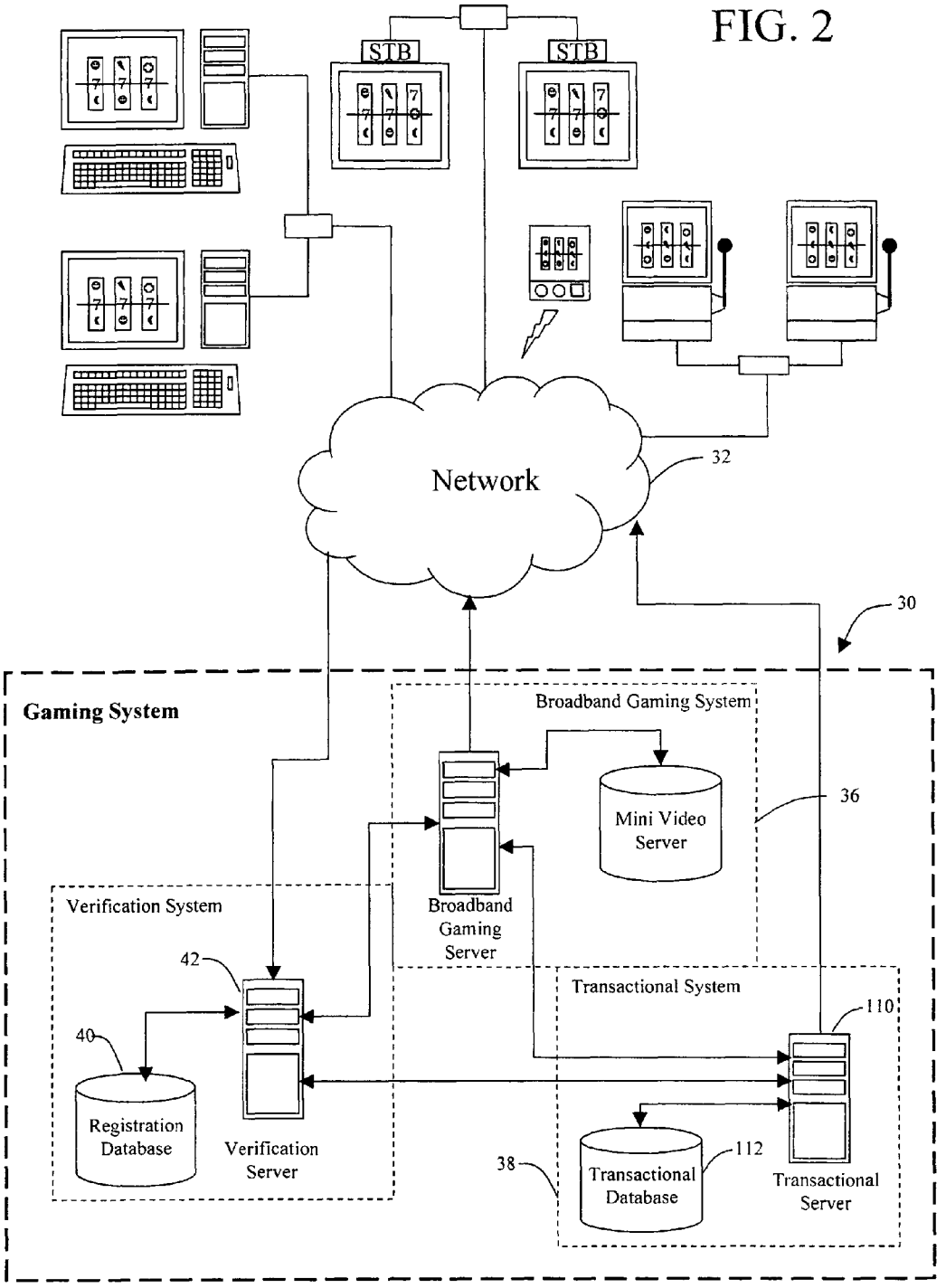


FIG. 1d

FIG. 2


STB
STB
Network
32
30
Gaming System
Broadband Gaming System
Mini Video Server
36
Broadband Gaming Server
Verification System
42
40
Registration Database
Verification Server
Transactional System
110
38
Transactional Database
112
Transactional Server

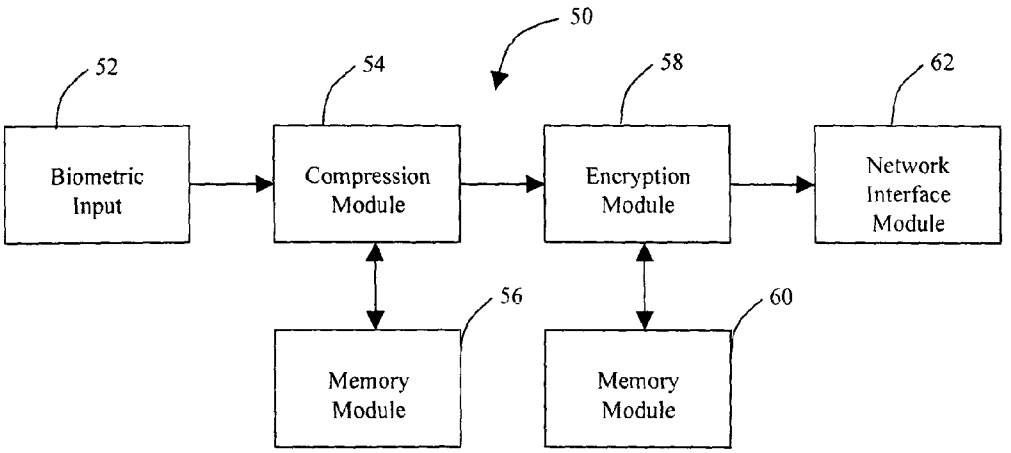

50
52
54
58
62
Biometric Input
Compression Module
Encryption Module
Network Interface Module
56
60
Memory Module
Memory Module

FIG. 3

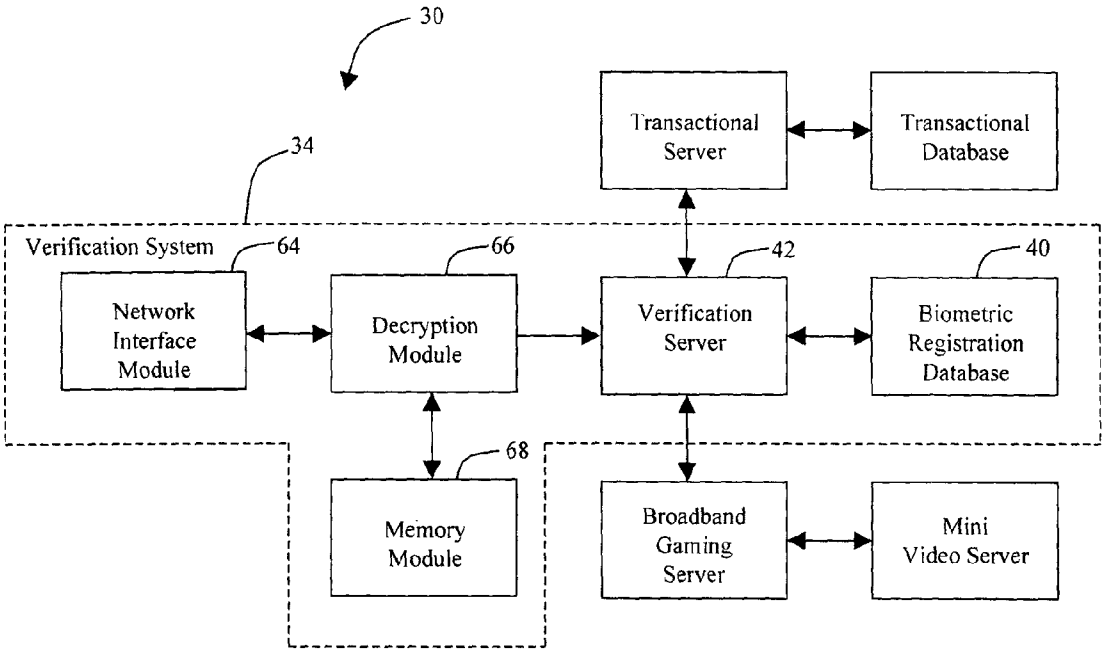

30
34
Transactional Server
Transactional Database
Verification System
64
66
42
40
Network Interface Module
Decryption Module
Verification Server
Biometric Registration Database
68
Memory Module
Broadband Gaming Server
Mini Video Server

FIG. 4

70

REGISTRATION DATA FIELDS	
NAME	BIOMETRIC
ADDRESS	PLAYER ID
USER NAME	MAC ID
PASSWORD	IP ADDRESS
CREDIT CARD	BROWSER
DATE	COOKIES
TIME	CRYPTO KEYS

72

USER SUBMITTED DATA	
NAME	BIOMETRIC
ADDRESS	PLAYER ID
USER NAME	MAC ID
PASSWORD	IP ADDRESS
CREDIT CARD	BROWSER
DATE	COOKIES
TIME	CRYPTO KEYS

FIG. 5

74

PLAYER DATA FIELDS	
PLAYER ID	SESSION TIME FOR TYPE OF GAME
DATE	AMOUNT PLAYED DURING SESSION
TIME IN	CREDIT CARD INFORMATION
TIME OUT	TRANSACTION REQUEST
TYPE GAME	TRANSACTION APPROVAL
CREDITS IN	TRANSFER OF CREDITS
CREDITS OUT	TRANSFER TO PLAYER CREDIT CRD
BONUS	CRYPTO KEYS

FIG. 6

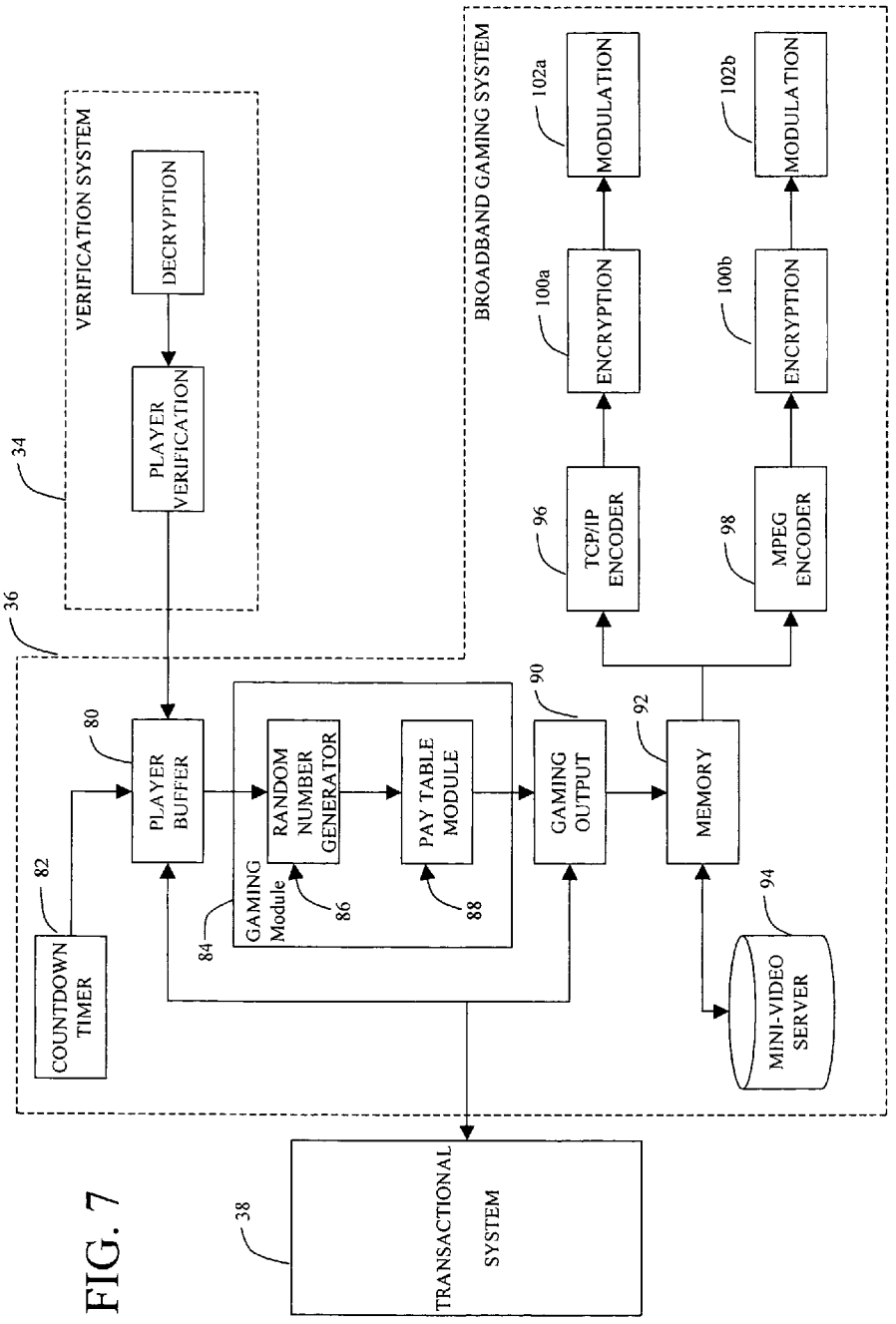

VERIFICATION SYSTEM
DECRYPTION
PLAYER VERIFICATION
34
36
BROADBAND GAMING SYSTEM
102a
MODULATION
102b
MODULATION
100a
ENCRYPTION
100b
ENCRYPTION
96
TCP/IP ENCODER
98
MPEG ENCODER
80
PLAYER BUFFER
RANDOM NUMBER GENERATOR
PAY TABLE MODULE
90
GAMING OUTPUT
92
MEMORY
82
COUNTDOWN TIMER
GAMING Module
84
86
88
94
MINI-VIDEO SERVER
38
TRANSACTIONAL SYSTEM

FIG. 7

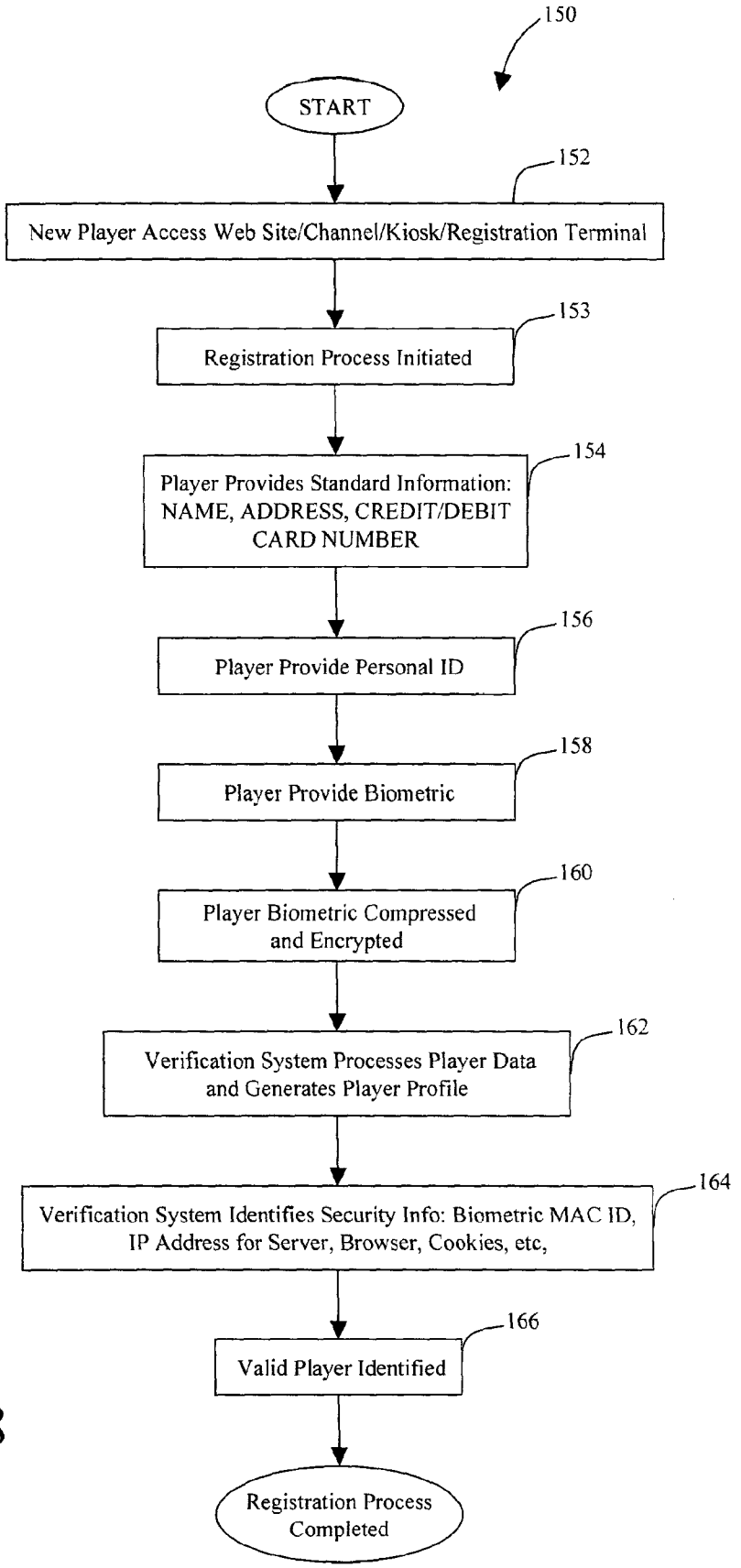

150
START
152
New Player Access Web Site/Channel/Kiosk/Registration Terminal
153
Registration Process Initiated
154
Player Provides Standard Information: NAME, ADDRESS, CREDIT/DEBIT CARD NUMBER
156
Player Provide Personal ID
158
Player Provide Biometric
160
Player Biometric Compressed and Encrypted
162
Verification System Processes Player Data and Generates Player Profile
164
Verification System Identifies Security Info: Biometric MAC ID, IP Address for Server, Browser, Cookies, etc,
166
Valid Player Identified
Registration Process Completed

FIG. 8

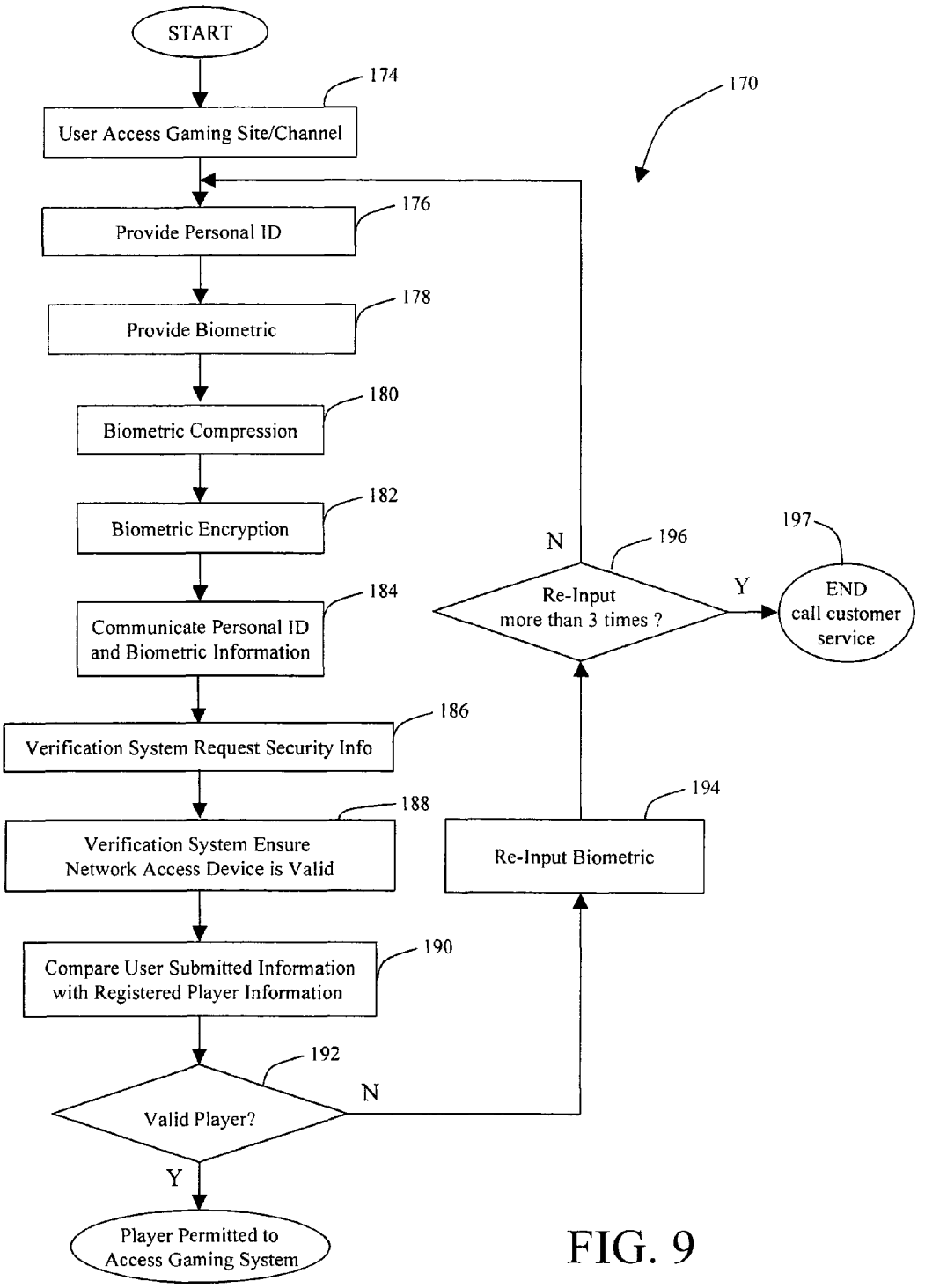

START
174
User Access Gaming Site/Channel
170
176
Provide Personal ID
178
Provide Biometric
180
Biometric Compression
182
Biometric Encryption
184
Communicate Personal ID and Biometric Information
186
Verification System Request Security Info
188
Verification System Ensure Network Access Device is Valid
190
Compare User Submitted Information with Registered Player Information
192
Valid Player?
N
Y
Player Permitted to Access Gaming System
194
Re-Input Biometric
196
Re-Input more than 3 times ?
N
Y
197
END call customer service

FIG. 9

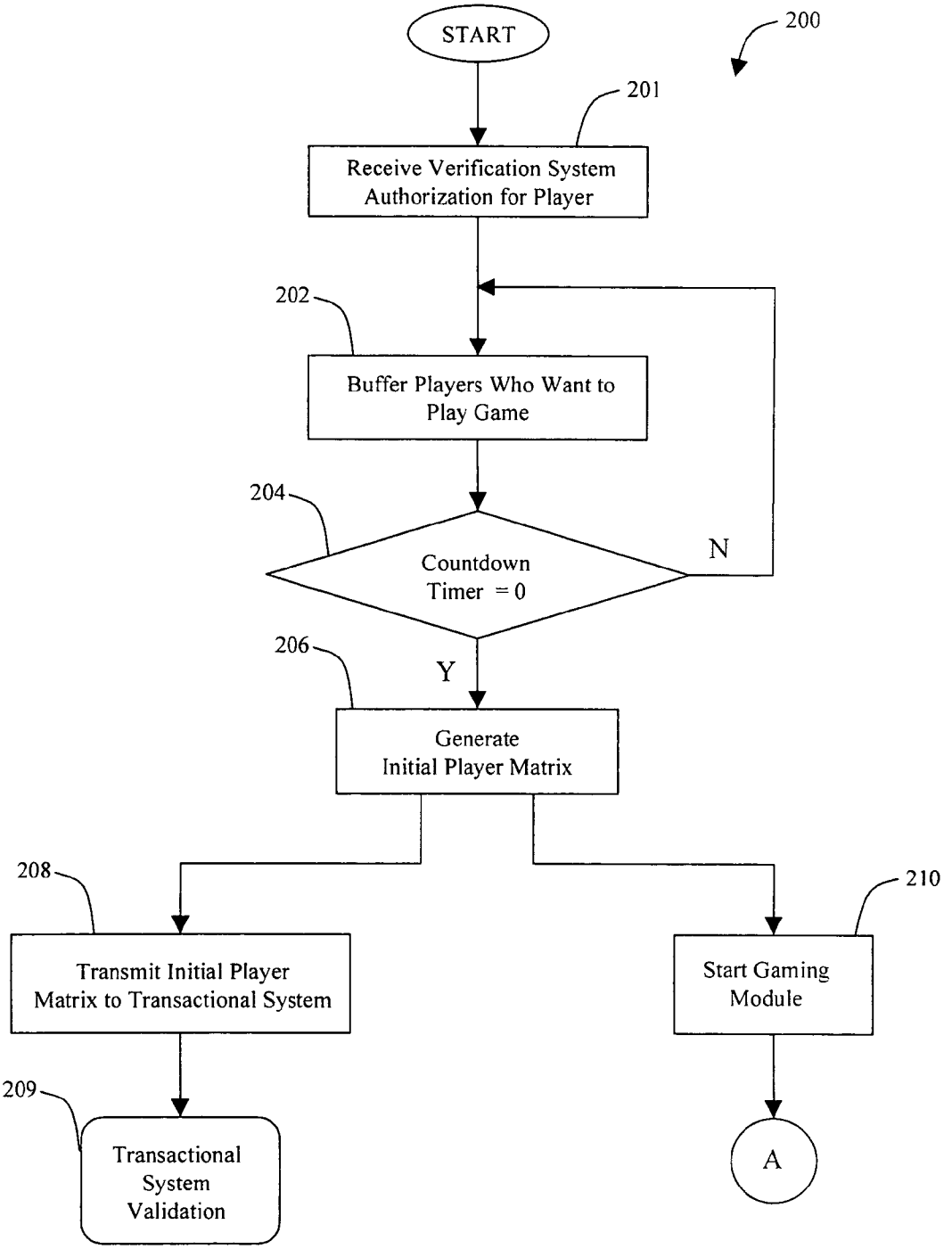

START
200
201
Receive Verification System Authorization for Player
202
Buffer Players Who Want to Play Game
204
Countdown Timer = 0
N
Y
206
Generate Initial Player Matrix
208
Transmit Initial Player Matrix to Transactional System
209
Transactional System Validation
210
Start Gaming Module
A

FIG. 10

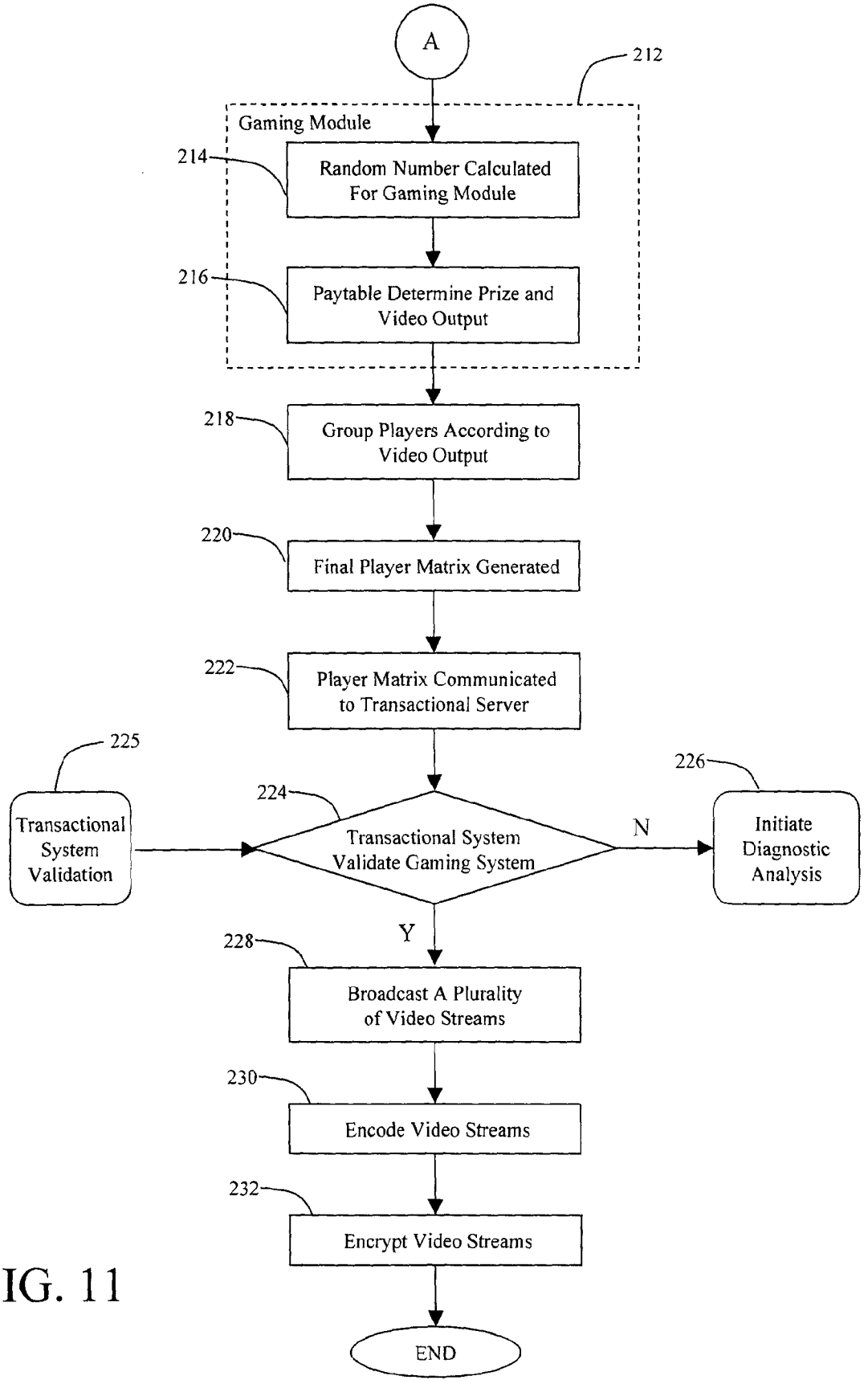

A
212
Gaming Module
214
Random Number Calculated For Gaming Module
216
Paytable Determine Prize and Video Output
218
Group Players According to Video Output
220
Final Player Matrix Generated
222
Player Matrix Communicated to Transactional Server
225
Transactional System Validation
224
Transactional System Validate Gaming System
N
226
Initiate Diagnostic Analysis
Y
228
Broadcast A Plurality of Video Streams
230
Encode Video Streams
232
Encrypt Video Streams
END

FIG. 11

GAMING SYSTEM NETWORK AND METHOD FOR DELIVERING GAMING MEDIA

CROSS REFERENCES TO RELATED APPLICATIONS

This patent application is a continuation of Ser. No. 10/681,034, filed Oct. 8, 2003 now U.S. Pat. No. 8,403,755, which is a continuation of patent application Ser. No. 09/899,559 having a filing date of Jul. 5, 2001, now abandoned, which claims the benefit of provisional patent application 60/266,956 filed Feb. 6, 2001.

BACKGROUND

1. Field

The present invention is an interactive gaming system network and method for delivering gaming media. More particularly, the interactive gaming system and method operates in a networked environment that interfaces with a gaming server and a video server.

2. Description of Related Art

The related art includes gaming devices, on-line gaming, networked interactive gaming, and biometrics.

Gaming Devices

For purposes of this patent, the term "gaming" shall refer to either gambling and/or gaming applications. Gaming devices include games of skill and games of chance. Games of chance include many casino-type gaming devices in which the outcome of the game depends, at least in part, on a randomly generated event. For example, a game of chance may use a random number generator to generate a random or pseudo-random number. The random number may then be compared to a predefined table to determine the outcome of the event. If the random number falls within a certain range of numbers on the table, the player may win a predefined prize. The table may also contain display information that allows the gaming device to generate a display that corresponds to the outcome of the game. The gaming device may present the outcome of the game on a large variety of display devices, such as mechanical spinning reels or video screens.

Games of skill comprise a skill component in which a player combines letters or words (word puzzles), answers questions (trivia), overcomes challenges (video games), competes with other players (networked video games), and the like. Generally, a game of skill is a game requiring a level of skill which does not rely solely on chance. Some games of skill require a high degree of expertise and knowledge and other games of skill require very limited expertise or knowledge.

On-Line Gaming

In June 2001, Nevada signed a bill that could result in Nevada being the first state to offer legalized gambling over the Internet. The new law authorizes state gaming regulators to set up an infrastructure to license and oversee online gaming in Nevada when such gaming becomes legal. Online gaming is a federal issue whose legality is unclear at present.

A variety of technological limitations have been asserted as preventing Congress's endorsement of on-line gaming. These technological limitations are related to the prevention of underage gambling, controlling of gambling addiction, and ensuring the security and reliability of on-line gaming.

To prevent underage gambling prior art systems and methods use passwords, user IDs, credit cards and "click-through" agreements that ask the player to agree to being of legal gambling age by clicking on a button. Presently, there are no

systems and methods to control on-line gambling addiction. With respect to ensuring that on-line gaming is secure and reliable, prior art systems and methods use various cryptographic techniques such as RSA encryption, digital certificates, or other similar well known cryptographic methods. These cryptographic methods are helpful in ensuring secure communications, however these cryptographic methods do not ensure that the individual accessing the on-line game is a valid user.

In view of the prior art systems, a minor or other unauthorized individual simply needs a user ID and a corresponding password to access a gaming site. The obtaining of a user ID and password is a relatively simple task as this information is generally not modified. Commonly the user ID information is acquired by identifying the web site's naming convention for the player. The player password can be easily determined by remembering the pattern of keys typed by the player during the log-on procedures or by simply requesting the password from the player as part of a diagnostic procedure. The latter is a trick commonly used by hackers to access a system. The password problem may be overcome by modifying the password on a regular basis, however the player must then remember the modified password. Should the player forget the password a new password is mailed. During the mailing process it is common for e-mail to be easily intercepted in cyberspace. Additionally, it is common for unauthorized users to simulate being at a certain location by submitting an IP address that identifies an authorized user.

Therefore, a better system and method for identifying a valid user is needed. Additionally, it would be beneficial to provide a gaming system and method that would prevent underage gambling, be simple to implement, prevent gambling addiction, and provide a higher degree of security and reliability from unauthorized users.

Networked Interactive Gaming

Networked interactive gaming in an open networked environment such as the Internet is well-known. However, interactive gaming in an open network such as the Internet is confined to communicating with other devices using the same TCP/IP protocols. Currently networked interactive gaming systems using the TCP/IP protocol are not configured to communicate with interactive set-top boxes using MPEG protocols.

Networked interactive gaming in an open networked environment using traditional security methods such as secure socket layers and digital certificates are well known. However, networked interactive gaming in an open networked environment using traditional security methods does not prevent gambling from a minor having acquired a parent's user ID and password without the parent's consent.

Networked interactive gaming using LANs and WANs for progressive slot machines having large jackpots are also well-known. However, networked interactive systems using LANs and WANs for progressive slot machines generally exist in a highly secure proprietary network environment. Thus, the creation of a progressive slot machine with a large jackpot in an open network environment is not well known.

Biometrics

A biometric is a measurable psychological and/or behavioral trait that can be captured and subsequently compared with another instance at the time of verification. This definition includes the matching of fingerprints, voice patterns, hand geometry, iris and retina scans, vein patterns and other such methodologies. For purposes of the invention described heretofore, the definition of biometrics also includes signature verification, keystroke patterns and other methodologies weighted towards individual behavior.

Biometric applications for games of skill and games of chance are limited. For example biometric gaming applications are taught in U.S. Pat. No. 6,010,404 granted to Walker et al. teaches a method and apparatus for using player input codes (e.g., numeric, biometric or physical) to affect the outcomes of electronic gambling devices, such as slot machines. Additionally, U.S. Pat. No. 6,142,876 granted to Cumbers teaches a system and method for passively tracking the play of players playing gaming devices such as slot machines. Players provide identification information and facial recognition data is acquired by a digital or video camera. For each player an account file and a file of the facial image data is stored. When the player plays the slot machine, a camera scans the player and acquires facial image data which is compared to stored data to identify the player. Furthermore, U.S. Pat. No. 5,902,983 granted to Crevelt et al. teaches a gaming machine configured to perform EFT transactions which are limited to preset amounts. The patent teaches the use of a fingerprint imaging device, and retinal scans for verifying a player's identity.

Although biometric applications for gaming applications are known, biometric applications for on-line gaming systems are not known. Furthermore, the managing of biometric information and gaming information in an open network environment are not known. Additionally, the use of biometrics in a gaming system and method to prevent underage gambling and prevent gambling addiction is not known.

SUMMARY

A gaming server system is described, the gaming server system configured to communicate with at least one network access device communicatively coupled to a network. The gaming server system includes a verification system, a memory module, a centralized gaming server, and a paytable module. The verification system is configured to access a registration database having a plurality of registration data associated with each registered user. The memory module is configured to store a plurality of images corresponding to at least one game outcome that are communicated to the at least one network access device. The centralized gaming server is communicatively coupled to each of the at least one network access device, the centralized gaming server configured to generate at least one random game outcome by random generation at the centralized gaming server. The paytable module is associated with the centralized gaming server, and it is configured to determine one or more prizes associated with a game outcome. The centralized gaming server is also configured to access the memory module and communicate the plurality of images corresponding to the at least one random game outcome to the at least one network access device

In one embodiment, the verification system is configured to receive user identification information associated with a player from each network access device, and verify the player accessing the network access device is a registered user by comparing the user identification information to the registration data.

A method for generating a game outcome with a gaming server system configured to communicate with a plurality of network access devices that are communicatively coupled to a network is also described. The method comprises enabling a verification system to receive user identification information from at least one network access device. The method further comprises verifying with the verification system that the user accessing the at least one network access device is a registered user by comparing the user identification information to registration data stored in a registration database. The method includes generating, with a centralized gaming server communicatively coupled to each of the plurality of network access devices, at least one random game outcome with random generation at the centralized gaming server. Finally, the method includes determining one or more prizes associated with the random game outcome with a paytable module associated with the centralized gaming server, and communicating a plurality of images corresponding to the at least one random game outcome from the centralized gaming server to each network access device.

One advantage of the present invention is that it provides a system and method to prevent underage gambling.

A further advantage of the present invention is that it provides a more secure and reliable and secure gaming system and method.

Another advantage of the present invention is that it provides a system and method for managing biometric information and gaming information in an open network environment.

Another advantage of the present invention is that it permits a plurality of users in a geographically broad area to play the same game.

A further advantage of the present invention is that it provides a pseudo-real time gaming system and method.

Another advantage of the present invention is that it simulates a game of chance such as a slot machine in an on-line environment.

An additional advantage of the present invention is that it provides a networked jackpot.

BRIEF DESCRIPTION

A networked gaming system that comprises a verification system, a broadband gaming system and a transactional system is described. The verification system operations include ensuring that a user is a registered player by using a biometric input. The broadband gaming system operations include managing and performing at least one game. The transactional system operations include providing oversight for each transaction conducted by the verification system and the broadband gaming system.

A verification system for playing the networked gaming system is described. The networked games include games of chance and games of skill. The verification system communicates with a biometric input module and a network access device to generate a user identification information. The user identification information is compared to information in a registration database. If an acceptable match is made between the user identification information and the information in the registration database, the user is designated as a player. The player then has access to both the broadband gaming system and the transactional system.

A broadband gaming system which is in communication with the verification system is described. The broadband gaming system includes a buffer which stores information about players who desire to play a game. The buffer is operatively coupled to a random number generator that generates a random number for each player in the buffer. A paytable module in communication with the random number generator determines the outcome associated with the random number generator. The paytable also determines which images are associated with the outcome for each player. Preferably, the images are stored on a mini video server and then cached in a memory module. The images are intelligently buffered for downstream communications. In its preferred embodiment, a plurality of encoders are operatively coupled to the memory module caching the broadcast video streams. The plurality of

encoders encode the broadcast downstream images according the requirements for each network access device. Each encoder is operatively coupled to an encryption module that encrypts the broadcast. A modulation module is operatively coupled to the encryption module and modulates encrypted images for downstream transmission. Each network access device includes a tuner, a demodulation module, and a decryption module that permits an image to be viewed by the network access device.

A transactional system and method that ensures secure communications occur in the verification system and the broadband gaming system is described. The transactional system also performs accounting, bonusing, tracking and other such functions. Preferably, the transactional system is capable of receiving a plurality of funds from a financial account and converting them to credits that are used in the broadband gaming system.

The above description sets forth, rather broadly, the more important features of the present invention so that the detailed description of the preferred embodiment that follows may be better understood and contributions of the present invention to the art may be better appreciated. There are, of course, additional features of the invention that will be described below and will form the subject matter of claims. In this respect, before explaining at least one preferred embodiment of the invention in detail, it is to be understood that the invention is not limited in its application to the details of the construction and to the arrangement of the components set forth in the following description or as illustrated in the drawings. The invention is capable of other embodiments and of being practiced and carried out in various ways. Also, it is to be understood that the phraseology and terminology employed herein are for the purpose of description and should not be regarded as limiting.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the present invention are shown in the accompanying drawings wherein:

FIG. **1***a* through FIG. **1***d* provide diagrams of a plurality of network access devices.

FIG. **2** is a high level diagram of a gaming system networked to a plurality of network access devices.

FIG. **3** is a block diagram of an illustrative biometric input module.

FIG. **4** is a block diagram of a gaming system configured to receive a biometric input from a network access device.

FIG. **5** is a table of the data fields in a verification system.

FIG. **6** is a table of the data fields in a broadband gaming system and in a transactional system.

FIG. **7** is a block diagram of a broadband gaming system.

FIG. **8** is a flowchart of the registration method for the gaming system.

FIG. **9** is a flowchart of the verification method for the gaming system.

FIG. **10** is a flowchart of the information processed by the gaming system.

FIG. **11** is a continuation of the flowchart of the information processed by the gaming system in FIG. **10**.

DETAILED DESCRIPTION

In the following detailed description of the preferred embodiments, reference is made to the accompanying drawings, which form a part of this application. The drawings show, by way of illustration, specific embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

Network Access Devices

Referring to FIG. **1***a* through FIG. **1***d* there is shown a plurality of illustrative network access devices. Each of the network access devices is configured to be capable of running a gaming application. For illustrative purposes the gaming application shown simulates the spinning reels of a slot machine.

The network access device in FIG. **1***a* is a personal computer **10** having a network interface card (not shown) that may be operatively coupled to a modem (not shown). Another network access device shown in FIG. **1***b* includes a television **12** operatively coupled to an interactive set-top box **14** that is operatively coupled to a cable network (not shown). The other network access device shown in FIG. **1***c* is a wireless device **16** such as a digital phone or personal digital system (PDA) or other such wireless device which is configured to communicate with a network using wireless networking protocols. Yet another network access device is shown in FIG. **1***d* and includes a gaming terminal **18** such as a slot machine on a casino floor that is operatively coupled to a plurality of other gaming terminals. It shall be appreciated by those skilled in the art of networking that the distinguishing feature between each of these network access devices is the type of communications protocols used by each device to enable communications between similar network access devices.

Each of the network access devices either includes a biometric input module operatively coupled to the network access device or includes a biometric input module communicatively coupled to the network access device. A biometric is a measurable psychological and/or behavioral trait that can be captured and subsequently compared with another instance at the time of verification. This definition includes the matching of fingerprints, voice patterns, hand geometry, iris and retina scans, vein patterns and other such methodologies. For purposes of the invention described heretofore, the definition of biometrics also includes signature verification, keystroke patterns and other methodologies weighted towards individual behavior.

In one illustrative embodiment, the biometric input module is a fingerprint scanner **20** resident on the gaming terminal **18** wherein the biometric input is a fingerprint. In another illustrative embodiment, the biometric input module is the screen **22** of wireless device **16** wherein the screen is configured to receive a biometric input such as a user signature. In yet another illustrative embodiment, the biometric input module is a telephone **24** that is configured to receive a voice pattern from a user prior to engaging communications with the interactive set-top box **14**. In yet another illustrative embodiment the biometric input module is a keyboard **26** operatively coupled to computer **10** wherein the user is requested to input a keystroke pattern. An illustrative example of a biometric input module operatively coupled to the network access device is shown in FIG. **1***d* having the fingerprint scanner **20** on the gaming terminal **18**. An illustrative example of a biometric input module, e.g. the telephone **24**, communicatively coupled to the network access device, e.g. the interactive set-top box **14**, is shown in FIG. **1***b*.

The biometric input is used to prevent unauthorized gaming activity and efficiently store credits on the user's behalf. By way of example and not of limitation, unauthorized gaming activity includes preventing underage gaming and prohibiting players with histories of gambling addiction. Additionally, player credits may be stored on a network so that the player does not need to carry coins, paper currency, coupons,

credit cards or debits cards to play a game. It shall be appreciated by those skilled in the art having the benefit of this disclosure that different biometric input modules may be used in conjunction with different network access devices.

Gaming System

Referring to FIG. **2** there is shown a high level block diagram of a gaming system **30** in communication with a plurality of network access devices coupled to a network **32**. The gaming system includes a verification system **34**, a broadband gaming system **36** and a transactional system **38**. The verification system **34** verifies that a user operating a network access device is a registered player. The broadband gaming system **36** performs the function of generating a game and broadcasting the game results to each of the network access devices. The transactional system **38** performs a plurality of functions including tracking each transaction performed by both the verification system and the broadband gaming system and conducting electronic fund transfers.

Verification System

The verification system **34** verifies that a user desiring to play the game is a registered player. The verification system **34** communicates with the biometric input module and a network access device to generate user identification information. The user identification information includes information such as cryptographic keys that are necessary to securely identify the network access device. The user identification information also includes media access control (MAC) identification and confirmation of the user Internet Protocol (IP) address. The user identification information is compared to information in a registration database **40** by a verification server **42**. If an acceptable match is made between the user identification information and the information in the registration database, the user is designated as a player. The player then has access to either the broadband gaming system **36** or the transactional system **38**.

In an alternative embodiment the user identification information is housed in a smart card (not shown) that is in communication with the verification system **34**. The smart card includes a stored biometric which is used to identify the user as a player. Cryptographic keys are then exchanged between the verification system **34** and the smart card to provide the player access to either the broadband gaming system or the transactional system **38**.

Referring to FIG. **3** there is shown an illustrative biometric input module **50**. By way of example, the illustrative biometric input module **50** is a fingerprint scanner. It shall be appreciated by those skilled in the art having the benefit of this disclosure that the use of the fingerprint scanner as the illustrative biometric input module is not restrictive. A scanned fingerprint image is collected by the biometric input **52**. After the scanned fingerprint image is collected, the fingerprint image is compressed by the compression module **54**. A memory module **56** provides fast memory resources for the compression of the fingerprint image. After compression, the fingerprint image is encrypted by the encryption module **58** for downstream transmission. The encryption module **58** also includes a memory module **60** that provides fast memory resources for the encryption of the compressed fingerprint image. An encrypted compressed fingerprint image is then communicated to network **32** (see FIG. **2**) using the network interface module **62**.

Referring to FIG. **4** there is shown a block diagram of the verification system **34**. The verification system is operatively coupled to network **32** with network interface module **64**. The network interface module **64** is configured to receive user identification information generated by the network access devices and from the biometric input module. Preferably, the biometric and other user identification information received by the verification system is an encrypted biometric that is decrypted by decryption module **66**. A memory module **68** is preferably a fast memory that expedites the decryption process. After decryption the biometric and remaining user identification information is processed by the verification server. It shall be appreciated by those skilled in the art that the verification server **42** may house the network interface module **64**, decryption module **66** and the memory module **68**. The verification server **42** is also in operative communication with a registration database **40**. The verification server **42** performs the function of matching the user identification information collected from the network access device with the player information in the registration database **40**. Additionally, the verification server **42** performs the caching functions needed to ensure that once a player has been identified during an initial game, subsequent usage by the same player proceeds quickly.

Preferably, the verification server **42** identifies registered players using a biometric template of the registered player residing on the registration database **40**. The registered players are referenced with Personal ID numbers. When a transaction is undertaken the user firstly calls up the particular template from the registration database **40** by inputting a Personal ID. The Personal ID includes a particular number, user ID, password or other such identification techniques. The inputting of the Personal ID is accomplished with a familiar numeric keypad, keyboard, magstripe card or smart card. The correct template is called and held in memory ready for comparison with the biometric sample provided by the user. A comparison takes place that results in a binary true or false condition as to the identity of the user. The user is in effect claiming an identity by inputting the Personal ID and the system is subsequently verifying that the claim is genuine according to the matching criteria setup within the system.

Referring to FIG. **5** there is shown the registration data fields **70** and user submitted data fields **72**. The registration data fields **70** include data fields that comprise the user identification information. The registration data fields include user identification information such as player name, address, user name, password, credit card information, and the date and time of the registration. The player biometric and Personal ID also comprises the user identification information and provides unique information about the player. The Personal ID may be the same as the user name or password. It shall be appreciated by those skilled in the art that some biometric information may be compressed. Furthermore, the user identification information includes data about the network access device and the network connection such as MAC ID, IP addresses, browser type, any cookies resident on the network access device, etc. Finally, the user identification system includes cryptographic keys which are used to encrypt and decrypt the communications between the verification system and each of the network access devices.

The user submitted data fields **72** mirror the registration data fields **70**. The user submitted data fields receive data generated by a user that is attempting to access the broadband gaming system **36**. The user submitted information is carefully analyzed to ensure that a valid user is being identified. It is well known that the connection of one network access device to another network access device generates security concerns. Preferably, the present verification system operates using a fast hardware-type firewall that performs a stateful multilayer inspection. In its preferred embodiment the firewall provides packet filtering using a secure protocol such as IPSec. This protocol provides encryption of the data at the packet level as well as at the source address level. Without

access to the encryption keys, a potential intruder would have difficulty penetrating the firewall. Additionally, it would be preferable to provide a circuit level gateway and an application level gateway. The circuit level gateway works on the session layer of the OSI model or the TCP layer of the TCP/IP model and monitors TCP handshaking between packets to determine whether a requested session is legitimate. The application level gateway filters data packets at the application layer of the OSI model. A stateful multilayer inspection firewall offers a high level of security, good performance and transparency to end users.

Referring to FIG. **6** there is shown the player data fields **74** that are generated by the broadband gaming system and the transactional system after the user has been verified to be a registered player. The player data fields **74** are used to generate a player matrix which is used as an additional internal security measure. The player data fields **74** include a Player ID that identifies the player, a timestamp that provides the date, time in and time out by the player during the game. Additionally, the type of game, credits played, and credits remaining are monitored. Based on the level of player activity a bonus is provided to the player. Further still the session time for each type of game and the amount played during the session is monitored to better define the type of games the players' like. Transactional information is also monitored and updated, preferably, by the transactional system **38**. The transactional information includes credit card information, transaction requests, transaction approval, conversion of monetary funds to credits for playing the game, any transfers of credits for playing the game, and conversions from credits to monetary funds that are credited to the player's financial account. Preferably, communications between the transactional system and the broadband gaming system are conducted in a secure environment using cryptographic keys. Although the use of cryptography within the private network may appear excessive one of the greatest security threats within a private network comes from its own employees. Therefore, it is preferable to use internal firewalls for communications between the broadband gaming system, the transactional system and the verification system.

Broadband Gaming System

A more detailed drawing of the broadband gaming system is provided in FIG. **7**. The dashed boundary in FIG. **7** defines the broadband gaming system **36**. After player verification is completed at the verification system **34**, the broadband gaming system **34** is engaged. The broadband gaming system **34** includes a player buffer **84** configured to receive the players who will be playing the game. The player buffer **84** generates an initial player matrix with player data fields **74**.

A countdown timer **82** is coupled to the player buffer **80**. Preferably, the countdown timer **82** is also displayed to the player. The countdown timer **82** provides a window of time within which players may join the game. The players that have joined the game before the end of the timing period are stored in the buffer. When the timing period reaches zero the initial player matrix is communicated to the transactional system **38** and to the gaming module **84**.

The gaming module **84** provides a game that is played by the plurality of players. The game may include a plurality of different games and the type of game is not restrictive to this invention. Preferably, the gaming module **84** includes at least one random number generator **86** and a paytable module **88**.

The random number generator **86** is operatively coupled to the player buffer. The random number generator **86** generates at least one random number that is stored in the player matrix. In one embodiment, at least one random number is generated for the plurality of players playing the game. In an alternative embodiment, at least one random number is generated for each player. In yet another embodiment, a plurality of random numbers are generated that are applied to the plurality of players playing the game. Preferably, the random number generator **86** is a fast hardware module.

A paytable module **88** is operatively coupled to the random number generator **86**. The paytable module **88** is a programmable module that determines the type of prize awarded to the player based on the random number generated by the random number generator **86**. In one embodiment, the paytable module **88** is a field programmable gate array. Preferably, the paytable module **88** also includes an image ID that is associated with the outcome determined by the paytable module **88**.

A gaming output module **90** revises the player matrix to include the outcome for each player. Additionally, the gaming output module **90** groups the players according to the image ID. Based on the results generated by the gaming module **84**, the gaming output module **84** generates a final player matrix that is communicated to the transactional server **38** and to a memory module **92**.

Preferably, the memory module **92** has stored a plurality of images in a fast memory by the time the final player matrix is communicated to the memory module **92**. In operation, the memory module **92** is enabled before the final matrix is communicated to the memory module **92**. By way of example, when the game is engaged the memory module **92** begins the process of finding the applicable images associated with the image IDs in the mini-video server **94** and transferring the images to the fast memory module **92**. Thus, when the gaming output is received by the memory, the images are stored in the fast memory module **92**. In one embodiment, the memory module **92** then broadcasts the images to encoders **96** and **98**. In an alternative embodiment, the memory module **92** is operatively coupled to an intelligent router (not shown) that routes the images to the appropriate encoders **96** and **98**.

The appropriate encoder then receives the images and converts them to a format which meets the requirements for the appropriate network access device. By way of example, an IP encoder **96** encodes a plurality of JPEG images for viewing on a conventional web browser, and an MPEG encoder **98** encodes the plurality of JPEG images into an MPEG stream that is viewed on a television via an interactive set-top box.

An encryption module **100***a* and **100***b* operatively coupled to encoder **96** and **98**, respectively, then receives the encoded images and encrypts the encoded images in manner well known to those skilled in the art. A modulation module **102***a* and **102***b* is operatively coupled to encryption modules **100***a* and **100***b*, respectively, then modulates encrypted encoded images for downstream transmission in a manner well known to those skilled in the art.

Preferably, the broadband gaming system occupies one downstream band, i.e. one 6 or 8 MHz band, in the interactive set-top-box environment. In the web based broadcast environment, the broadband gaming system occupies a downstream channel much like a standard streaming media website.

It shall be appreciated by those skilled in the art having the benefit of this disclosure that the broadband gaming system can play more than one game at a time. The system may be designed to operate in a multi-tasking mode where more than one game is played at a time. Additionally, the system may be designed to operate in a fast serial mode in which a game is played while the countdown timer is waiting for the next queue to be filled.

Transactional System

Referring back to FIG. **2**, there is shown the transactional system **38** which comprises a transactional server **110** and a

transactional database **112**. The transactional system **38** performs a plurality of functions including tracking each transaction performed by both the verification system and the broadband gaming system. Additionally, the transactional system **38** is configured to authorize and conduct electronic fund transfers. Furthermore, the transactional system **38** performs such operations as player tracking, managing loyalty programs, engaging bonus games, determining bonus prizes and interfacing with accounting programs.

Method for Registering a Player

Referring to FIG. **8** there is shown a flowchart of the registration method for the gaming system **30**. The registration method **150** begins when a prospective player first accesses a website, channel, kiosk or other such registration terminals as described in block **152**. The method then proceeds to block **153**.

At block **153**, the registration process is initiated. By way of example and not of limitation, a registration terminal may provide a hyperlink to a registration window that prompts the prospective player for information. The method then proceeds to block **154**.

At block **154**, the prospective player provides registration identification information such as name, address, credit card number and other information necessary to create a registration file for the prospective player. The method then proceeds to block **156**.

At block **156**, the prospective player is prompted for a personal ID. The personal ID may be a user ID, a password, a numeric combination, or any other such identification information. The personal ID is used during the verification process to identify a biometric template for the prospective player. The method then proceeds to block **158**.

At block **158**, the prospective player submits a biometric to the registration terminal. By way of example and not of limitation the biometric is a fingerprint. Any other biometric may also be used. The method then proceeds to block **160** or **162**.

At block **160**, the biometric input is compressed and encrypted. It is preferable for certain biometric inputs to be compressed such as fingerprint scans, retinal scans and other such scanning techniques. Other biometric inputs such as voice patterns and signatures do not have to be compressed. The process of encrypting biometric inputs is necessary in an open network environment. The process of encrypting may not be necessary on a private proprietary network. Therefore, it shall be appreciated by those skilled in the art having the benefit of this disclosure that the compression and encryption processes in block **160** may not be necessary for every biometric input.

At block **162**, the prospective player information is stored in the verification system and a player profile is updated accordingly. Alternatively, the prospective player information is stored on a smart card. The method then proceeds to block **164**.

At block **164**, security information about the registration terminal is collected. The registration information identifies the registration terminal as being a secure terminal. The registration terminal provides information such as the MAC ID for the biometric input module, the IP address for the server communicating with the registration terminal, and the cryptographic keys associated with the registration terminal. The registration terminal includes the network access devices described in FIG. **1***a* through FIG. **1***d* as well as kiosks and other such registration terminals.

At block **166**, the prospective player is identified as a registered player and the registration database **40** is updated accordingly. The registration process is broken out into separate components for security purposes. Once a validly registered player is identified by the verification system, the registration process is completed.

Method for Player Verification

Referring to FIG. **9** there is shown a method **170** for player verification used by the verification system **34**. The player verification process includes receiving user identification information from a network access device. The method is initiated at block **174** when a user accesses a website or channel displaying the game. The method then proceeds to block **176**.

At block **176**, the personal ID is provided by the user. The personal ID is used by the verification system to find a biometric template for determining whether the user is a registered player. The method then proceeds to block **178**.

At block **178**, the biometric input module of the network access device receives a biometric from the user. As previously described the biometric input module can be one of plurality of biometric inputs. Depending on the type of biometric, the biometric may be compressed as described by block **180** and encrypted as described by block **182**. At block **184**, the biometric and the personal ID is then communicated through a network **32** to the verification system **34**. Alternatively, the biometric and Personal ID is communicated to a smart card for verification.

At block **186**, the verification system **34** requests security information from the network access devices. The security information identifies the network access devices as being a valid network access device. The method then proceeds to block **188**.

At block **188**, the verification system **34** processes the security information to ensure that the security information is generated by the appropriate network access device, and to ensure that the security information has not been compromised. Preferably, the verification system **34** performs a stateful multilayer inspection as described above. The method then proceeds to block **190**.

At block **190**, the user submitted player information is compared to the registered player information. If a determination is made at decision diamond **192** that the submitted player information is not a valid registered player the method proceeds to block **194**. At block **194**, the user is requested to re-input the biometric. If the biometric is input more than three times, as provided by decision diamond **196**, the user is requested to contact customer service.

If a match is found at decision diamond **192** between the user submitted information and the registered player information, the user is identified as a valid player then the player proceeds to the broadband gaming system **36**.

Method for Operation of Broadband Gaming System

Referring to FIG. **10** and FIG. **11** there is shown a flowchart **200** of the information processed by the broadband gaming system **34**. The process is engaged by performing the verification process in which the verification system identifies a player as in block **201**. After the verification process has been completed the method proceeds to block **202**.

At block **202**, the players who desire to play a particular game are stored in a buffer until the particular game is engaged. The method then proceeds to decision diamond **204**.

At decision diamond **204**, the countdown timer **82** determines if the period during which the game is open has been closed. If the game remains open, additional players may be received by the broadband gaming system. If the game is closed because the period during which the game is open has expired, then the method proceeds to block **206**.

At block **206**, the initial player matrix described above is generated. The initial player matrix includes information about the player, the type of game, and other such information

about the game as described by the player data fields **74** shown in FIG. **6**. The initial player matrix is then communicated to block **208** which transmits the initial player matrix to the transactional system for validation. Additionally, the initial player matrix is communicated to the next block **210** in the broadband gaming system which starts the gaming module.

At block **210**, the initial player matrix is received by the gaming module **84** and the gaming module **84** is engaged. At a minimum the gaming module **84** comprises a random number generator **86** and a paytable module **88**. The random number generator generates at least one random number that is used during the game. The paytable module **88** is used to determine the prize associated with the at least one random number.

Referring to FIG. **11**, a continuation of the broadband gaming system method is shown. By way of example, the gaming module may comprise a plurality of different random number generators. The blocks **214** and **216** describe the processes performed by a random number generator and a paytable module, respectively. The random number generator **86** of block **214** determines the winning combination of numbers for the game. At block **216**, the paytable module **88** is used to determine the prize awarded to the player. Preferably, the paytable module **88** is also configured to provide image IDs that identify the images associated with the prize. Preferably, the paytable module **88** is resident in both the broadband gaming system and the transactional system. The purpose for this redundancy is as a security check for output generated by the gaming module. The method then proceeds to block **218**.

At block **218** the player outputs with the same image IDs are grouped together. The grouping process is performed to simplify the broadcasting of the images to the plurality of players. By grouping the players according to the same image ID and having identified the network access device used by the player, a dynamic broadcasting method is created which occupies minimal downstream bandwidth. The method then proceeds to block **220**.

At block **220** a final player matrix is completed. The final player matrix includes the same data fields as the initial player matrix. Additionally, the final player matrix includes the random number output and the paytable output. The final player matrix is then communicated to the transactional system as described in block **222**. The method then proceeds to decision diamond **224**.

At decision diamond **224**, a validation procedure is conducted. The validation procedure essentially compares the transactional system's reverse calculation of the random numbers with the random numbers generated by the gaming module. If the random numbers in the transactional system are not the same or similar to the random numbers generated by the random number generator, a system failure or security breach is detected. If a security breach or system failure is detected, the method then proceeds to process block **226**, which initiates diagnostic procedures. If the random numbers match, then the method proceeds to block **228**.

At block **228**, the plurality of images is broadcast. The images are preferably broadcast along one downstream channel for each network access device. However, traffic considerations may require the use of a plurality of downstream channels. By way of example, for DOCSIS and DSL type downstream transmissions, the streaming video preferably occupies a portion of the bandwidth available for a cable modem or DSL modem, respectively. In an alternative example, for an interactive set-top box environment, the downstream channel preferably occupies one 6 MHz or 8 MHz band or a portion of the 6 MHz or 8 MHz band. The method then proceeds to the next block **230**.

At block **230**, the broadcast images are encoded for downstream transmission. It shall be appreciated by those skilled in the art having the benefit of this disclosure that downstream transmission systems are well known and can be easily integrated into the systems and method described in this patent. The method then proceeds to block **232**.

At block **232**, the broadcast images are encrypted for downstream transmission. The purpose for downstream encryption is to prevent unauthorized access to the downstream signal. It shall be appreciated by those skilled in the art that various secure systems and methods for downstream transmission of images are well known.

It shall be appreciated by those skilled in the art having the benefit of this disclosure that a plurality of games may be played simultaneously. The games may be played in a distributed/parallel manner or in serial manner.

An Illustrative Game

An illustrative game is described to show how the system and method described above operates. The illustrative game described herein is a progressive slot machine. It is well-known that in the United States many states have legalized lottery games even though other games of chance such as progressive slot machines have not been legalized. It is also well-known that in casino gaming floors the most popular games are progressive slot machines. The present illustrative game operates on the system and method described above and provides an output similar to a progressive slot machine with a lottery type input.

The illustrative game includes first having a player provide a plurality of letters or numbers that are either generated by the player or are selected in a random manner. The random number generator of the gaming module is then engaged and a gaming module random number is generated. Preferably, the order that the random numbers were generated is used to determine the prize awarded to the player. A programmed paytable is then used to compare the player selected numbers to the gaming module random numbers according to the rules programmed into the paytable module. Based on the results of this comparison a prize is awarded to the player. An image ID is associated with the prize awarded. The plurality of players are then grouped according to their respective image IDs. A broadcast stream for the plurality of images associated with each image ID is broadcast to each player.

A more concrete example includes having a player select a plurality of numbers, such as the numbers below:

25 35 8 15 42

The random number generator of the gaming module is then engaged. By way of example the random number results are:

56 2 3 8 42

The paytable module is then programmed to interpret the random numbers generated by the gaming module according to the following illustrative rules:

1. If a match between one number is achieved, then a prize of IX the initial bet credit is awarded and an image ID X023-1396 is used. Image ID X023-1396 is an animated plurality of images representing three cherries.
2. If a match between one number at the same location is achieved, then a prize of 2× the initial bet credit is awarded and an image ID X023-1397 is used. Image ID X023-1397 is an animated plurality of images representing four cherries.
3. If a match between a first number is achieved and a match between a second number is achieved, then a prize of 5× the initial credit is awarded and an image ID X023-1998

is used. Image ID X023-1998 is an animated plurality of images representing 3 oranges.

4. If a match between a first number at the same location is achieved and a match between a second number is achieved, than a prize of 7× the initial credit is awarded and an image ID X023-1999 is used. Image ID X023-1999 is an animated plurality of images representing 4 oranges.

Thus, for the illustrative example provided above, the player having selected the numbers: 23, 35, 8, 15 and 42 is entitled to a prize of 7× the initial credit for a random number: 56, 2, 3, 8, and 42. The associated images displayed on the network access device is an animated plurality of images representing 4 oranges.

The scope of the invention should be determined by the appended claims and their legal equivalents rather than by the examples given.

What is claimed is:

1. A gaming server system configured to communicate with at least one network access device communicatively coupled to a network, the gaming server system comprising:

a verification system configured to access a registration database having a plurality of registration data associated with each registered user;

a memory module configured to store a plurality of images corresponding to at least one game outcome that are communicated to the at least one network access device;

a centralized gaming server communicatively coupled to each of the at least one network access device, the centralized gaming server configured to generate at least one random game outcome by random generation at the centralized gaming server;

a paytable module associated with the centralized gaming server, the paytable module configured to determine one or more prizes associated with a game outcome; and

the centralized gaming server configured to access the memory module and communicate the plurality of images corresponding to the at least one random game outcome to the at least one network access device.

2. The gaming server system of claim **1**, wherein the centralized gaming server includes a player buffer configured to receive one or more player data for one or more players from the at least one network access device.

3. The gaming server system of claim **2**, wherein the centralized gaming server comprises a countdown timer coupled to the player buffer, the countdown timer configured to limit the time during which the player buffer is capable of receiving player data.

4. The gaming server system of claim **2**, wherein the random game outcome generated at the centralized gaming server is one random number per each player data in the player buffer.

5. The gaming server system of claim **2**, wherein the random game outcome generated at the centralized gaming server is one random number for all the player data in the player buffer.

6. The gaming server system of claim **1**, further comprising an encoding module configured to convert the plurality of images to a format meeting the requirements of each network access device.

7. The gaming server system of claim **1**, further comprising an encryption module, the encryption module configured to encrypt the plurality of images communicated to each network access device.

8. The gaming server system of claim **1**, wherein the verification system is configured to receive a player biometric from the at least one network access device and compare the player biometric to the registration data.

9. A gaming server system configured to communicate with a plurality of network access devices that are communicatively coupled to a network, the gaming server system comprising:

a verification system configured to access a registration database having a plurality of registration data associated with each registered user, wherein the verification system is configured to:

receive user identification information associated with a player from at least one network access device, and

verify the player accessing the network access device is a registered user by comparing the user identification information to the registration data;

a memory module configured to store a plurality of images corresponding to at least one game outcome that are communicated to the plurality of network access devices;

a centralized gaming server communicatively coupled to each of the plurality of network access devices, the centralized gaming server configured to generate at least one random game outcome by random generation at the centralized gaming server;

a paytable module associated with the centralized gaming server, the paytable module configured to determine one or more prizes associated with a game outcome; and

the centralized gaming server configured to access the memory module and communicate the plurality of images corresponding to the at least one random game outcome to each network access device.

10. The gaming server system of claim **9**, further comprising a player buffer configured to receive one or more player data sets, each player data set associated with a particular player.

11. The gaming server system of claim **10**, further comprising a countdown timer coupled to the player buffer, the countdown timer configured to limit the time during which the player buffer is capable of receiving the one or more player data sets.

12. The gaming server system of claim **10**, wherein the random game outcome is based on a random number from a random number generator, the random number generated for each player data set in the player buffer.

13. The gaming server system of claim **10**, wherein the random game outcome is based on a random number from a random number generator, the random number generated for all player data sets in the player buffer.

14. The gaming server system of claim **9**, further comprising an encoding module configured to convert the images to a format meeting the requirements of each network access device.

15. The gaming server system of claim **9**, further comprising an encryption module, the encryption module configured to encrypt the plurality of images communicated to each network access device.

16. The gaming server system of claim **9**, wherein the verification system is configured to receive a player biometric as user identification information that is associated with the player from each network access device.

17. A method for generating a game outcome with a gaming server system configured to communicate with a plurality of network access devices that are communicatively coupled to a network, the gaming server system comprising:

enabling a verification system to receive user identification information from at least one network access device;

verifying with the verification system that the user accessing the at least one network access device is a registered user by comparing the user identification information to registration data stored in a registration database;

generating, with a centralized gaming server communicatively coupled to each of the plurality of network access devices, at least one random game outcome with random generation at the centralized gaming server;

determining one or more prizes associated with the random game outcome with a paytable module associated with the centralized gaming server; and

communicating a plurality of images corresponding to the at least one random game outcome from the centralized gaming server to each network access device.

18. The method of claim **17**, further comprising receiving one or more player data sets with a player buffer at the centralized gaming server.

19. The method of claim **18**, further comprising limiting the time during which the player buffer is capable of receiving the one or more player data sets with a countdown timer at the centralized gaming server.

20. The method of claim **18**, wherein generating at least one random game outcome comprises generating a random game output at the centralized gaming server for each player data set in the player buffer.

21. The method of claim **18**, wherein generating at least one random game outcome comprises generating a random game output at the centralized gaming server for all player data sets in the player buffer.

22. The method of claim **17**, further comprising converting the plurality of images to a format meeting the requirements of each network access device with an encoding module.

23. The method of claim **17**, further comprising encrypting the plurality of images communicated to each network access device with an encryption module.

24. The method of claim **17**, wherein verifying with the verification system includes receiving a player biometric from the at least one network access device and comparing the player biometric to the registration data stored in the registration database.

* * * * *

US008506406B2

(12) **United States Patent**
Kerr

(10) **Patent No.: US 8,506,406 B2**
(45) **Date of Patent: *Aug. 13, 2013**

(54) **NETWORK ACCESS DEVICE AND METHOD TO RUN A GAME APPLICATION**

(75) Inventor: **Michael A. Kerr**, Reno, NV (US)

(73) Assignee: **NexRF, Corp.**

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 60 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **12/982,018**

(22) Filed: **Dec. 30, 2010**

(65) **Prior Publication Data**

US 2011/0159953 A1 Jun. 30, 2011

Related U.S. Application Data

(63) Continuation of application No. 10/681,034, filed on Oct. 8, 2003, now Pat. No. 8,403,755, which is a continuation of application No. 09/899,559, filed on Jul. 5, 2001, now abandoned.

(60) Provisional application No. 60/266,956, filed on Feb. 6, 2001.

(51) **Int. Cl.**
A63F 9/24 (2006.01)

(52) **U.S. Cl.**
USPC **463/42**; 463/17; 463/13; 705/44

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,339,798	A	7/1982	Hedges et al.
4,856,787	A	8/1989	Itkis
5,586,937	A	12/1996	Menashe
5,594,491	A	1/1997	Hodge et al.
5,630,757	A	5/1997	Gagin et al.
5,643,086	A	7/1997	Alcorn et al.
5,738,583	A	4/1998	Comas et al.
5,761,416	A	6/1998	Mandal et al.
5,762,552	A	6/1998	Vuong et al.
5,768,382	A	6/1998	Schneier et al.
5,779,545	A	7/1998	Berg et al.
5,800,268	A	9/1998	Molnick
5,851,149	A	12/1998	Xidos et al.
5,871,398	A	2/1999	Schneier et al.
5,902,983	A	5/1999	Crevalt et al.
5,971,849	A	10/1999	Falciglia
6,001,016	A	12/1999	Walker et al.

(Continued)

OTHER PUBLICATIONS

"Internet Industry Interacting Gambling Code: A Code for Industry Co-Regulation in the Area of Internet Gambling Content Pursuant to the Requirements of the Interactive Gaming Act of 2001". Internet Industry Association. Dec. 2001.

(Continued)

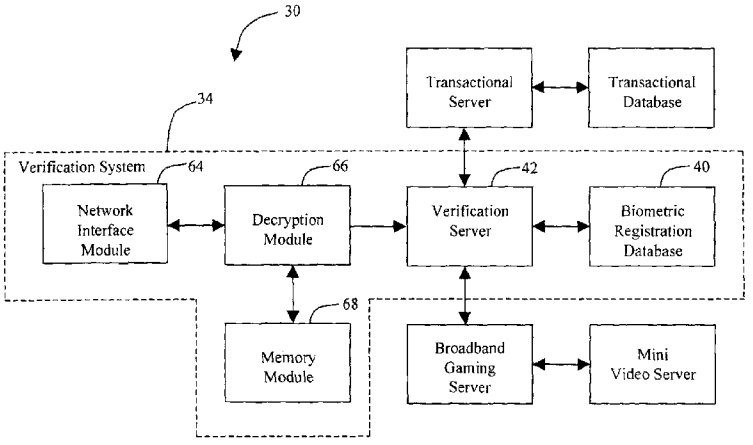
Primary Examiner — Paul A D'Agostino

(74) *Attorney, Agent, or Firm* — Michael A. Kerr; Kerr IP Group, LLC

(57) **ABSTRACT**

A network access device and method to run a gaming application on a network access device are described. The network access device comprises a communications module configured to allow the network access device to communicate with a network. The network access device is configured to transmit user identification information to a verification system and transmit security information to a verification system. When the user identification information and security information have been verified by the verification system, the network access device receives a random game output generated by a gaming system.

19 Claims, 9 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

6,010,404	A	1/2000	Walker et al.	
6,106,396	A	8/2000	Alcorn et al.	
6,142,876	A	11/2000	Cumbers	
6,159,095	A *	12/2000	Frohm et al.	463/19
6,178,510	B1	1/2001	O'Connor et al.	
6,203,428	B1 *	3/2001	Giobbi et al.	463/16
6,409,602	B1	6/2002	Wiltshire et al.	
6,500,068	B2	12/2002	Walker et al.	
6,508,709	B1	1/2003	Karmarker	
6,508,710	B1	1/2003	Paravia et al.	
6,527,638	B1	3/2003	Walker et al.	
6,575,834	B1	6/2003	Lindo	
6,612,928	B1	9/2003	Bradford et al.	
6,628,939	B2	9/2003	Paulsen	
6,676,522	B2	1/2004	Rowe	
6,682,421	B1	1/2004	Rowe et al.	
6,709,333	B1	3/2004	Bradford et al.	
6,709,631	B2	3/2004	Mori et al.	
6,719,631	B1 *	4/2004	Tulley et al.	463/17
6,749,512	B2	6/2004	MacGregor et al.	
6,875,110	B1 *	4/2005	Crumby	463/42
6,884,162	B2	4/2005	Raverdy et al.	
6,942,574	B1	9/2005	LeMay et al.	
7,107,245	B1 *	9/2006	Kowalick	705/44
7,338,372	B2	3/2008	Morrow et al.	
7,341,522	B2	3/2008	Yamagishi	
7,534,169	B2	5/2009	Amaitis et al.	
7,611,407	B1	11/2009	Itkis et al.	
7,753,772	B1 *	7/2010	Walker et al.	463/17
8,029,349	B2	10/2011	Lind	
2001/0004768	A1	6/2001	Hodge et al.	
2001/0005908	A1	6/2001	Hodge et al.	
2002/0002073	A1	1/2002	Montgomery et al.	
2002/0007494	A1	1/2002	Hodge	
2002/0056125	A1	5/2002	Hodge et al.	
2002/0056143	A1	5/2002	Hodge et al.	
2002/0077167	A1 *	6/2002	Merari	463/13
2002/0142815	A1	10/2002	Candelore	
2002/0142844	A1	10/2002	Kerr	
2003/0119578	A1 *	6/2003	Newson	463/20
2006/0003830	A1 *	1/2006	Walker et al.	463/20
2006/0189382	A1	8/2006	Muir et al.	
2007/0087834	A1	4/2007	Moser et al.	
2007/0270212	A1	11/2007	Cockerille et al.	
2008/0026844	A1	1/2008	Wells	
2008/0057894	A1	3/2008	Aleksic et al.	
2008/0097858	A1	4/2008	Vucina et al.	

OTHER PUBLICATIONS

Wirelss Network. Wikipedia. http://en.wikipedia.org/wiki/Wireless_network. Nov. 17, 2008.

"Tracking Cookie." Wikipedia. http://en.wikipedia.org/wiki/Tracking_cookie. May 24, 2009.

* cited by examiner

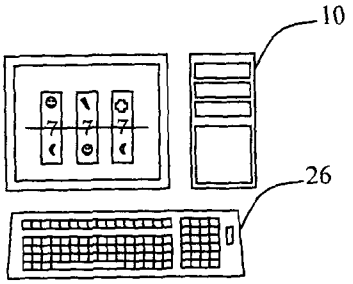


FIG. 1a

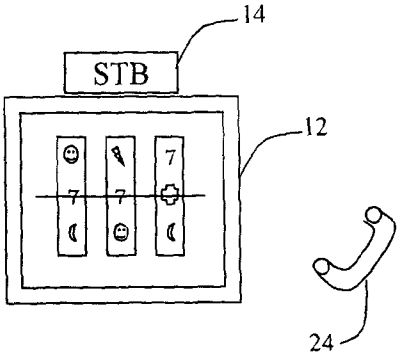


FIG. 1b

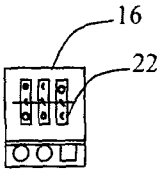


FIG. 1c

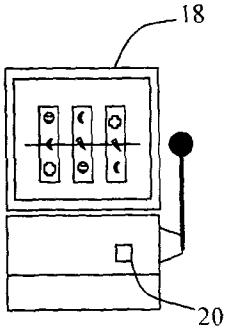
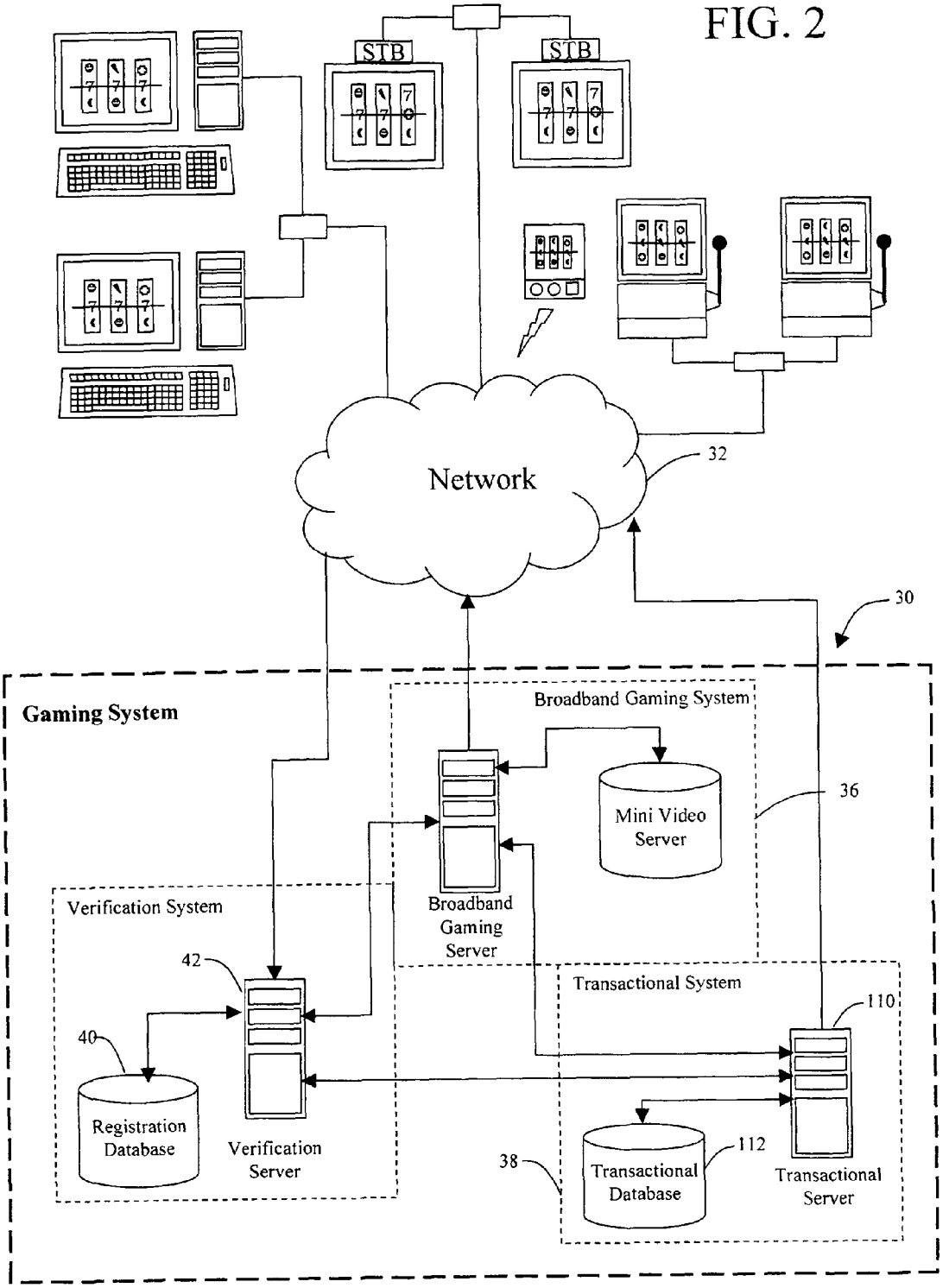


FIG. 1d

FIG. 2


STB
STB
Network
32
30
Gaming System
Broadband Gaming System
Mini Video Server
36
Broadband Gaming Server
Verification System
42
40
Registration Database
Verification Server
Transactional System
110
38
Transactional Database
112
Transactional Server

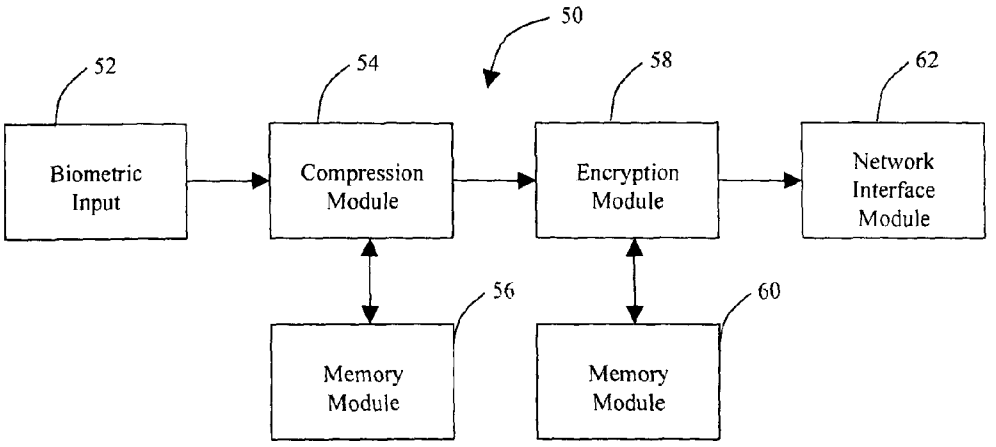

50
52
54
58
62
Biometric Input
Compression Module
Encryption Module
Network Interface Module
56
60
Memory Module
Memory Module

FIG. 3

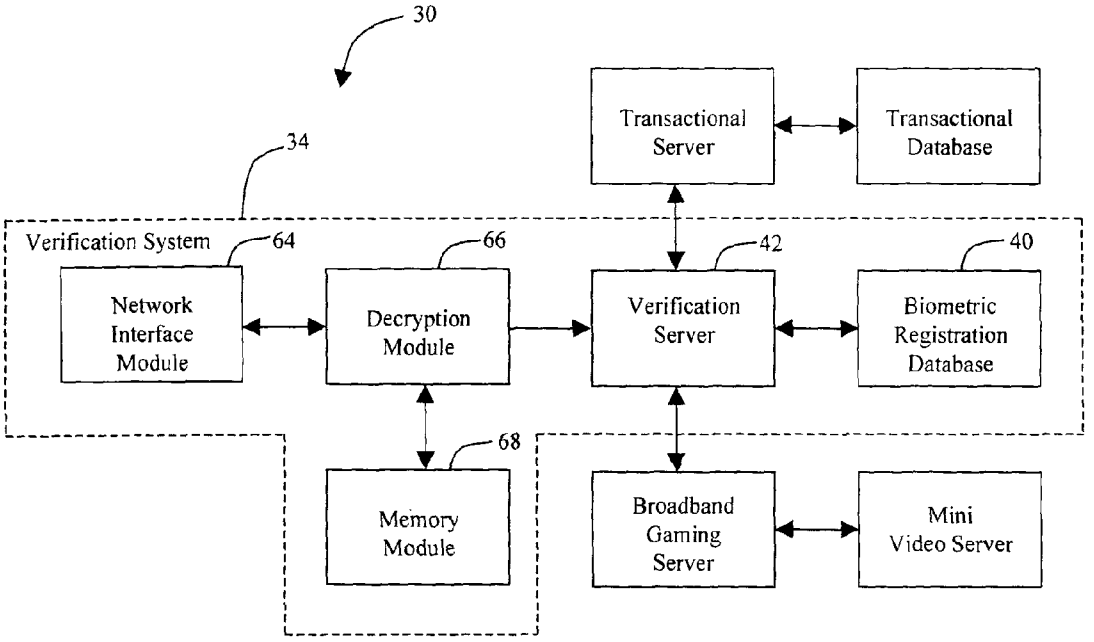

30
34
Transactional Server
Transactional Database
Verification System
64
66
42
40
Network Interface Module
Decryption Module
Verification Server
Biometric Registration Database
68
Memory Module
Broadband Gaming Server
Mini Video Server

FIG. 4

70

REGISTRATION DATA FIELDS	
NAME	BIOMETRIC
ADDRESS	PLAYER ID
USER NAME	MAC ID
PASSWORD	IP ADDRESS
CREDIT CARD	BROWSER
DATE	COOKIES
TIME	CRYPTO KEYS

72

USER SUBMITTED DATA	
NAME	BIOMETRIC
ADDRESS	PLAYER ID
USER NAME	MAC ID
PASSWORD	IP ADDRESS
CREDIT CARD	BROWSER
DATE	COOKIES
TIME	CRYPTO KEYS

FIG. 5

74

PLAYER DATA FIELDS	
PLAYER ID	SESSION TIME FOR TYPE OF GAME
DATE	AMOUNT PLAYED DURING SESSION
TIME IN	CREDIT CARD INFORMATION
TIME OUT	TRANSACTION REQUEST
TYPE GAME	TRANSACTION APPROVAL
CREDITS IN	TRANSFER OF CREDITS
CREDITS OUT	TRANSFER TO PLAYER CREDIT CRD
BONUS	CRYPTO KEYS

FIG. 6

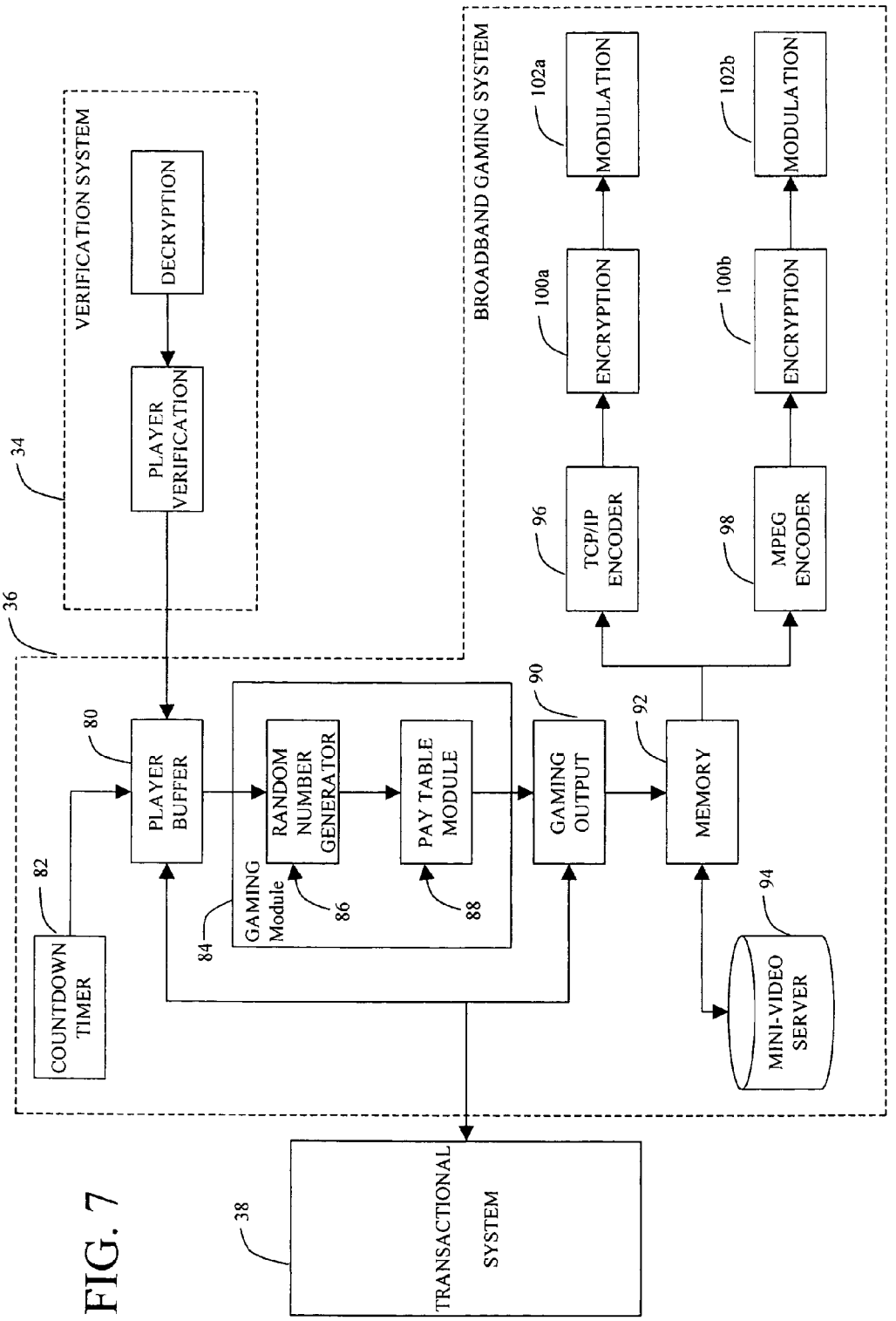

VERIFICATION SYSTEM
DECRYPTION
PLAYER VERIFICATION
34
36
BROADBAND GAMING SYSTEM
102a
MODULATION
102b
MODULATION
100a
ENCRYPTION
100b
ENCRYPTION
96
TCP/IP ENCODER
98
MPEG ENCODER
80
PLAYER BUFFER
RANDOM NUMBER GENERATOR
PAY TABLE MODULE
90
GAMING OUTPUT
92
MEMORY
82
COUNTDOWN TIMER
GAMING Module
84
86
88
94
MINI-VIDEO SERVER
38
TRANSACTIONAL SYSTEM

FIG. 7

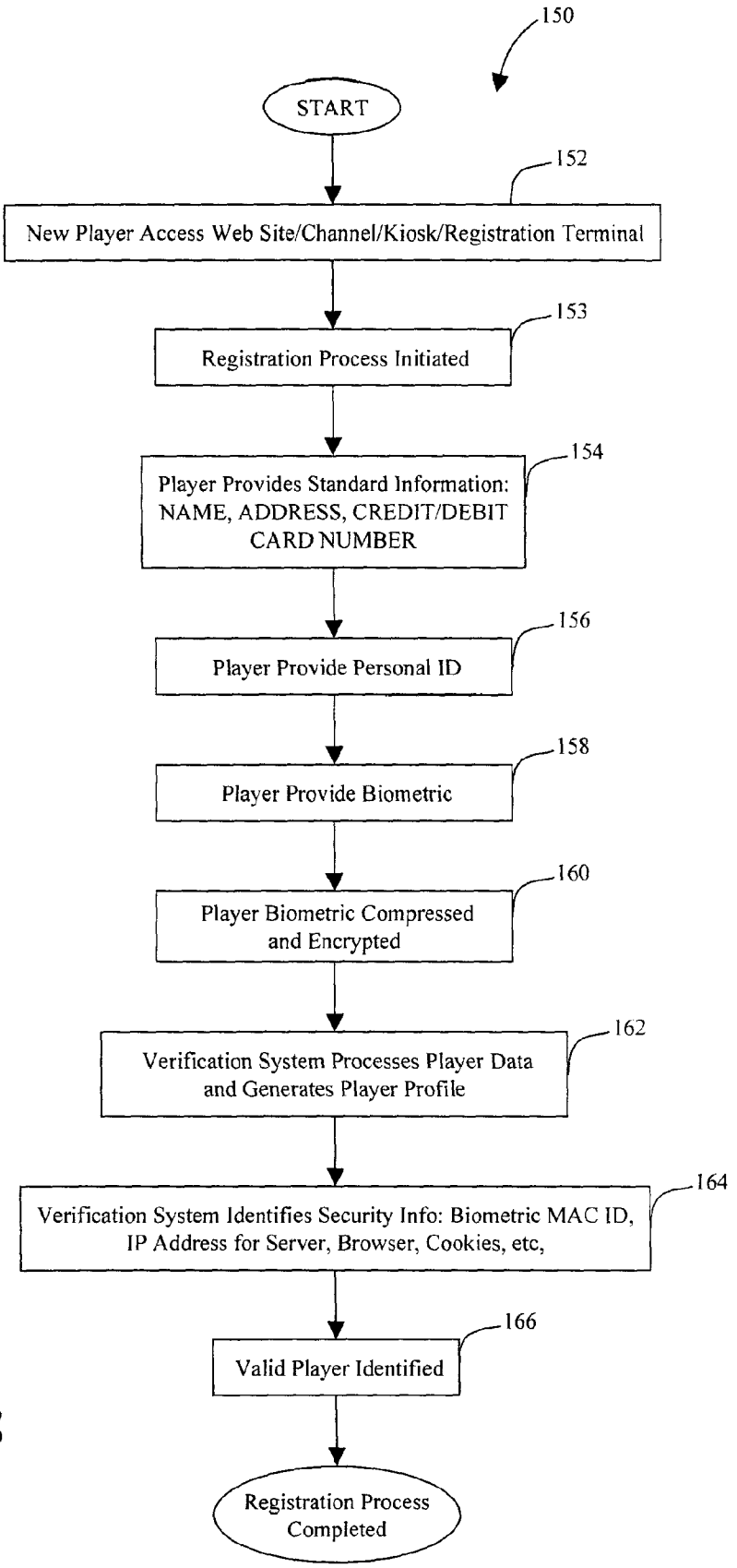

150
START
152
New Player Access Web Site/Channel/Kiosk/Registration Terminal
153
Registration Process Initiated
154
Player Provides Standard Information: NAME, ADDRESS, CREDIT/DEBIT CARD NUMBER
156
Player Provide Personal ID
158
Player Provide Biometric
160
Player Biometric Compressed and Encrypted
162
Verification System Processes Player Data and Generates Player Profile
164
Verification System Identifies Security Info: Biometric MAC ID, IP Address for Server, Browser, Cookies, etc,
166
Valid Player Identified
Registration Process Completed

FIG. 8

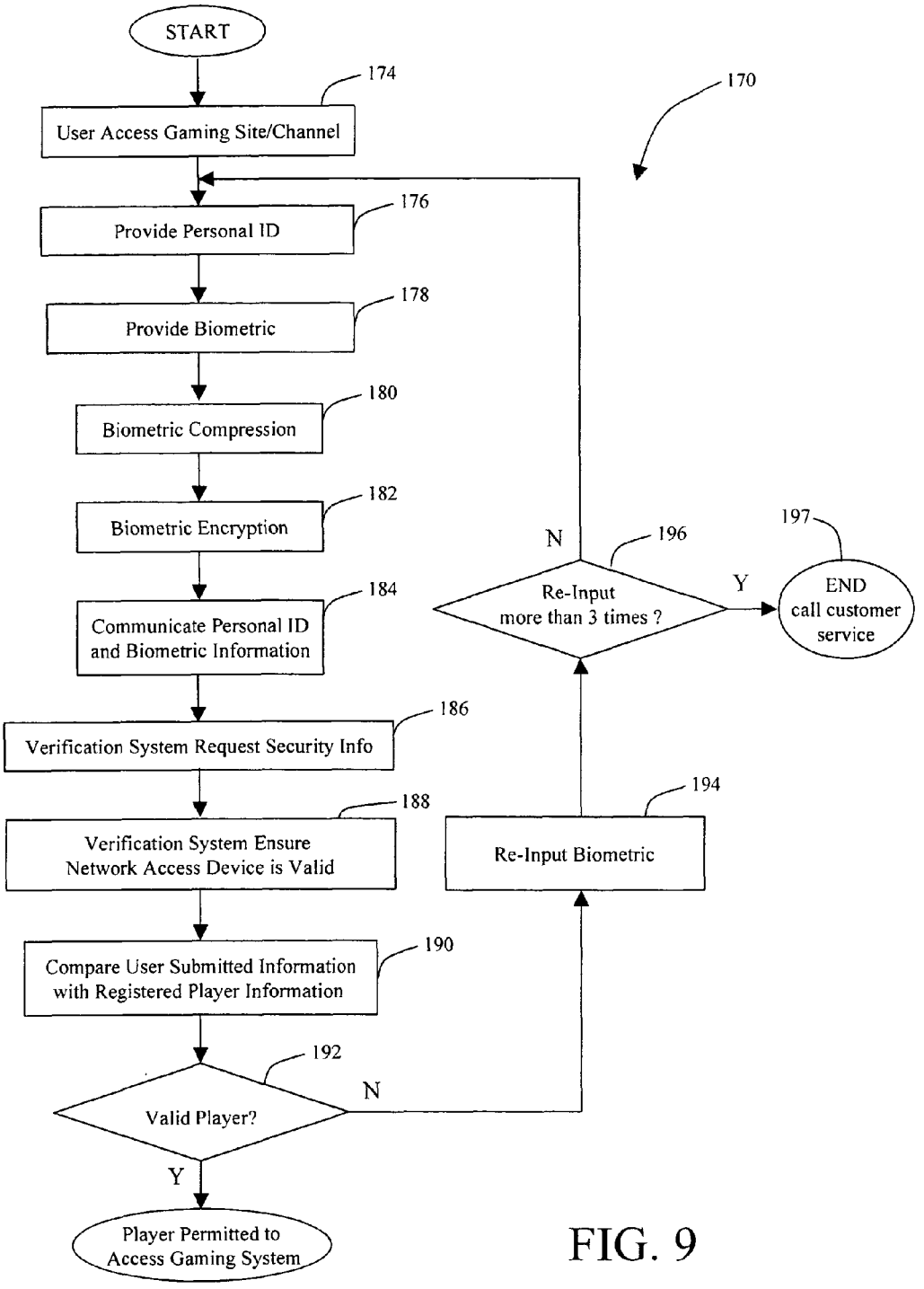

START
174
User Access Gaming Site/Channel
170
176
Provide Personal ID
178
Provide Biometric
180
Biometric Compression
182
Biometric Encryption
184
Communicate Personal ID and Biometric Information
186
Verification System Request Security Info
188
Verification System Ensure Network Access Device is Valid
190
Compare User Submitted Information with Registered Player Information
192
Valid Player?
N
Y
Player Permitted to Access Gaming System
196
Re-Input more than 3 times ?
N
Y
197
END call customer service
194
Re-Input Biometric

FIG. 9

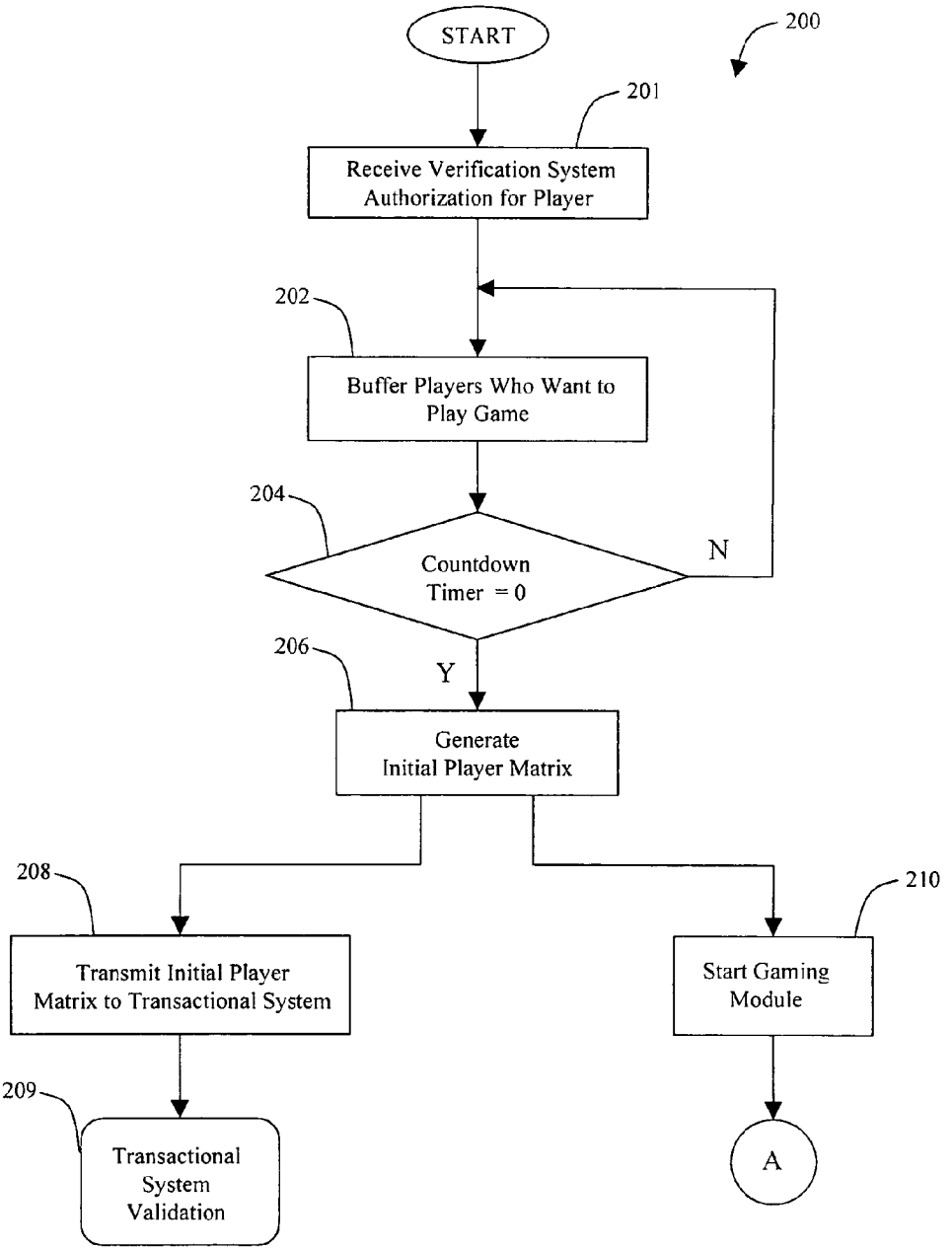

START
200
201
Receive Verification System Authorization for Player
202
Buffer Players Who Want to Play Game
204
Countdown Timer = 0
N
Y
206
Generate Initial Player Matrix
208
Transmit Initial Player Matrix to Transactional System
210
Start Gaming Module
209
Transactional System Validation
A

FIG. 10

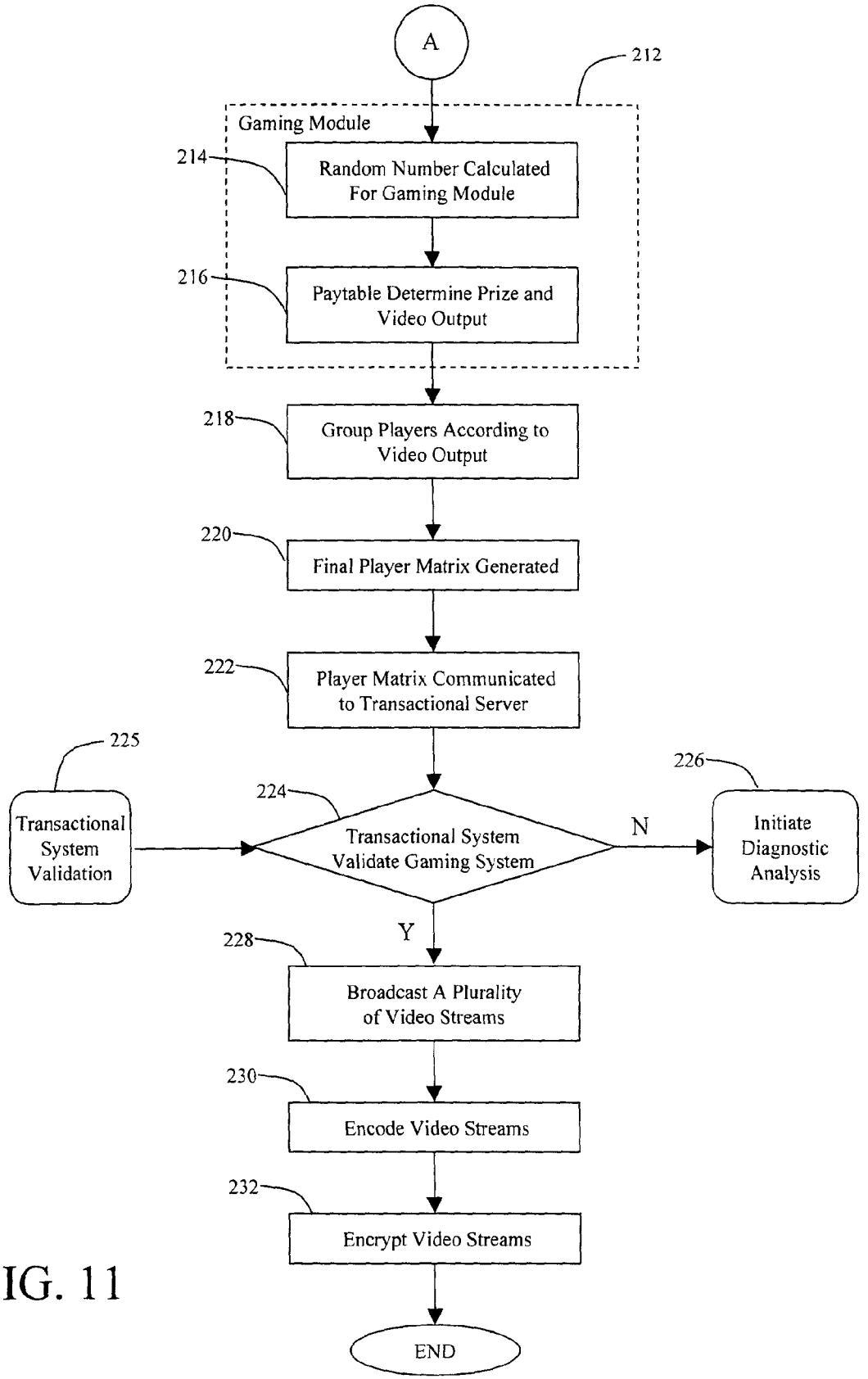

A
212
Gaming Module
214
Random Number Calculated For Gaming Module
216
Paytable Determine Prize and Video Output
218
Group Players According to Video Output
220
Final Player Matrix Generated
222
Player Matrix Communicated to Transactional Server
225
Transactional System Validation
224
Transactional System Validate Gaming System
N
226
Initiate Diagnostic Analysis
Y
228
Broadcast A Plurality of Video Streams
230
Encode Video Streams
232
Encrypt Video Streams
END

FIG. 11

NETWORK ACCESS DEVICE AND METHOD TO RUN A GAME APPLICATION

CROSS REFERENCES TO RELATED APPLICATIONS

This patent application is a continuation of Ser. No. 10/681,034, filed Oct. 8, 2003 now U.S. Pat. No. 8,403,755 which is a continuation of patent application Ser. No. 09/899,559 having a filing date of Jul. 5, 2001, now abandoned, which claims the benefit of provisional patent application 60/266,956 filed Feb. 6, 2001.

BACKGROUND

1. Field

The present invention is a network access device to run a gaming application and method for running a gaming application on a network access device. More particularly, the network access device and method receives a gaming output from a gaming server when identification and security information have been verified by a verification system.

2. Description of Related Art

The related art includes gaming devices, on-line gaming, networked interactive gaming, and biometrics.

Gaming Devices

For purposes of this patent, the term "gaming" shall refer to either gambling and/or gaming applications. Gaming devices include games of skill and games of chance. Games of chance include many casino-type gaming devices in which the outcome of the game depends, at least in part, on a randomly generated event. For example, a game of chance may use a random number generator to generate a random or pseudo-random number. The random number may then be compared to a predefined table to determine the outcome of the event. If the random number falls within a certain range of numbers on the table, the player may win a predefined prize. The table may also contain display information that allows the gaming device to generate a display that corresponds to the outcome of the game. The gaming device may present the outcome of the game on a large variety of display devices, such as mechanical spinning reels or video screens.

Games of skill comprise a skill component in which a player combines letters or words (word puzzles), answers questions (trivia), overcomes challenges (video games), competes with other players (networked video games), and the like. Generally, a game of skill is a game requiring a level of skill which does not rely solely on chance. Some games of skill require a high degree of expertise and knowledge and other games of skill require very limited expertise or knowledge.

On-Line Gaming

In June 2001, Nevada signed a bill that could result in Nevada being the first state to offer legalized gambling over the Internet. The new law authorizes state gaming regulators to set up an infrastructure to license and oversee online gaming in Nevada when such gaming becomes legal. Online gaming is a federal issue whose legality is unclear at present.

A variety of technological limitations have been asserted as preventing Congress's endorsement of on-line gaming. These technological limitations are related to the prevention of underage gambling, controlling of gambling addiction, and ensuring the security and reliability of on-line gaming.

To prevent underage gambling prior art systems and methods use passwords, user IDs, credit cards and "click-through" agreements that ask the player to agree to being of legal gambling age by clicking on a button. Presently, there are no

systems and methods to control on-line gambling addiction. With respect to ensuring that on-line gaming is secure and reliable, prior art systems and methods use various cryptographic techniques such as RSA encryption, digital certificates, or other similar well known cryptographic methods. These cryptographic methods are helpful in ensuring secure communications, however these cryptographic methods do not ensure that the individual accessing the on-line game is a valid user.

In view of the prior art systems, a minor or other unauthorized individual simply needs a user ID and a corresponding password to access a gaming site. The obtaining of a user ID and password is a relatively simple task as this information is generally not modified. Commonly the user ID information is acquired by identifying the web site's naming convention for the player. The player password can be easily determined by remembering the pattern of keys typed by the player during the log-on procedures or by simply requesting the password from the player as part of a diagnostic procedure. The latter is a trick commonly used by hackers to access a system. The password problem may be overcome by modifying the password on a regular basis, however the player must then remember the modified password. Should the player forget the password a new password is mailed. During the mailing process it is common for e-mail to be easily intercepted in cyberspace. Additionally, it is common for unauthorized users to simulate being at a certain location by submitting an IP address that identifies an authorized user.

Therefore, a better system and method for identifying a valid user is needed. Additionally, it would be beneficial to provide a gaming system and method that would prevent underage gambling, be simple to implement, prevent gambling addiction, and provide a higher degree of security and reliability from unauthorized users.

Networked Interactive Gaming

Networked interactive gaming in an open networked environment such as the Internet is well-known. However, interactive gaming in an open network such as the Internet is confined to communicating with other devices using the same TCP/IP protocols. Currently networked interactive gaming systems using the TCP/IP protocol are not configured to communicate with interactive set-top boxes using MPEG protocols.

Networked interactive gaming in an open networked environment using traditional security methods such as secure socket layers and digital certificates are well known. However, networked interactive gaming in an open networked environment using traditional security methods does not prevent gambling from a minor having acquired a parent's user ID and password without the parent's consent.

Networked interactive gaming using LANs and WANs for progressive slot machines having large jackpots are also well-known. However, networked interactive systems using LANs and WANs for progressive slot machines generally exist in a highly secure proprietary network environment. Thus, the creation of a progressive slot machine with a large jackpot in an open network environment is not well known.

Biometrics

A biometric is a measurable psychological and/or behavioral trait that can be captured and subsequently compared with another instance at the time of verification. This definition includes the matching of fingerprints, voice patterns, hand geometry, iris and retina scans, vein patterns and other such methodologies. For purposes of the invention described heretofore, the definition of biometrics also includes signature verification, keystroke patterns and other methodologies weighted towards individual behavior.

Biometric applications for games of skill and games of chance are limited. For example biometric gaming applications are taught in U.S. Pat. No. 6,010,404 granted to Walker et al. teaches a method and apparatus for using player input codes (e.g., numeric, biometric or physical) to affect the outcomes of electronic gambling devices, such as slot machines. Additionally, U.S. Pat. No. 6,142,876 granted to Cumbers teaches a system and method for passively tracking the play of players playing gaming devices such as slot machines. Players provide identification information and facial recognition data is acquired by a digital or video camera. For each player an account file and a file of the facial image data is stored. When the player plays the slot machine, a camera scans the player and acquires facial image data which is compared to stored data to identify the player. Furthermore, U.S. Pat. No. 5,902,983 granted to Crevelt et al. teaches a gaming machine configured to perform EFT transactions which are limited to preset amounts. The patent teaches the use of a fingerprint imaging device, and retinal scans for verifying a player's identity.

Although biometric applications for gaming applications are known, biometric applications for on-line gaming systems are not known. Furthermore, the managing of biometric information and gaming information in an open network environment are not known. Additionally, the use of biometrics in a gaming system and method to prevent underage gambling and prevent gambling addiction is not known.

SUMMARY

A network access device to run a gaming application is described. The network access device comprises a communications module configured to allow the network access device to communicate with a network. The network access device is configured to transmit user identification information to a verification system and transmit security information to a verification system. When the user identification information and security information have been verified by the verification system, the network access device receives a random game output generated by a gaming system.

In another embodiment, the network access device to run a gaming application comprises a communications module configured to allow the network access device to communicate with a network, a means for transmitting user identification information to a verification system and a means for transmitting security information to a verification system. The network access device also comprises a means for receiving a random game output generated by a gaming system. The network access device further comprises a means for displaying the images associated with the game output.

A method for running a gaming application on a network access device is also described. The method comprises transmitting user identification information to a verification system. The method further comprises transmitting security to the verification system. When the user identification information and security information are verified by the verification system, the network access device receives a random game output generated by a gaming system. The network access device displays at least one image associated with the random game output.

One advantage of the present invention is that it provides a system and method to prevent underage gambling.

A further advantage of the present invention is that it provides a more secure and reliable and secure gaming system and method.

Another advantage of the present invention is that it provides a system and method for managing biometric information and gaming information in an open network environment.

Another advantage of the present invention is that it permits a plurality of users in a geographically broad area to play the same game.

A further advantage of the present invention is that it provides a pseudo-real time gaming system and method.

Another advantage of the present invention is that it simulates a game of chance such as a slot machine in an on-line environment.

An additional advantage of the present invention is that it provides a networked jackpot.

BRIEF DESCRIPTION

A networked gaming system that comprises a verification system, a broadband gaming system and a transactional system is described. The verification system operations include ensuring that a user is a registered player by using a biometric input. The broadband gaming system operations include managing and performing at least one game. The transactional system operations include providing oversight for each transaction conducted by the verification system and the broadband gaming system.

A verification system for playing the networked gaming system is described. The networked games include games of chance and games of skill. The verification system communicates with a biometric input module and a network access device to generate a user identification information. The user identification information is compared to information in a registration database. If an acceptable match is made between the user identification information and the information in the registration database, the user is designated as a player. The player then has access to both the broadband gaming system and the transactional system.

A broadband gaming system which is in communication with the verification system is described. The broadband gaming system includes a buffer which stores information about players who desire to play a game. The buffer is operatively coupled to a random number generator that generates a random number for each player in the buffer. A paytable module in communication with the random number generator determines the outcome associated with the random number generator. The paytable also determines which images are associated with the outcome for each player. Preferably, the images are stored on a mini video server and then cached in a memory module. The images are intelligently buffered for downstream communications. In its preferred embodiment, a plurality of encoders are operatively coupled to the memory module caching the broadcast video streams. The plurality of encoders encode the broadcast downstream images according the requirements for each network access device. Each encoder is operatively coupled to an encryption module that encrypts the broadcast. A modulation module is operatively coupled to the encryption module and modulates encrypted images for downstream transmission. Each network access device includes a tuner, a demodulation module, and a decryption module that permits an image to be viewed by the network access device.

A transactional system and method that ensures secure communications occur in the verification system and the broadband gaming system is described. The transactional system also performs accounting, bonusing, tracking and other such functions. Preferably, the transactional system is

capable of receiving a plurality of funds from a financial account and converting them to credits that are used in the broadband gaming system.

The above description sets forth, rather broadly, the more important features of the present invention so that the detailed description of the preferred embodiment that follows may be better understood and contributions of the present invention to the art may be better appreciated. There are, of course, additional features of the invention that will be described below and will form the subject matter of claims. In this respect, before explaining at least one preferred embodiment of the invention in detail, it is to be understood that the invention is not limited in its application to the details of the construction and to the arrangement of the components set forth in the following description or as illustrated in the drawings. The invention is capable of other embodiments and of being practiced and carried out in various ways. Also, it is to be understood that the phraseology and terminology employed herein are for the purpose of description and should not be regarded as limiting.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the present invention are shown in the accompanying drawings wherein:

FIG. **1***a* through FIG. **1***d* provide diagrams of a plurality of network access devices.

FIG. **2** is a high level diagram of a gaming system networked to a plurality of network access devices.

FIG. **3** is a block diagram of an illustrative biometric input module.

FIG. **4** is a block diagram of a gaming system configured to receive a biometric input from a network access device.

FIG. **5** is a table of the data fields in a verification system.

FIG. **6** is a table of the data fields in a broadband gaming system and in a transactional system.

FIG. **7** is a block diagram of a broadband gaming system.

FIG. **8** is a flowchart of the registration method for the gaming system.

FIG. **9** is a flowchart of the verification method for the gaming system.

FIG. **10** is a flowchart of the information processed by the gaming system.

FIG. **11** is a continuation of the flowchart of the information processed by the gaming system in FIG. **10**.

DETAILED DESCRIPTION

In the following detailed description of the preferred embodiments, reference is made to the accompanying drawings, which form a part of this application. The drawings show, by way of illustration, specific embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

Network Access Devices

Referring to FIG. **1***a* through FIG. **1***d* there is shown a plurality of illustrative network access devices. Each of the network access devices is configured to be capable of running a gaming application. For illustrative purposes the gaming application shown simulates the spinning reels of a slot machine.

The network access device in FIG. **1***a* is a personal computer **10** having a network interface card (not shown) that may be operatively coupled to a modem (not shown). Another network access device shown in FIG. **1***b* includes a television **12** operatively coupled to an interactive set-top box **14** that is operatively coupled to a cable network (not shown). The other network access device shown in FIG. **1***c* is a wireless device **16** such as a digital phone or personal digital system (PDA) or other such wireless device which is configured to communicate with a network using wireless networking protocols. Yet another network access device is shown in FIG. **1***d* and includes a gaming terminal **18** such as a slot machine on a casino floor that is operatively coupled to a plurality of other gaming terminals. It shall be appreciated by those skilled in the art of networking that the distinguishing feature between each of these network access devices is the type of communications protocols used by each device to enable communications between similar network access devices.

Each of the network access devices either includes a biometric input module operatively coupled to the network access device or includes a biometric input module communicatively coupled to the network access device. A biometric is a measurable psychological and/or behavioral trait that can be captured and subsequently compared with another instance at the time of verification. This definition includes the matching of fingerprints, voice patterns, hand geometry, iris and retina scans, vein patterns and other such methodologies. For purposes of the invention described heretofore, the definition of biometrics also includes signature verification, keystroke patterns and other methodologies weighted towards individual behavior.

In one illustrative embodiment, the biometric input module is a fingerprint scanner **20** resident on the gaming terminal **18** wherein the biometric input is a fingerprint. In another illustrative embodiment, the biometric input module is the screen **22** of wireless device **16** wherein the screen is configured to receive a biometric input such as a user signature. In yet another illustrative embodiment, the biometric input module is a telephone **24** that is configured to receive a voice pattern from a user prior to engaging communications with the interactive set-top box **14**. In yet another illustrative embodiment the biometric input module is a keyboard **26** operatively coupled to computer **10** wherein the user is requested to input a keystroke pattern. An illustrative example of a biometric input module operatively coupled to the network access device is shown in FIG. **1***d* having the fingerprint scanner **20** on the gaming terminal **18**. An illustrative example of a biometric input module, e.g. the telephone **24**, communicatively coupled to the network access device, e.g. the interactive set-top box **14**, is shown in FIG. **1***b*.

The biometric input is used to prevent unauthorized gaming activity and efficiently store credits on the user's behalf. By way of example and not of limitation, unauthorized gaming activity includes preventing underage gaming and prohibiting players with histories of gambling addiction. Additionally, player credits may be stored on a network so that the player does not need to carry coins, paper currency, coupons, credit cards or debits cards to play a game. It shall be appreciated by those skilled in the art having the benefit of this disclosure that different biometric input modules may be used in conjunction with different network access devices.

Gaming System

Referring to FIG. **2** there is shown a high level block diagram of a gaming system **30** in communication with a plurality of network access devices coupled to a network **32**. The gaming system includes a verification system **34**, a broadband gaming system **36** and a transactional system **38**. The verification system **34** verifies that a user operating a network access device is a registered player. The broadband gaming system **36** performs the function of generating a game and broadcasting the game results to each of the network

access devices. The transactional system **38** performs a plurality of functions including tracking each transaction performed by both the verification system and the broadband gaming system and conducting electronic fund transfers.

Verification System

The verification system **34** verifies that a user desiring to play the game is a registered player. The verification system **34** communicates with the biometric input module and a network access device to generate user identification information. The user identification information includes information such as cryptographic keys that are necessary to securely identify the network access device. The user identification information also includes media access control (MAC) identification and confirmation of the user Internet Protocol (IP) address. The user identification information is compared to information in a registration database **40** by a verification server **42**. If an acceptable match is made between the user identification information and the information in the registration database, the user is designated as a player. The player then has access to either the broadband gaming system **36** or the transactional system **38**.

In an alternative embodiment the user identification information is housed in a smart card (not shown) that is in communication with the verification system **34**. The smart card includes a stored biometric which is used to identify the user as a player. Cryptographic keys are then exchanged between the verification system **34** and the smart card to provide the player access to either the broadband gaming system or the transactional system **38**.

Referring to FIG. **3** there is shown an illustrative biometric input module **50**. By way of example, the illustrative biometric input module **50** is a fingerprint scanner. It shall be appreciated by those skilled in the art having the benefit of this disclosure that the use of the fingerprint scanner as the illustrative biometric input module is not restrictive. A scanned fingerprint image is collected by the biometric input **52**. After the scanned fingerprint image is collected, the fingerprint image is compressed by the compression module **54**. A memory module **56** provides fast memory resources for the compression of the fingerprint image. After compression, the fingerprint image is encrypted by the encryption module **58** for downstream transmission. The encryption module **58** also includes a memory module **60** that provides fast memory resources for the encryption of the compressed fingerprint image. An encrypted compressed fingerprint image is then communicated to network **32** (see FIG. **2**) using the network interface module **62**.

Referring to FIG. **4** there is shown a block diagram of the verification system **34**. The verification system is operatively coupled to network **32** with network interface module **64**. The network interface module **64** is configured to receive user identification information generated by the network access devices and from the biometric input module. Preferably, the biometric and other user identification information received by the verification system is an encrypted biometric that is decrypted by decryption module **66**. A memory module **68** is preferably a fast memory that expedites the decryption process. After decryption the biometric and remaining user identification information is processed by the verification server. It shall be appreciated by those skilled in the art that the verification server **42** may house the network interface module **64**, decryption module **66** and the memory module **68**. The verification server **42** is also in operative communication with a registration database **40**. The verification server **42** performs the function of matching the user identification information collected from the network access device with the player information in the registration database **40**. Additionally, the verification server **42** performs the caching functions needed to ensure that once a player has been identified during an initial game, subsequent usage by the same player proceeds quickly.

Preferably, the verification server **42** identifies registered players using a biometric template of the registered player residing on the registration database **40**. The registered players are referenced with Personal ID numbers. When a transaction is undertaken the user firstly calls up the particular template from the registration database **40** by inputting a Personal ID. The Personal ID includes a particular number, user ID, password or other such identification techniques. The inputting of the Personal ID is accomplished with a familiar numeric keypad, keyboard, magstripe card or smart card. The correct template is called and held in memory ready for comparison with the biometric sample provided by the user. A comparison takes place that results in a binary true or false condition as to the identity of the user. The user is in effect claiming an identity by inputting the Personal ID and the system is subsequently verifying that the claim is genuine according to the matching criteria setup within the system.

Referring to FIG. **5** there is shown the registration data fields **70** and user submitted data fields **72**. The registration data fields **70** include data fields that comprise the user identification information. The registration data fields include user identification information such as player name, address, user name, password, credit card information, and the date and time of the registration. The player biometric and Personal ID also comprises the user identification information and provides unique information about the player. The Personal ID may be the same as the user name or password. It shall be appreciated by those skilled in the art that some biometric information may be compressed. Furthermore, the user identification information includes data about the network access device and the network connection such as MAC ID, IP addresses, browser type, any cookies resident on the network access device, etc. Finally, the user identification system includes cryptographic keys which are used to encrypt and decrypt the communications between the verification system and each of the network access devices.

The user submitted data fields **72** mirror the registration data fields **70**. The user submitted data fields receive data generated by a user that is attempting to access the broadband gaming system **36**. The user submitted information is carefully analyzed to ensure that a valid user is being identified. It is well known that the connection of one network access device to another network access device generates security concerns. Preferably, the present verification system operates using a fast hardware-type firewall that performs a stateful multilayer inspection. In its preferred embodiment the firewall provides packet filtering using a secure protocol such as IPSec. This protocol provides encryption of the data at the packet level as well as at the source address level. Without access to the encryption keys, a potential intruder would have difficulty penetrating the firewall. Additionally, it would be preferable to provide a circuit level gateway and an application level gateway. The circuit level gateway works on the session layer of the OSI model or the TCP layer of the TCP/IP model and monitors TCP handshaking between packets to determine whether a requested session is legitimate. The application level gateway filters data packets at the application layer of the OSI model. A stateful multilayer inspection firewall offers a high level of security, good performance and transparency to end users.

Referring to FIG. **6** there is shown the player data fields **74** that are generated by the broadband gaming system and the transactional system after the user has been verified to be a

registered player. The player data fields **74** are used to generate a player matrix which is used as an additional internal security measure. The player data fields **74** include a Player ID that identifies the player, a timestamp that provides the date, time in and time out by the player during the game. Additionally, the type of game, credits played, and credits remaining are monitored. Based on the level of player activity a bonus is provided to the player. Further still the session time for each type of game and the amount played during the session is monitored to better define the type of games the players' like. Transactional information is also monitored and updated, preferably, by the transactional system **38**. The transactional information includes credit card information, transaction requests, transaction approval, conversion of monetary funds to credits for playing the game, any transfers of credits for playing the game, and conversions from credits to monetary funds that are credited to the player's financial account. Preferably, communications between the transactional system and the broadband gaming system are conducted in a secure environment using cryptographic keys. Although the use of cryptography within the private network may appear excessive one of the greatest security threats within a private network comes from its own employees. Therefore, it is preferable to use internal firewalls for communications between the broadband gaming system, the transactional system and the verification system.

Broadband Gaming System

A more detailed drawing of the broadband gaming system is provided in FIG. **7**. The dashed boundary in FIG. **7** defines the broadband gaming system **36**. After player verification is completed at the verification system **34**, the broadband gaming system **34** is engaged. The broadband gaming system **34** includes a player buffer **84** configured to receive the players who will be playing the game. The player buffer **84** generates an initial player matrix with player data fields **74**.

A countdown timer **82** is coupled to the player buffer **80**. Preferably, the countdown timer **82** is also displayed to the player. The countdown timer **82** provides a window of time within which players may join the game. The players that have joined the game before the end of the timing period are stored in the buffer. When the timing period reaches zero the initial player matrix is communicated to the transactional system **38** and to the gaming module **84**.

The gaming module **84** provides a game that is played by the plurality of players. The game may include a plurality of different games and the type of game is not restrictive to this invention. Preferably, the gaming module **84** includes at least one random number generator **86** and a paytable module **88**.

The random number generator **86** is operatively coupled to the player buffer. The random number generator **86** generates at least one random number that is stored in the player matrix. In one embodiment, at least one random number is generated for the plurality of players playing the game. In an alternative embodiment, at least one random number is generated for each player. In yet another embodiment, a plurality of random numbers are generated that are applied to the plurality of players playing the game. Preferably, the random number generator **86** is a fast hardware module.

A paytable module **88** is operatively coupled to the random number generator **86**. The paytable module **88** is a programmable module that determines the type of prize awarded to the player based on the random number generated by the random number generator **86**. In one embodiment, the paytable module **88** is a field programmable gate array. Preferably, the paytable module **88** also includes an image ID that is associated with the outcome determined by the paytable module **88**.

A gaming output module **90** revises the player matrix to include the outcome for each player. Additionally, the gaming output module **90** groups the players according to the image ID. Based on the results generated by the gaming module **84**, the gaming output module **84** generates a final player matrix that is communicated to the transactional server **38** and to a memory module **92**.

Preferably, the memory module **92** has stored a plurality of images in a fast memory by the time the final player matrix is communicated to the memory module **92**. In operation, the memory module **92** is enabled before the final matrix is communicated to the memory module **92**. By way of example, when the game is engaged the memory module **92** begins the process of finding the applicable images associated with the image IDs in the mini-video server **94** and transferring the images to the fast memory module **92**. Thus, when the gaming output is received by the memory, the images are stored in the fast memory module **92**. In one embodiment, the memory module **92** then broadcasts the images to encoders **96** and **98**. In an alternative embodiment, the memory module **92** is operatively coupled to an intelligent router (not shown) that routes the images to the appropriate encoders **96** and **98**.

The appropriate encoder then receives the images and converts them to a format which meets the requirements for the appropriate network access device. By way of example, an IP encoder **96** encodes a plurality of JPEG images for viewing on a conventional web browser, and an MPEG encoder **98** encodes the plurality of JPEG images into an MPEG stream that is viewed on a television via an interactive set-top box.

An encryption module **100***a* and **100***b* operatively coupled to encoder **96** and **98**, respectively, then receives the encoded images and encrypts the encoded images in manner well known to those skilled in the art. A modulation module **102***a* and **102***b* is operatively coupled to encryption modules **100***a* and **100***b*, respectively, then modulates encrypted encoded images for downstream transmission in a manner well known to those skilled in the art.

Preferably, the broadband gaming system occupies one downstream band, i.e. one 6 or 8 MHz band, in the interactive set-top-box environment. In the web based broadcast environment, the broadband gaming system occupies a downstream channel much like a standard streaming media website.

It shall be appreciated by those skilled in the art having the benefit of this disclosure that the broadband gaming system can play more than one game at a time. The system may be designed to operate in a multi-tasking mode where more than one game is played at a time. Additionally, the system may be designed to operate in a fast serial mode in which a game is played while the countdown timer is waiting for the next queue to be filled.

Transactional System

Referring back to FIG. **2**, there is shown the transactional system **38** which comprises a transactional server **110** and a transactional database **112**. The transactional system **38** performs a plurality of functions including tracking each transaction performed by both the verification system and the broadband gaming system. Additionally, the transactional system **38** is configured to authorize and conduct electronic fund transfers. Furthermore, the transactional system **38** performs such operations as player tracking, managing loyalty programs, engaging bonus games, determining bonus prizes and interfacing with accounting programs.

Method for Registering a Player

Referring to FIG. **8** there is shown a flowchart of the registration method for the gaming system **30**. The registration method **150** begins when a prospective player first accesses a

website, channel, kiosk or other such registration terminals as described in block **152**. The method then proceeds to block **153**.

At block **153**, the registration process is initiated. By way of example and not of limitation, a registration terminal may provide a hyperlink to a registration window that prompts the prospective player for information. The method then proceeds to block **154**.

At block **154**, the prospective player provides registration identification information such as name, address, credit card number and other information necessary to create a registration file for the prospective player. The method then proceeds to block **156**.

At block **156**, the prospective player is prompted for a personal ID. The personal ID may be a user ID, a password, a numeric combination, or any other such identification information. The personal ID is used during the verification process to identify a biometric template for the prospective player. The method then proceeds to block **158**.

At block **158**, the prospective player submits a biometric to the registration terminal. By way of example and not of limitation the biometric is a fingerprint. Any other biometric may also be used. The method then proceeds to block **160** or **162**.

At block **160**, the biometric input is compressed and encrypted. It is preferable for certain biometric inputs to be compressed such as fingerprint scans, retinal scans and other such scanning techniques. Other biometric inputs such as voice patterns and signatures do not have to be compressed. The process of encrypting biometric inputs is necessary in an open network environment. The process of encrypting may not be necessary on a private proprietary network. Therefore, it shall be appreciated by those skilled in the art having the benefit of this disclosure that the compression and encryption processes in block **160** may not be necessary for every biometric input.

At block **162**, the prospective player information is stored in the verification system and a player profile is updated accordingly. Alternatively, the prospective player information is stored on a smart card. The method then proceeds to block **164**.

At block **164**, security information about the registration terminal is collected. The registration information identifies the registration terminal as being a secure terminal. The registration terminal provides information such as the MAC ID for the biometric input module, the IP address for the server communicating with the registration terminal, and the cryptographic keys associated with the registration terminal. The registration terminal includes the network access devices described in FIG. **1***a* through FIG. **1***d* as well as kiosks and other such registration terminals.

At block **166**, the prospective player is identified as a registered player and the registration database **40** is updated accordingly. The registration process is broken out into separate components for security purposes. Once a validly registered player is identified by the verification system, the registration process is completed.

Method for Player Verification

Referring to FIG. **9** there is shown a method **170** for player verification used by the verification system **34**. The player verification process includes receiving user identification information from a network access device. The method is initiated at block **174** when a user accesses a website or channel displaying the game. The method then proceeds to block **176**.

At block **176**, the personal ID is provided by the user. The personal ID is used by the verification system to find a biometric template for determining whether the user is a registered player. The method then proceeds to block **178**.

At block **178**, the biometric input module of the network access device receives a biometric from the user. As previously described the biometric input module can be one of plurality of biometric inputs. Depending on the type of biometric, the biometric may be compressed as described by block **180** and encrypted as described by block **182**. At block **184**, the biometric and the personal ID is then communicated through a network **32** to the verification system **34**. Alternatively, the biometric and Personal ID is communicated to a smart card for verification.

At block **186**, the verification system **34** requests security information from the network access devices. The security information identifies the network access devices as being a valid network access device. The method then proceeds to block **188**.

At block **188**, the verification system **34** processes the security information to ensure that the security information is generated by the appropriate network access device, and to ensure that the security information has not been compromised. Preferably, the verification system **34** performs a stateful multilayer inspection as described above. The method then proceeds to block **190**.

At block **190**, the user submitted player information is compared to the registered player information. If a determination is made at decision diamond **192** that the submitted player information is not a valid registered player the method proceeds to block **194**. At block **194**, the user is requested to re-input the biometric. If the biometric is input more than three times, as provided by decision diamond **196**, the user is requested to contact customer service.

If a match is found at decision diamond **192** between the user submitted information and the registered player information, the user is identified as a valid player then the player proceeds to the broadband gaming system **36**.

Method for Operation of Broadband Gaming System

Referring to FIG. **10** and FIG. **11** there is shown a flowchart **200** of the information processed by the broadband gaming system **34**. The process is engaged by performing the verification process in which the verification system identifies a player as in block **201**. After the verification process has been completed the method proceeds to block **202**.

At block **202**, the players who desire to play a particular game are stored in a buffer until the particular game is engaged. The method then proceeds to decision diamond **204**.

At decision diamond **204**, the countdown timer **82** determines if the period during which the game is open has been closed. If the game remains open, additional players may be received by the broadband gaming system. If the game is closed because the period during which the game is open has expired, then the method proceeds to block **206**.

At block **206**, the initial player matrix described above is generated. The initial player matrix includes information about the player, the type of game, and other such information about the game as described by the player data fields **74** shown in FIG. **6**. The initial player matrix is then communicated to block **208** which transmits initial player matrix to the transactional system for validation. Additionally, the initial player matrix is communicated to the next block **210** in the broadband gaming system which starts the gaming module.

At block **210**, the initial player matrix is received by the gaming module **84** and the gaming module **84** is engaged. At a minimum the gaming module **84** comprises a random number generator **86** and a paytable module **88**. The random number generator generates at least one random number that

is used during the game. The paytable module **88** is used to determine the prize associated with the at least one random number.

Referring to FIG. **11**, a continuation of the broadband gaming system method is shown. By way of example, the gaming module may comprise a plurality of different random number generators. The blocks **214** and **216** describe the processes performed by a random number generator and a paytable module, respectively. The random number generator **86** of block **214** determines the winning combination of numbers for the game. At block **216**, the paytable module **88** is used to determine the prize awarded to the player. Preferably, the paytable module **88** is also configured to provide image IDs that identify the images associated with the prize. Preferably, the paytable module **88** is resident in both the broadband gaming system and the transactional system. The purpose for this redundancy is as a security check for output generated by the gaming module. The method then proceeds to block **218**.

At block **218** the player outputs with the same image IDs are grouped together. The grouping process is performed to simplify the broadcasting of the images to the plurality of players. By grouping the players according to the same image ID and having identified the network access device used by the player, a dynamic broadcasting method is created which occupies minimal downstream bandwidth. The method then proceeds to block **220**.

At block **220** a final player matrix is completed. The final player matrix includes the same data fields as the initial player matrix. Additionally, the final player matrix includes the random number output and the paytable output. The final player matrix is then communicated to the transactional system as described in block **222**. The method then proceeds to decision diamond **224**.

At decision diamond **224**, a validation procedure is conducted. The validation procedure essentially compares the transactional system's reverse calculation of the random numbers with the random numbers generated by the gaming module. If the random numbers in the transactional system are not the same or similar to the random numbers generated by the random number generator, a system failure or security breach is detected. If a security breach or system failure is detected, the method then proceeds to process block **226**, which initiates diagnostic procedures. If the random numbers match, then the method proceeds to block **228**.

At block **228**, the plurality of images are broadcast. The images are preferably broadcast along one downstream channel for each network access device. However, traffic considerations may require the use of a plurality of downstream channels. By way of example, for DOCSIS and DSL type downstream transmissions, the streaming video preferably occupies a portion of the bandwidth available for a cable modem or DSL modem, respectively. In an alternative example, for an interactive set-top box environment, the downstream channel preferably occupies one 6 MHz or 8 MHz band or a portion of the 6 MHz or 8 MHz band. The method then proceeds to the next block **230**.

At block **230**, the broadcast images are encoded for downstream transmission. It shall be appreciated by those skilled in the art having the benefit of this disclosure that downstream transmission systems are well known and can be easily integrated into the systems and method described in this patent. The method then proceeds to block **232**.

At block **232**, the broadcast images are encrypted for downstream transmission. The purpose for downstream encryption is to prevent unauthorized access to the downstream signal. It shall be appreciated by those skilled in the art that various secure systems and methods for downstream transmission of images are well known.

It shall be appreciated by those skilled in the art having the benefit of this disclosure that a plurality of games may be played simultaneously. The games may be played in a distributed/parallel manner or in serial manner.

An Illustrative Game

An illustrative game is described to show how the system and method described above operates. The illustrative game described herein is a progressive slot machine. It is well-known that in the United States many states have legalized lottery games even though other games of chance such as progressive slot machines have not been legalized. It is also well-known that in casino gaming floors the most popular games are progressive slot machines. The present illustrative game operates on the system and method described above and provides an output similar to a progressive slot machine with a lottery type input.

The illustrative game includes first having a player provide a plurality of letters or numbers that are either generated by the player or are selected in a random manner. The random number generator of the gaming module is then engaged and a gaming module random number is generated. Preferably, the order that the random numbers were generated is used to determine the prize awarded to the player. A programmed paytable is then used to compare the player selected numbers to the gaming module random numbers according to the rules programmed into the paytable module. Based on the results of this comparison a prize is awarded to the player. An image ID is associated with the prize awarded. The plurality of players are then grouped according to their respective image IDs. A broadcast stream for the plurality of images associated with each image ID is broadcast to each player.

A more concrete example includes having a player select a plurality of numbers, such as the numbers below:

25 35 8 15 42

The random number generator of the gaming module is then engaged. By way of example the random number results are:

56 2 3 8 42

The paytable module is then programmed to interpret the random numbers generating by the gaming module according to the following illustrative rules:

1. If a match between one number is achieved, then a prize of 1× the initial bet credit is awarded and an image ID XQ23-1396 is used. Image ID XQ231396 is an animated plurality of images representing three cherries.

2. If a match between one number at the same location is achieved, then a prize of 2× the initial bet credit is awarded and an image ID XQ23-1397 is used. Image ID XQ23-1397 is an animated plurality of images representing four cherries.

3. If a match between a first number is achieved and a match between a second number is achieved, then a prize of 5× the initial credit is awarded and an image ID XQ23-1998 is used. Image ID XQ23-1998 is an animated plurality of images representing 3 oranges.

4. If a match between a first number at the same location is achieved and a match between a second number is achieved, than a prize of 7× the initial credit is awarded and an image ID XQ23-1999 is used. Image ID XQ23-1999 is an animated plurality of images representing 4 oranges.

Thus, for the illustrative example provided above, the player having selected the numbers: 23, 35, 8, 15 and 42 is entitled to a prize of 7× the initial credit for a random number: 56, 2, 3, 8, and 42. The associated images displayed on the network access device is an animated plurality of images representing 4 oranges.

The scope of the invention should be determined by the appended claims and their legal equivalents rather than by the examples given.

What is claimed is:

1. A system to run a gaming application on a network access device, comprising:

the network access device; and

a remote gaming system including a verification system;

the network access device configured to transmit user identification information and security information to the verification system;

the network access device configured to receive an acknowledgement from the verification system indicating that the user identification information and security information are valid;

the network access device configured to receive a game input from a user of the network access device and transmit the game input to the remote gaming system;

the remote gaming system configured to receive the game input and generate a random game output, the remote gaming system further configured to associate an image ID with the random game output and select one or more images associated with the image ID for encoding and broadcasting to the network access device;

the network access device configured to receive a plurality of broadcast images generated by the remote gaming system.

2. The system of claim **1**, wherein the plurality of broadcast images received by the network access device is displayed on a web browser.

3. The system of claim **1**, wherein the plurality of broadcast images is encrypted.

4. The system of claim **1**, wherein the network access device is a gaming terminal.

5. The system of claim **3**, wherein the gaming terminal is a slot machine.

6. The system of claim **1**, wherein the network access device is a wireless device.

7. The system of claim **1**, wherein the network access device is a display that is operatively coupled to an interactive set-top box.

8. The system of claim **1**, wherein the network access device is a personal computer having a network interface card.

9. A system to run a gaming application on a network access device, comprising:

the network access device;

a remote gaming system including a verification system;

means for transmitting user identification information and security information from the network access device to the verification system;

means for receiving an acknowledgement from the verification system indicating that the user identification information and the security information are valid;

means for receiving a game input from a user of the network access device and for transmitting the game input to the remote gaming system;

means for generating a random game output with the remote gaming system, the remote gaming system including means for associating an image ID with the random game output and selecting one or more images associated with the image ID for encoding and broadcasting to the network access device;

means for receiving on the network access device a plurality of broadcast images generated by the remote gaming system; and

means for displaying on the network access device the plurality of broadcast images.

10. The system of claim **9**, wherein the means for displaying the plurality of broadcast images comprises a web browser.

11. The system of claim **9**, wherein the means for displaying a plurality of broadcast images comprises a means for displaying encrypted broadcast images.

12. The system of claim **9**, wherein the network access device is a gaming terminal.

13. The system of claim **12**, wherein the gaming terminal is a slot machine.

14. The system of claim **9**, wherein the network access device is a wireless device.

15. The system of claim **9**, wherein the network access device is a display that is operatively coupled to an interactive set-top box.

16. The system of claim **9**, wherein the network access device is a personal computer having a network interface card.

17. A method for running a gaming application on a network access device, comprising:

transmitting user identification information and security information to a verification system;

receiving an acknowledgement from the verification system indicating that the user identification information and the security information are valid;

receiving a game input from a user of the network access device;

transmitting the game input to a remote gaming system, the remote gaming system generating a random game output and associating an image ID with the random game output; and

receiving a plurality of broadcast images generated by the remote gaming system, the remote gaming system selecting one or more images associated with the image ID, the remote gaming system encoding the one or more images into the plurality of broadcast images and broadcasting the plurality of broadcast images to the network access device.

18. The method of claim **17**, further comprising displaying the plurality of broadcast images on a web browser.

19. The method of claim **17**, wherein receiving a plurality of broadcast images includes:

receiving a plurality of encrypted broadcast images from the remote gaming system;

decrypting the plurality of encrypted broadcast images, resulting in a plurality of decrypted images; and

displaying the plurality of decrypted images.

* * * * *

US009646454B1

(12) **United States Patent**
Kerr

(10) **Patent No.: US 9,646,454 B1**
(45) **Date of Patent: *May 9, 2017**

(54) **NETWORKED GAMING SYSTEM AND METHOD**

(71) Applicant: **NEXRF, CORP.**, Reno, NV (US)

(72) Inventor: **Michael A. Kerr**, Reno, NV (US)

(73) Assignee: **NEXRF CORP**, Reno, NV (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 260 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/189,918**

(22) Filed: **Feb. 25, 2014**

Related U.S. Application Data

(63) Continuation of application No. 12/981,403, filed on Dec. 29, 2010, now Pat. No. 8,747,229, which is a continuation of application No. 10/681,034, filed on Oct. 8, 2003, now Pat. No. 8,403,755, which is a (Continued)

(51) **Int. Cl.**

G06F 17/00	(2006.01)
G07F 17/32	(2006.01)
G07F 17/34	(2006.01)

(52) **U.S. Cl.**
CPC ***G07F 17/3225*** (2013.01); ***G07F 17/329*** (2013.01); ***G07F 17/34*** (2013.01)

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,339,798 A	7/1982	Hedges et al.
4,856,787 A	8/1989	Itkis
5,586,937 A	12/1996	Menashe

(Continued)

FOREIGN PATENT DOCUMENTS

WO	2008065257 A1	6/2008

OTHER PUBLICATIONS

"Internet Industry Interacting Gambling Code: A Code for Industry Co-Regulation in the Area of Internet Gambling Content Pursuant to the Requirements of the Interactive Gaming Act of 2001." Internet Industry Association. Dec. 2001.

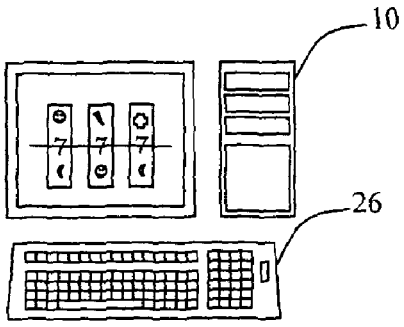
(Continued)

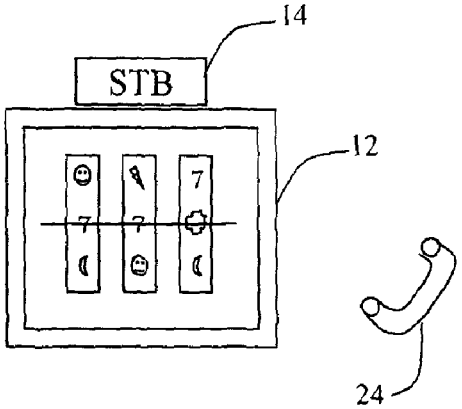
Primary Examiner — Paul A D'Agostino
(74) *Attorney, Agent, or Firm* — Kerr IP Group, LLC

(57) **ABSTRACT**

A networked gaming system and method is described. The networked gaming system and method include a user identification, a transactional component, a networked gaming module, and at least one network access device. The user identification is received by the network access device. The received user identification is compared with registration data in a registration database. A player is provided access to a game when the received user identification matches the registered player data. The transactional component charges the registered player at least one credit for a game outcome. The networked gaming module performs the game operations and generates at least one random game output by random generation at the networked gaming module. The networked gaming module then associates the at least one random game output with an image ID. The networked gaming module then communicates the one or more images corresponding to the image ID to the network access device.

28 Claims, 9 Drawing Sheets





Related U.S. Application Data

continuation of application No. 09/899,599, filed on Jul. 5, 2001, now abandoned.

(60) Provisional application No. 60/266,856, filed on Feb. 6, 2001.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,594,491	A	1/1997	Hodge et al.	
5,630,757	A	5/1997	Gagin et al.	
5,643,086	A	7/1997	Alcorn et al.	
5,738,583	A	4/1998	Comas et al.	
5,761,416	A	6/1998	Mandal et al.	
5,761,647	A	6/1998	Boushy	
5,762,552	A	6/1998	Vuong et al.	
5,768,382	A *	6/1998	Schneier	A63F 13/12 380/251
5,779,545	A	7/1998	Berg et al.	
5,795,228	A *	8/1998	Trumbull	A63F 13/12 463/42
5,800,268	A	9/1998	Molnick	
5,851,149	A	12/1998	Xidos et al.	
5,871,398	A	2/1999	Schneier et al.	
5,902,983	A	5/1999	Crevelt et al.	
5,947,821	A	9/1999	Stone	
5,970,143	A *	10/1999	Schneier	A63F 13/12 380/251
5,971,849	A	10/1999	Falciglia	
6,001,016	A *	12/1999	Walker	G07F 17/32 463/20
6,010,404	A *	1/2000	Walker	G07F 17/32 463/16
6,106,396	A	8/2000	Alcorn et al.	
6,142,876	A	11/2000	Cumbers	
6,159,095	A	12/2000	Frohn et al.	
6,178,510	B1	1/2001	O'Connor et al.	
6,203,428	B1	3/2001	Giobbi et al.	
6,217,447	B1 *	4/2001	Lofink	A63F 1/18 273/292
6,220,961	B1 *	4/2001	Keane	A63F 1/00 463/12
6,259,405	B1	7/2001	Stewart et al.	
6,322,446	B1	11/2001	Yacenda	
6,327,535	B1	12/2001	Evans et al.	
6,409,602	B1	6/2002	Wiltshire et al.	
6,500,068	B2	12/2002	Walker et al.	
6,508,709	B1	1/2003	Karmarker	
6,508,710	B1	1/2003	Paravia et al.	
6,527,638	B1	3/2003	Walker et al.	
6,554,705	B1	4/2003	Cumbers	
6,575,834	B1	6/2003	Lindo	
6,606,494	B1	8/2003	Arpee et al.	
6,612,928	B1	9/2003	Bradford et al.	
6,628,939	B2	9/2003	Paulsen	
6,638,170	B1	10/2003	Crumby	
6,640,218	B1	10/2003	Golding et al.	
6,676,522	B2	1/2004	Rowe	
6,682,421	B1	1/2004	Rowe et al.	
6,702,672	B1	3/2004	Angell et al.	
6,709,333	B1	3/2004	Bradford et al.	
6,709,631	B2	3/2004	Mori et al.	
6,719,631	B1	4/2004	Tulley et al.	
6,749,512	B2	6/2004	MacGregor et al.	
6,782,253	B1	8/2004	Shteyn et al.	
6,834,195	B2	12/2004	Brandenberg et al.	
6,875,110	B1	4/2005	Crumby	
6,879,838	B2	4/2005	Rankin et al.	
6,884,162	B2	4/2005	Raverdy et al.	
6,942,574	B1	9/2005	LeMay et al.	
7,035,651	B2	4/2006	Schreiner et al.	
7,076,243	B2	7/2006	Parupudi et al.	
7,107,245	B1 *	9/2006	Kowalick	G06Q 20/10 235/380
7,136,915	B2	11/2006	Rieger, III	
7,196,662	B2	3/2007	Misikangas et al.	
7,209,752	B2	4/2007	Myllymaki et al.	
7,213,048	B1	5/2007	Parupudi et al.	
7,218,941	B1	5/2007	Kubo et al.	
7,228,136	B2	6/2007	Myllymaki et al.	
7,299,059	B2	11/2007	Misikangas et al.	
7,338,372	B2	3/2008	Morrow et al.	
7,341,522	B2	3/2008	Yamagishi	
7,349,683	B2	3/2008	Misikangas	
7,359,714	B2	4/2008	Parupudi et al.	
7,397,424	B2	7/2008	Houri	
7,450,954	B2	11/2008	Randall	
7,493,565	B2	2/2009	Parupudi et al.	
7,529,639	B2	5/2009	Kikta et al.	
7,534,169	B2	5/2009	Amaitis et al.	
7,611,407	B1	11/2009	Itkis	
7,753,772	B1 *	7/2010	Walker	A63F 13/12 273/138.1
8,002,617	B1	8/2011	Uskela et al.	
8,029,349	B2	10/2011	Lind	
8,172,684	B2	5/2012	Adiraju et al.	
8,403,755	B2	3/2013	Kerr	
8,492,995	B2	7/2013	Maxik et al.	
8,506,406	B2	8/2013	Kerr	
8,506,407	B2	8/2013	Kerr	
8,523,679	B2	9/2013	Kerr	
8,738,024	B1	5/2014	Kerr et al.	
8,747,229	B2	6/2014	Kerr	
8,942,995	B1	1/2015	Kerr	
9,043,222	B1	5/2015	Kerr et al.	
2001/0004768	A1	6/2001	Hodge et al.	
2001/0005908	A1	6/2001	Hodge et al.	
2001/0031654	A1 *	10/2001	Walker	G07F 17/32 463/1
2001/0031656	A1 *	10/2001	Marshall	G06Q 50/34 463/6
2001/0036224	A1	11/2001	Demello et al.	
2001/0039210	A1	11/2001	St-Denis	
2001/0044337	A1	11/2001	Rowe	
2002/0002073	A1	1/2002	Montgomery et al.	
2002/0007494	A1	1/2002	Hodge	
2002/0056125	A1	5/2002	Hodge et al.	
2002/0056143	A1	5/2002	Hodge et al.	
2002/0061778	A1 *	5/2002	Acres	G07F 17/32 463/40
2002/0069105	A1	6/2002	do Rosario Botelho et al.	
2002/0077130	A1	6/2002	Owensby	
2002/0077167	A1	6/2002	Merari	
2002/0091568	A1	7/2002	Kraft et al.	
2002/0103028	A1	8/2002	Carter et al.	
2002/0111210	A1	8/2002	Luciano et al.	
2002/0111907	A1	8/2002	Ling	
2002/0133707	A1	9/2002	Newcombe	
2002/0142815	A1	10/2002	Candelore	
2002/0142844	A1	10/2002	Kerr	
2002/0142846	A1	10/2002	Paulsen	
2002/0144151	A1	10/2002	Shell et al.	
2002/0174436	A1	11/2002	Wu et al.	
2002/0198775	A1	12/2002	Ryan	
2003/0009385	A1	1/2003	Tucciarone et al.	
2003/0030666	A1	2/2003	Najmi et al.	
2003/0032409	A1	2/2003	Hutcheson et al.	
2003/0064805	A1	4/2003	Wells	
2003/0119578	A1	6/2003	Newson	
2003/0144017	A1	7/2003	Inselberg	
2004/0023721	A1	2/2004	Giobbi	
2004/0192438	A1	9/2004	Wells et al.	
2004/0224757	A1	11/2004	Yamamura et al.	
2005/0046608	A1	3/2005	Schantz et al.	
2005/0048990	A1	3/2005	Lauriol	
2005/0085257	A1	4/2005	Laird	
2005/0114212	A1	5/2005	Carrez et al.	
2005/0136949	A1	6/2005	Barnes, Jr.	
2005/0154646	A1	7/2005	Chermesino	
2005/0159883	A1	7/2005	Humphries et al.	
2005/0181804	A1	8/2005	Misikangas et al.	
2005/0246334	A1	11/2005	Tao et al.	
2005/0261063	A1	11/2005	Boyd et al.	
2006/0003830	A1	1/2006	Walker et al.	

(56) **References Cited**

U.S. PATENT DOCUMENTS

2006/0004627 A1 1/2006 Baluja
2006/0058102 A1 3/2006 Nguyen et al.
2006/0063575 A1 3/2006 Gatto et al.
2006/0125693 A1 6/2006 Recker
2006/0181411 A1 8/2006 Fast et al.
2006/0189382 A1 8/2006 Muir et al.
2006/0194633 A1 8/2006 Paulsen
2006/0238382 A1 10/2006 Kimchi et al.
2006/0240891 A1 10/2006 Klinkhammer et al.
2006/0287810 A1 12/2006 Sadri et al.
2007/0024580 A1 2/2007 Sands et al.
2007/0025265 A1 2/2007 Porras et al.
2007/0060306 A1 3/2007 Amaitis et al.
2007/0061229 A1 3/2007 Ramer et al.
2007/0087834 A1 4/2007 Moser et al.
2007/0100963 A1 5/2007 Ban et al.
2007/0136132 A1 6/2007 Weiser et al.
2007/0149215 A1 6/2007 Misikangas
2007/0149216 A1 6/2007 Misikangas
2007/0167210 A1 7/2007 Kelly et al.
2007/0168127 A1 7/2007 Zaruba et al.
2007/0184852 A1 8/2007 Johnson et al.
2007/0218975 A1 9/2007 Iddings et al.
2007/0243925 A1 10/2007 LeMay et al.
2007/0244633 A1 10/2007 Phillips et al.
2007/0257831 A1 11/2007 Mathews et al.
2007/0270212 A1 11/2007 Cockerille et al.
2007/0281692 A1 12/2007 Bucher et al.
2008/0026844 A1 1/2008 Wells
2008/0032705 A1 2/2008 Patel et al.
2008/0039192 A1 2/2008 Laut
2008/0057894 A1 3/2008 Aleksic et al.
2008/0076572 A1 3/2008 Nguyen et al.
2008/0085692 A1 4/2008 Hart et al.
2008/0096659 A1 4/2008 Kreloff et al.
2008/0097858 A1 4/2008 Vucina et al.
2008/0102947 A1 5/2008 Hays et al.
2008/0108430 A1 5/2008 Evans
2008/0113785 A1 5/2008 Alderucci et al.
2008/0153515 A1 6/2008 Mock et al.
2008/0162037 A1 7/2008 Mahmoud
2008/0166973 A1 7/2008 Hart et al.
2008/0167106 A1 7/2008 Lutnick et al.
2008/0186234 A1 8/2008 Alles et al.
2008/0189360 A1 8/2008 Kiley et al.
2008/0207296 A1 8/2008 Lutnick et al.
2008/0227473 A1 9/2008 Haney
2008/0249833 A1 10/2008 Ali et al.
2008/0252527 A1 10/2008 Garcia
2008/0281668 A1 11/2008 Nurminen
2009/0197684 A1 8/2009 Arezina et al.
2009/0213771 A1 8/2009 Celentano et al.
2009/0325708 A9 12/2009 Kerr
2010/0022308 A1 1/2010 Hartmann et al.
2010/0027521 A1 2/2010 Huber et al.
2010/0039929 A1 2/2010 Cho et al.
2010/0048242 A1 2/2010 Rhoads et al.
2010/0063854 A1 3/2010 Purvis et al.
2010/0121567 A1 5/2010 Mendelson
2010/0167771 A1 7/2010 Raghothaman et al.
2010/0287033 A1 11/2010 Mathur
2010/0302056 A1 12/2010 Dutton et al.
2010/0305855 A1 12/2010 Dutton et al.
2010/0331016 A1 12/2010 Dutton et al.
2011/0078167 A1 3/2011 Sundaresan et al.
2011/0103360 A1 5/2011 Ku et al.
2011/0159953 A1 6/2011 Kerr
2011/0165936 A1 7/2011 Kerr
2012/0115512 A1 5/2012 Grainger et al.
2012/0122476 A1 5/2012 Lee et al.
2013/0003572 A1 1/2013 Kim et al.

OTHER PUBLICATIONS

Wireless Network. "Wikipedia. http://en.wikipedia.org/wiki/Wireless_network." Nov. 17, 2008.
"Tracking Cookie." Wikipedia. http://en.wikipedia.org/wiki/Tracking_cookie. May 24, 2009.
"Ekahau Positioning Engine 4.2." 2008. http://www.nowire.se/images/produktblad/ekahau/datasheet.sub.--epe.sub.-42.sub.--en.sub.--11022008.sub.--lo.pdf. Sep. 29, 2008.
"Internet Industry Interacting Gambling Code: A Code for Industry Co-Regulation in the Area of Internet Gambling Content Pursuant to the Requirements of the Interactive Gaming Act of 2001". Internet Industry Association. Dec. 2001.
"Location in SIP/IP Core Architecture." Open Mobile Alliance. Sep. 4, 2008. Accessed Dec. 2008. http://www.openmobilealliance.org/technical/release.sub.--program/locsip.- sub.--archive.aspx.
"The New Normal of Retailing: The Rise of the Mobile Shopper." Next Generation Retail Summit. 2010. http://www.ngrsummit.com/media/whitepapers/Microsoft.sub.--NGRUS.pdf.
"Wi-Fi Location-Based Services—Design and Deployment Considerations." 2006 Cisco Systems. Accessed Dec. 2008. https://learningnetwork.cisco.com/docs/DOC-3418.
"Wireless Network." Wikipedia. http://en.wikipedia.org/wiki/Wireless.sub.--network. Nov. 17, 2008.
Balakrishnan et al. "Lessons from Developing and Deploying the Cricket Indoor Location System." Nov. 7, 2003. http://www.sds.lcs.mit.edu/projects/cricket/V1Exp.pdf.
Blom et al. "Transmission Power Measurements for Wireless Sensor Nodes and their Relationship to Battery Level." Symposium on Wireless Communication Systems. pp. 342-345, Sep. 7, 2005.
Borriello et al. "Delivering Real-World Ubiquitous Location Systems." Communications of the ACM. pp. 36-41, vol. 48, Issue 3, Mar. 2005.
Capkun et al. "Mobility Helps Peer-to-Peer Security." IEEE Transactions on Mobile Computing. vol. 5, Issue 1, pp. 43-51, Jan. 2006.
Chawathe et al. "A Case Study in Building Layered DHT Applications." Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications. vol. 35, Issue 4, Oct. 2005.
Chen et al. "Practical Metropolitan-Scale Positioning for GSM Phone." UbiComp 2006: Ubiquitous Computing Lecture Notes in Computer Science, 2006, vol. 4206/2006, pp. 225-242.
Cheng et al. "Accuracy Characterization for Metropolitan-scale Wi-Fi Localization." Proceedings of the 3rd international conference on Mobile systems, applications, and services. 2005.
Heidari, Mohannad. "A Testbed for Real-Time Performance Evaluation of RSS-Based Indoor Geolocation Systems in a Laboratory Environment". Apr. 21, 2005. Accessed Dec. 2008. https://www.wpi.edu/Pubs/ETD/Available/etd-050407-112549/unrestricted/mas- sad.pdf.
Hightower et al. "Practical Lessons from the Place Lab." IEEE Pervasive Computing. pp. 32-39, vol. 5, Issue 3, Jul.-Sep. 2006.
Hile et al. "Indoor Location Estimation with Placelab." http://www.cs.washington.edu/education/courses/cse590gb/04wi/projects/hile-liu/. Jan. 8, 2004. Accessed on Sep. 25, 2008.
HTTP Cookie, redirected from tracking cookie as downloaded from wikipedia, 41 pages.
Interactive Gambling Industry Code, Dec. 2001, 7 pages.
Kang "Extracting Places from Traces of Locations." ACM SIGMOBILE Mobile Computing and Communications Review. vol. 9, Issue 3, Jul. 2005.
Kitasuka et al. "Positioning Technique of Wireless LAN Terminal Using RSSI between Terminals". Jun. 2005. Accessed Dec. 2008. http://www.techrepublic.com/whitepapers/positioning-technique-of-wireless- -lan-terminals-using-rssi-between-terminals/330959.
Ladd et al. "On the Feasibility of Using Wireless Ethernet for Indoor Localization." IEEE Transactions on Robotics and Automation, pp. 555-559, vol. 20, Issue 3, No. 3, Jun. 2004.

(56) **References Cited**

OTHER PUBLICATIONS

Ladd et al. "Using Wireless Ethernet for Localization." IEEE/RJS International Conference on Intelligent Robots and Systems. 2002.
Lafargue, Edouard. "Wireless Network Audits using Open Source Tools". SANS Institute 2003. Accessed Dec. 2008. http://www.sans.org/reading.sub.--room/whitepapers/auditing/wireless-netw- ork-audits-open-source-tools.sub.--1235.
Lamarca et al. "Finding Yourself: Experimental location technology relies on Wi-Fi and cellphone signals instead of orbiting satellites." Dec. 2004. http://spectrum.ieee.org/computing/networks/finding-yourself.
Lamarca et al. "Place Lab: Positioning Using Radio Beacons in the Wild." Pervasive 2005, LNCS 3468, pp. 116-133, 2005.
Lamarca et al. "Self-Mapping in 802.11 Location Systems." UbiComp 2005: Ubiquitous Computing Lecture Notes in Computer Science, 2005, vol. 3660/2005, 903, DOI: 10.1007/11551201.sub.--6.
Letchner et al. "Large-Scale Localization from Wireless Signal Strength." In Proceedings of the National Conference on Artificial Intelligence (AAAI), 2005.
Li et al. "A New Method for Yielding a Database of Location Fingerprints in WLAN" IEE Communications Proceedings, pp. 580-586, vol. 152, Issue 5, Oct. 7, 2005.
Milojicic et al. "Peer-to-Peer Computing" Jul. 10, 2002. https://www.hpl.hp.com/techreports/2002/HPL-2002-57R1.pdf.
Muthukrishnan, et al. "Sensing motion using spectral and spatial analysis of WLAN RSSI." Proceedings of the 2nd European conference on Smart sensing and context. 2007. pp. 62-76.
Otsason et al. "Accurate GSM Indoor Localization." Ubiquitous Computing 2005, LNCS 3660, pp. 141-158, 2005.
Sakata et al. "An efficient algorithm for Kriging approximation and optimization with large-scale sampling data". Computer Methods in Applied Mechanics and Engineering. vol. 193, Issues 3-5, pp. 385-404, Jan. 23, 2004.
Schilit et al. "Challenge: Ubiquitous Location-Aware Computing and the "Place Lab" Initiative." WMASH Proceedings of the 1st ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots. 2003.
Varshaysky et al. "Are GSM Phones the Solution for Localization?" 7th IEEE Workshop on Mobile Computing Systems and Applications, 2006. pp. 34-42, Aug. 1, 2005.
Vegni et al. "Local Positioning Services on IEEE 802.11 Networks." Radio Engineering, pp. 42-47, vol. 17, No. 2, Jun. 2008.
Want et al. "The Active Badge Location System." ACM Transactions on Office Information Systems (TOIS) vol. 10. No. 1, pp. 91-102, Jan. 1992.
Welbourne et al. "Mobile Context Inference Using Low-Cost Sensors." Location and Context-Awareness Lecture Notes in Computer Science, 2005, vol. 3479/2005, pp. 95-127.
Wirelss Network. Wikipedia. http://en.wikipedia.org/wiki/Wireless.sub.--network. Nov. 17, 2008.
Youssef et al. "Location-Clustering Techniques for WLAN Location Determination Systems." 2006. http://wrc.ejust.edu.eg/papers/ijca.pdf.

* cited by examiner

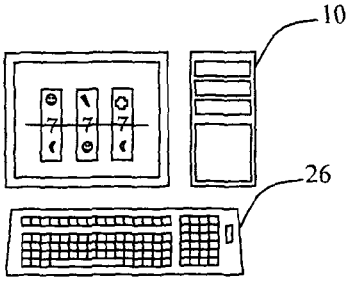


FIG. 1a

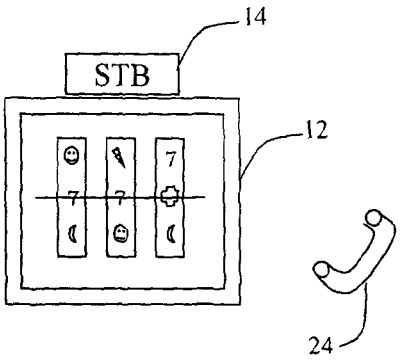


FIG. 1b

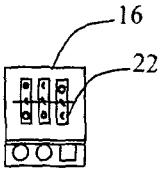


FIG. 1c

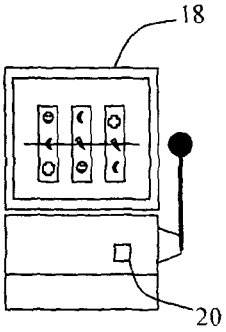
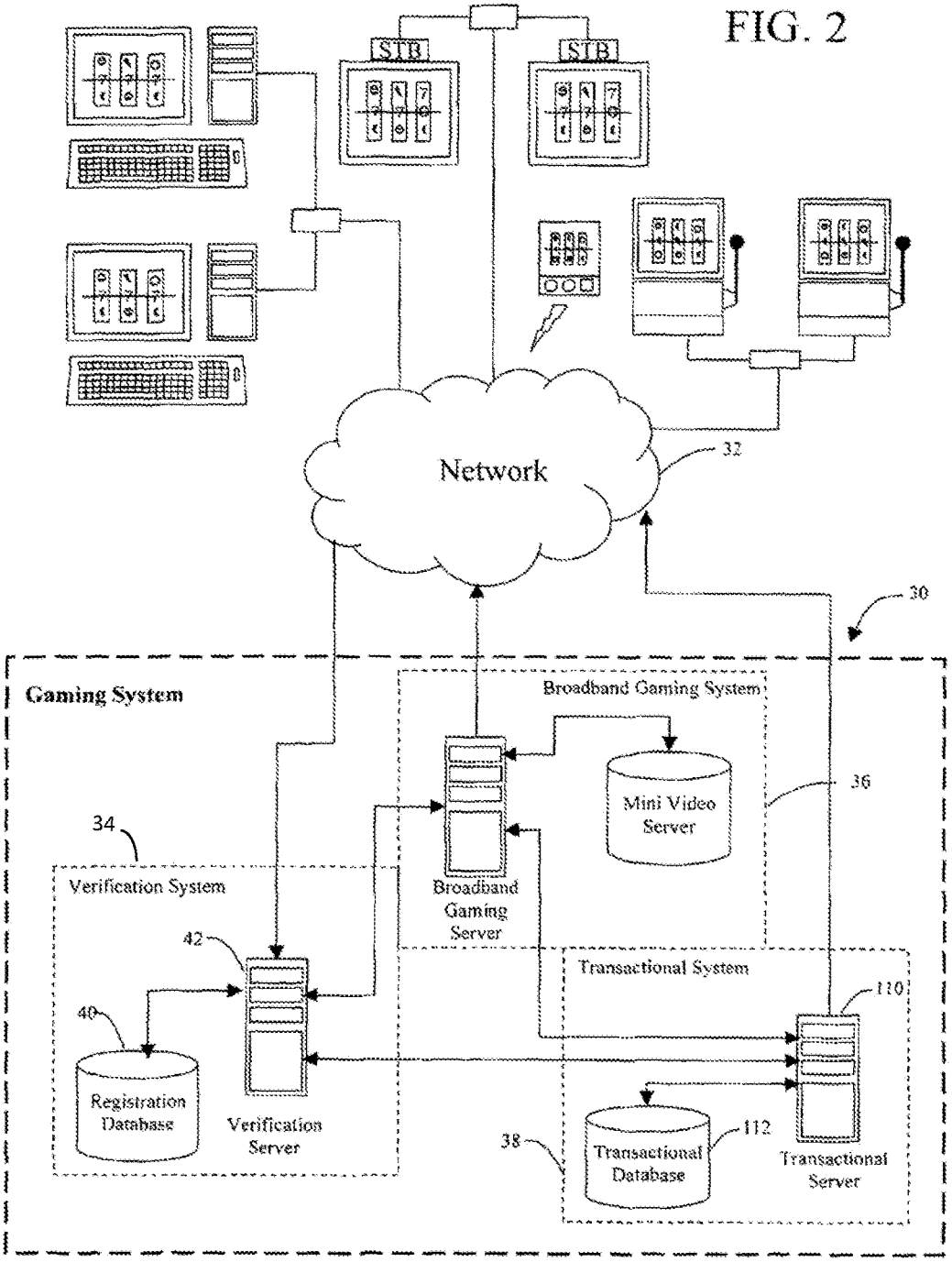


FIG. 1d

FIG. 2


STB
STB
Network
32
30
Gaming System
Broadband Gaming System
Mini Video Server
36
34
Verification System
Broadband Gaming Server
42
Transactional System
110
40
Registration Database
Verification Server
38
Transactional Database
112
Transactional Server

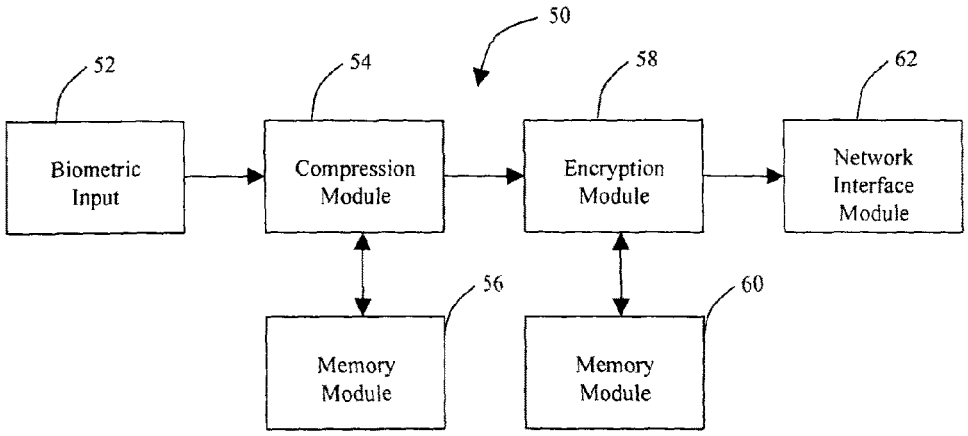

50
52
54
58
62
Biometric Input
Compression Module
Encryption Module
Network Interface Module
56
60
Memory Module
Memory Module

FIG. 3

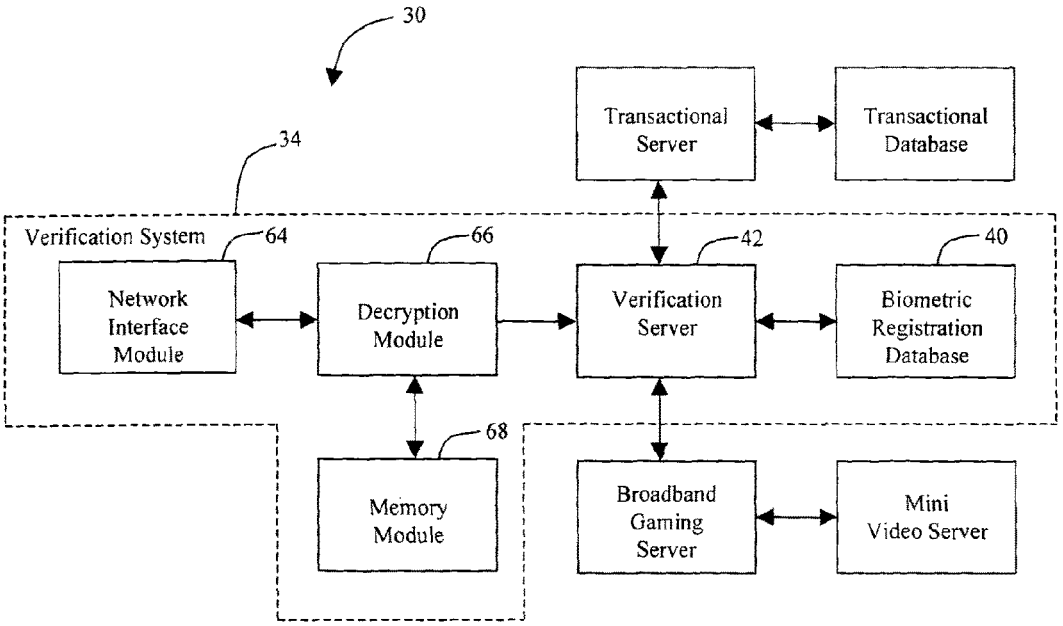

30
34
Transactional Server
Transactional Database
Verification System
64
66
42
40
Network Interface Module
Decryption Module
Verification Server
Biometric Registration Database
68
Memory Module
Broadband Gaming Server
Mini Video Server

FIG. 4

70

REGISTRATION DATA FIELDS	
NAME	BIOMETRIC
ADDRESS	PLAYER ID
USER NAME	MAC ID
PASSWORD	IP ADDRESS
CREDIT CARD	BROWSER
DATE	COOKIES
TIME	CRYPTO KEYS

72

USER SUBMITTED DATA	
NAME	BIOMETRIC
ADDRESS	PLAYER ID
USER NAME	MAC ID
PASSWORD	IP ADDRESS
CREDIT CARD	BROWSER
DATE	COOKIES
TIME	CRYPTO KEYS

FIG. 5

74

PLAYER DATA FIELDS	
PLAYER ID	SESSION TIME FOR TYPE OF GAME
DATE	AMOUNT PLAYED DURING SESSION
TIME IN	CREDIT CARD INFORMATION
TIME OUT	TRANSACTION REQUEST
TYPE GAME	TRANSACTION APPROVAL
CREDITS IN	TRANSFER OF CREDITS
CREDITS OUT	TRANSFER TO PLAYER CREDIT CRD
BONUS	CRYPTO KEYS

FIG. 6

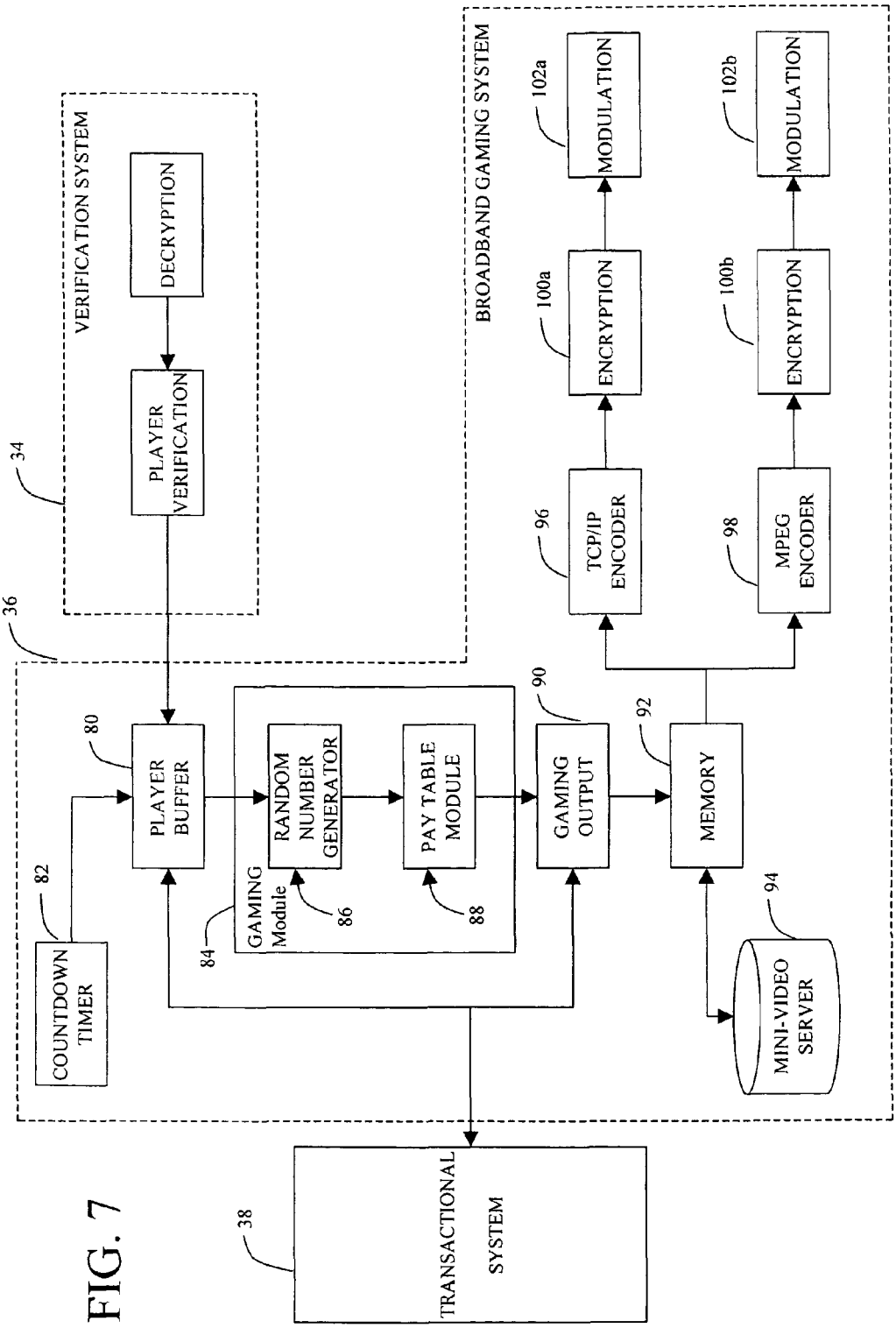

VERIFICATION SYSTEM
DECRYPTION
PLAYER VERIFICATION
34
36
BROADBAND GAMING SYSTEM
102a
MODULATION
102b
MODULATION
100a
ENCRYPTION
100b
ENCRYPTION
96
TCP/IP ENCODER
98
MPEG ENCODER
80
PLAYER BUFFER
RANDOM NUMBER GENERATOR
PAY TABLE MODULE
90
GAMING OUTPUT
92
MEMORY
GAMING Module
84
86
88
82
COUNTDOWN TIMER
94
MINI-VIDEO SERVER
38
TRANSACTIONAL SYSTEM

FIG. 7

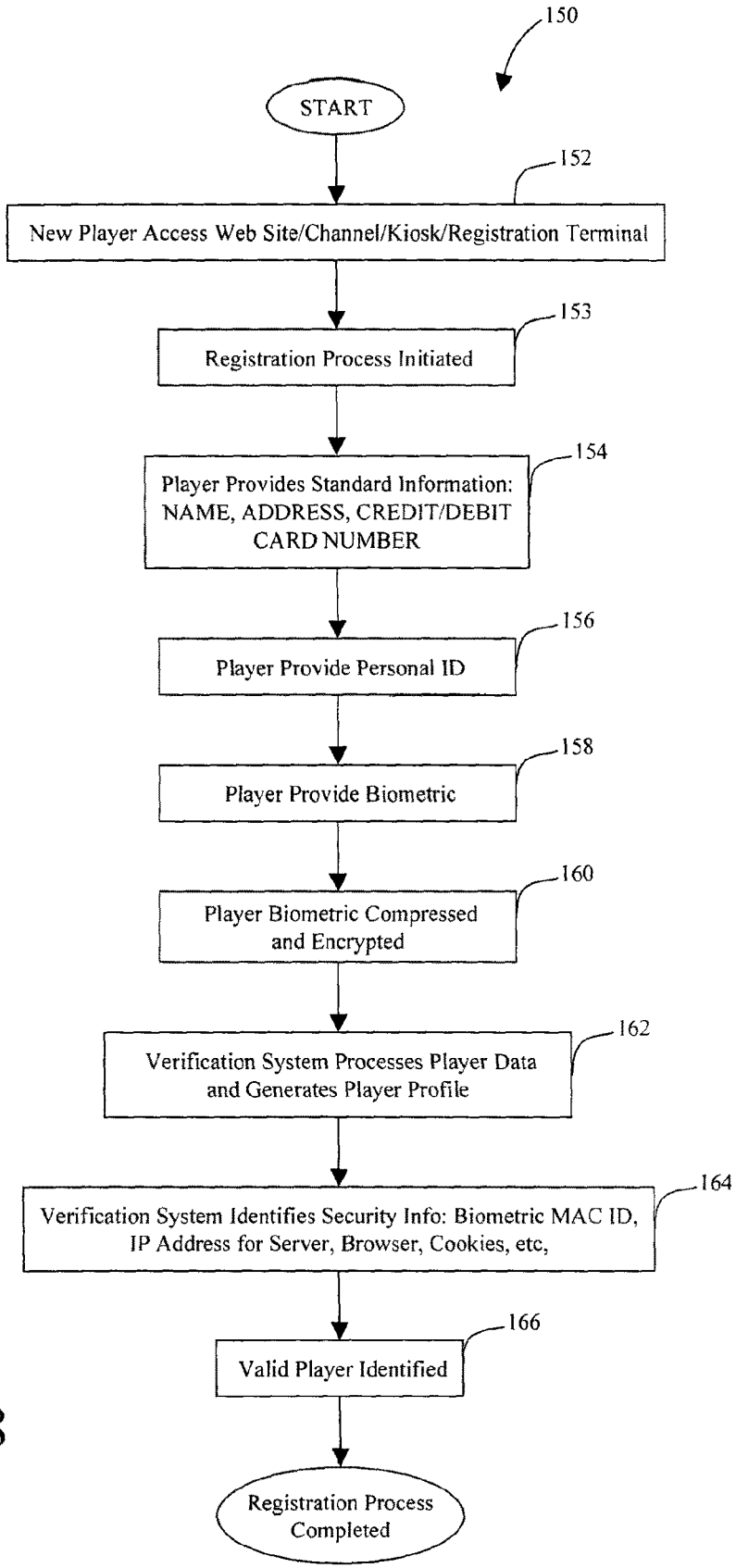

150
START
152
New Player Access Web Site/Channel/Kiosk/Registration Terminal
153
Registration Process Initiated
154
Player Provides Standard Information: NAME, ADDRESS, CREDIT/DEBIT CARD NUMBER
156
Player Provide Personal ID
158
Player Provide Biometric
160
Player Biometric Compressed and Encrypted
162
Verification System Processes Player Data and Generates Player Profile
164
Verification System Identifies Security Info: Biometric MAC ID, IP Address for Server, Browser, Cookies, etc,
166
Valid Player Identified
Registration Process Completed

FIG. 8

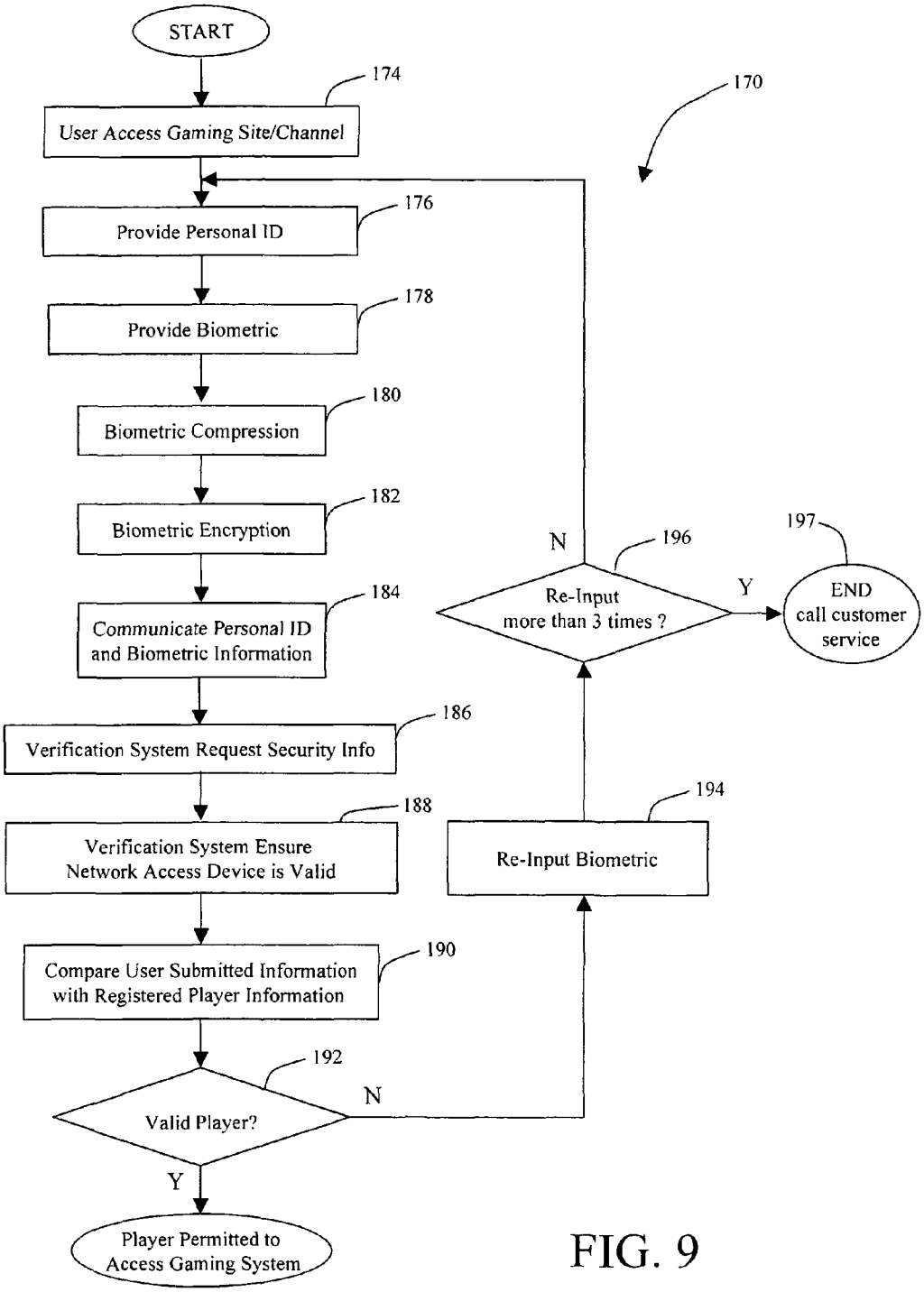

START
174
User Access Gaming Site/Channel
170
176
Provide Personal ID
178
Provide Biometric
180
Biometric Compression
182
Biometric Encryption
184
Communicate Personal ID and Biometric Information
186
Verification System Request Security Info
188
Verification System Ensure Network Access Device is Valid
190
Compare User Submitted Information with Registered Player Information
192
Valid Player?
N
Y
Player Permitted to Access Gaming System
196
Re-Input more than 3 times ?
N
Y
197
END call customer service
194
Re-Input Biometric

FIG. 9

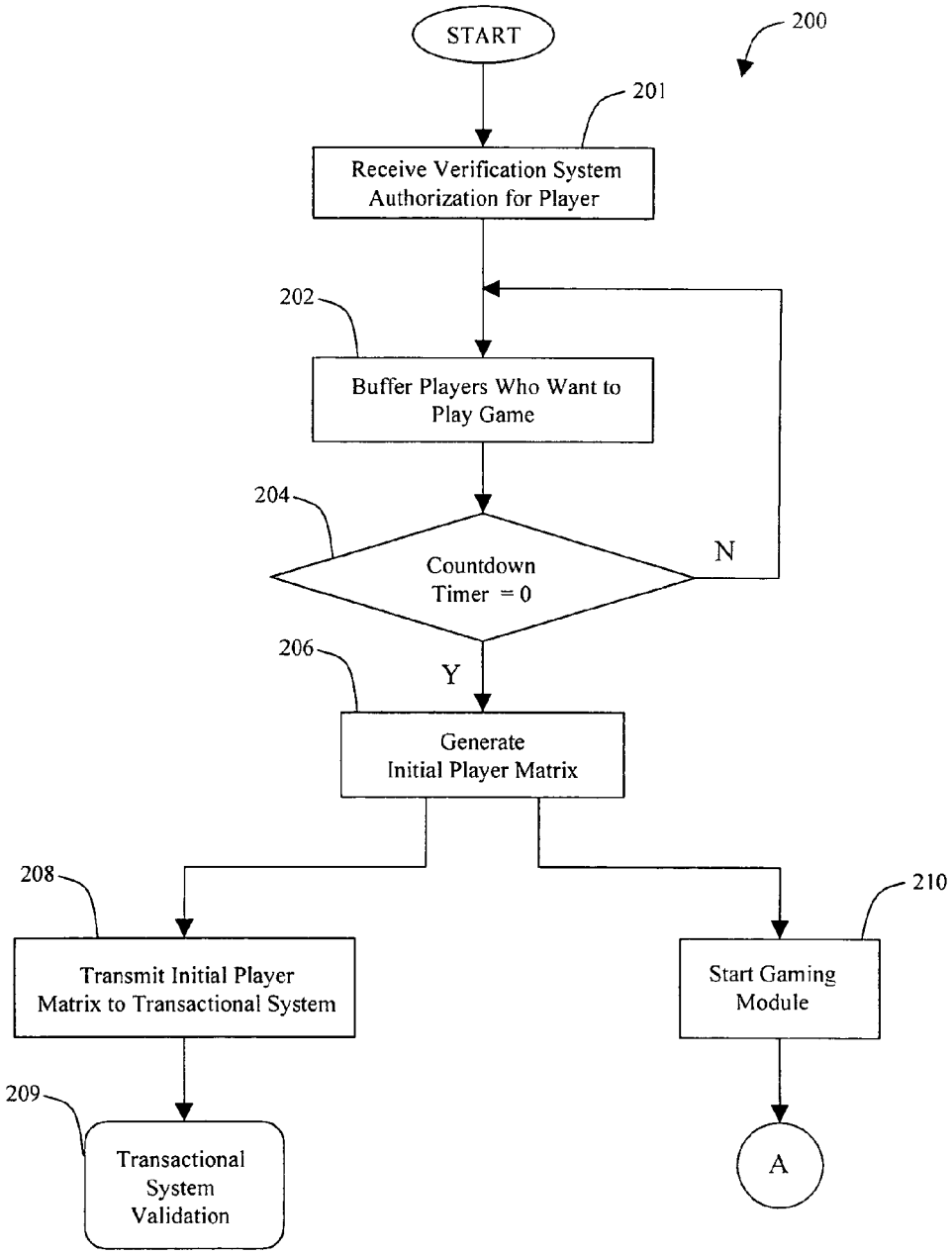

START
200
201
Receive Verification System Authorization for Player
202
Buffer Players Who Want to Play Game
204
Countdown Timer = 0
N
Y
206
Generate Initial Player Matrix
208
Transmit Initial Player Matrix to Transactional System
210
Start Gaming Module
209
Transactional System Validation
A

FIG. 10

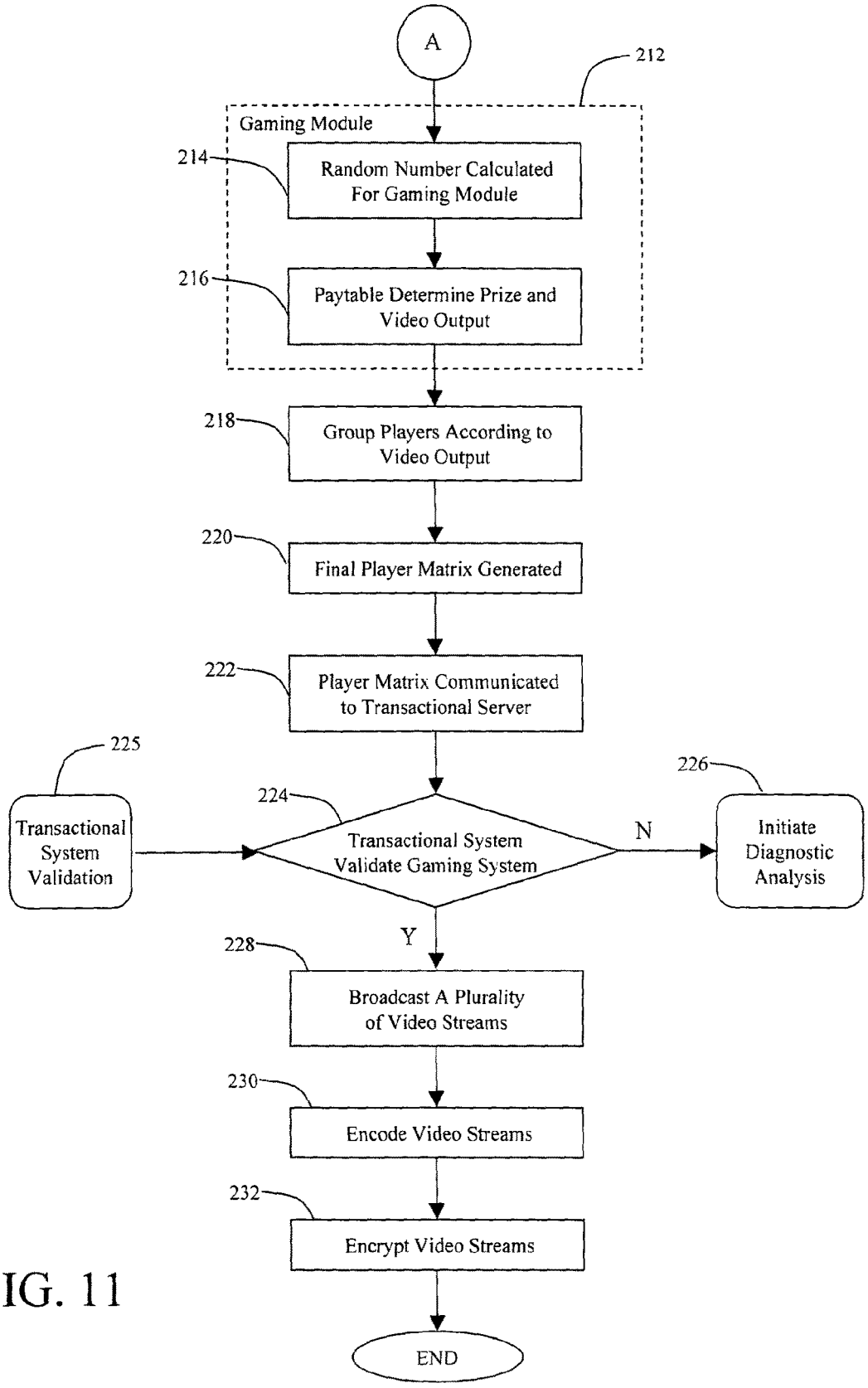

A
212
Gaming Module
214
Random Number Calculated For Gaming Module
216
Paytable Determine Prize and Video Output
218
Group Players According to Video Output
220
Final Player Matrix Generated
222
Player Matrix Communicated to Transactional Server
225
Transactional System Validation
224
Transactional System Validate Gaming System
N
226
Initiate Diagnostic Analysis
Y
228
Broadcast A Plurality of Video Streams
230
Encode Video Streams
232
Encrypt Video Streams
END

FIG. 11

NETWORKED GAMING SYSTEM AND METHOD

CROSS REFERENCE

This patent application is a Continuation of patent application Ser. No. 12/981,403 filed on Dec. 29, 2010 that is entitled GAMING SYSTEM NETWORK AND METHOD FOR DELIVERING GAMING MEDIA, which is a Continuation of patent application Ser. No. 10/681,034 (now U.S. Pat. No. 8,403,755) filed on Oct. 8, 2003 that is entitled WIRELESS BROADBAND GAMING SYSTEM AND METHOD, which is a Continuation of patent application Ser. No. 09/899,559 filed (now abandoned) on Jul. 5, 2001 that is entitled BIOMETRIC BROADBAND GAMING SYSTEM AND METHOD, which claims the benefit of provisional patent application Ser. No. 06/266,956 filed on Feb. 6, 2001. All of the above are herein incorporated by reference.

FIELD

The present invention relates to a networked gaming system and method. More particularly, the present invention relates to a networked gaming system and method that includes a networked gaming module that generates at least one random game output by random generation at the networked gaming module.

BACKGROUND

The related art includes gaming devices, online gaming, networked interactive gaming, and biometrics.

Gaming Devices

For purposes of this patent, the term "gaming" shall refer to either gambling and/or gaming applications. Gaming devices include games of skill and games of chance. Games of chance include many casino-type gaming devices in which the outcome of the game depends, at least in part, on a randomly generated event. For example, a game of chance may use a random number generator to generate a random or pseudo-random number. The random number may then be compared to a predefined table to determine the outcome of the event. If the random number falls within a certain range of numbers on the table, the player may win a predefined prize. The table may also contain display information that allows the gaming device to generate a display that corresponds to the outcome of the game. The gaming device may present the outcome of the game on a large variety of display devices, such as mechanical spinning reels or video screens.

Games of skill comprise a skill component in which a player combines letters or words (word puzzles), answers questions (trivia), overcomes challenges (video games), competes with other players (networked video games), and the like. Generally, a game of skill is a game requiring a level of skill which does not rely solely on chance. Some games of skill require a high degree of expertise and knowledge and other games of skill require very limited expertise or knowledge.

Online Gaming

In June 2001, Nevada signed a bill that could result in Nevada being the first state to offer legalized gambling over the Internet. The new law authorizes state gaming regulators to set up an infrastructure to license and oversee online gaming in Nevada when such gaming becomes legal. Online gaming is a federal issue whose legality is unclear at present.

A variety of technological limitations have been asserted as preventing Congress's endorsement of online gaming. These technological limitations are related to the prevention of underage gambling, controlling of gambling addiction, and ensuring the security and reliability of online gaming.

To prevent underage gambling, prior art systems and methods use passwords, user IDs, credit cards, and "click-through" agreements that ask the player to agree to being of legal gambling age by clicking on a button. Presently, there are no systems and methods to control online gambling addiction. With respect to ensuring that online gaming is secure and reliable, prior art systems and methods use various cryptographic techniques such as RSA encryption, digital certificates, or other similar well known cryptographic methods. These cryptographic methods are helpful in ensuring secure communications; however, these cryptographic methods do not ensure that the individual accessing the online game is a valid user.

In view of the prior art systems, a minor or other unauthorized individual simply needs a user ID and a corresponding password to access a gaming site. The obtaining of a user ID and password is a relatively simple task as this information is generally not modified. Commonly the user ID information is acquired by identifying the web site's naming convention for the player. The player password can be easily determined by remembering the pattern of keys typed by the player during the log-on procedures or by simply requesting the password from the player as part of a diagnostic procedure. The latter is a trick commonly used by hackers to access a system. The password problem may be overcome by modifying the password on a regular basis, however the player must then remember the modified password. Should the player forget the password a new password is emailed. During the emailing process it is common for email to be easily intercepted in cyberspace. Additionally, it is common for unauthorized users to simulate being at a certain location by submitting an IP address that identifies an authorized user.

Therefore, a better system and method for identifying a valid user is needed. Additionally, it would be beneficial to provide a gaming system and method that would prevent underage gambling, be simple to implement, prevent gambling addiction, and provide a higher degree of security and reliability from unauthorized users.

Networked Interactive Gaming

Networked interactive gaming in an open networked environment such as the Internet is well known. However, interactive gaming in an open network such as the Internet is confined to communicating with other devices using the same TCP/IP protocols. Currently, networked interactive gaming systems using the TCP/IP protocol are not configured to communicate with interactive set-top boxes using MPEG protocols.

Networked interactive gaming in an open networked environment using traditional security methods such as secure socket layers and digital certificates is well known. However, networked interactive gaming in an open networked environment using traditional security methods does not prevent gambling from a minor having acquired a parent's user ID and password without the parent's consent.

Networked interactive gaming using LANs and WANs for progressive slot machines having large jackpots is also well known. However, networked interactive systems using LANs and WANs for progressive slot machines generally exist in a highly secure proprietary network environment. Thus, the creation of a progressive slot machine with a large jackpot in an open network environment is not well known.

Biometrics

A biometric is a measurable psychological and/or behavioral trait that can be captured and subsequently compared with another instance at the time of verification. This definition includes the matching of fingerprints, voice patterns, hand geometry, iris and retina scans, vein patterns, and other such methodologies. For purposes of the disclosure described heretofore, the definition of biometrics also includes signature verification, keystroke patterns, and other methodologies weighted towards individual behavior.

Biometric applications for games of skill and games of chance are limited. For example biometric gaming applications are taught in U.S. Pat. No. 6,010,404 granted to Walker et al. teaches a method and apparatus for using player input codes (e.g., numeric, biometric or physical) to affect the outcomes of electronic gambling devices, such as slot machines. Additionally, U.S. Pat. No. 6,142,876 granted to Cumbers teaches a system and method for passively tracking the play of players playing gaming devices such as slot machines. Players provide identification information and facial recognition data is acquired by a digital or video camera. For each player an account file and a file of the facial image data is stored. When the player plays the slot machine, a camera scans the player and acquires facial image data which is compared to stored data to identify the player. Furthermore, U.S. Pat. No. 5,902,983 granted to Crevelt et al. teaches a gaming machine configured to perform EFT transactions which are limited to preset amounts. The patent teaches the use of a fingerprint imaging device and retinal scans for verifying a player's identity.

Although biometric applications for gaming applications are known, biometric applications for online gaming systems are not known. Furthermore, the managing of biometric information and gaming information in an open network environment is not known. Additionally, the use of biometrics in a gaming system and method to prevent underage gambling and prevent gambling addiction is not known.

SUMMARY

A networked gaming system and method is described. The networked gaming system and method includes a user identification, a transactional component, a networked gaming module, and at least one network access device. The user identification is received by the network access device. The received user identification is compared with registration data in a registration database. A player is provided access to a game when the received user identification matches the registered player data. The transactional component charges the registered player at least one credit for a game outcome. The networked gaming module performs the game operations and generates at least one random game output by random generation at the networked gaming module. The networked gaming module then associates the at least one random game output with an image ID. The networked gaming module then communicates the one or more images corresponding to the image ID to the network access device.

In one illustrative embodiment, the registration database includes a registered player biometric. Additionally, an input player biometric is received by the network access device and the player is provided access to the game when the input player biometric matches the registered player biometric.

In another illustrative embodiment, the networked gaming system and method includes a countdown timer that provides a window of time for other players to join the game.

In yet another illustrative embodiment, the networked gaming system and method includes an encryption module that encrypts the plurality of images communicated to each network access device.

In a further illustrative embodiment, the images communicated to the network access device by the networked gaming system are viewable on a browser.

In a still further illustrative embodiment, the one or more images communicated to the network access device game include a slot machine game outcome, and the networked gaming module generates the random game output with a lottery game.

DRAWINGS

Illustrative embodiments are shown in the accompanying drawings wherein:

FIG. **1***a* through FIG. **1***d* show diagrams of a plurality of illustrative network access devices.

FIG. **2** shows a high level diagram of a gaming system networked to a plurality of network access devices.

FIG. **3** shows a block diagram of an illustrative biometric input module.

FIG. **4** shows a block diagram of a gaming system configured to receive a biometric input from a network access device.

FIG. **5** shows a table of the data fields in a verification system.

FIG. **6** shows a table of the data fields in a broadband gaming system and in a transactional system.

FIG. **7** shows a block diagram of a broadband gaming system.

FIG. **8** shows a flowchart of the registration method for the gaming system.

FIG. **9** shows a flowchart of the verification method for the gaming system.

FIG. **10** shows a flowchart of the information processed by the gaming system.

FIG. **11** is a continuation of the flowchart of the information processed by the gaming system in FIG. **10**.

DESCRIPTION

A networked gaming system that comprises a verification system, a broadband gaming system, and a transactional system is described. The verification system operations include ensuring that a user is a registered player by using a biometric input. The broadband gaming system operations include managing and performing at least one game. The transactional system operations include providing oversight for each transaction conducted by the verification system and the broadband gaming system.

A verification system for playing the networked gaming system is described. The networked games include games of chance and games of skill. The verification system communicates with a biometric input module and a network access device to generate a user identification information. The user identification information is compared to information in a registration database. If an acceptable match is made between the user identification information and the information in the registration database, the user is designated as a player. The player then has access to both the broadband gaming system and the transactional system.

A broadband gaming system which is in communication with the verification system is described. The broadband gaming system includes a buffer which stores information about players who desire to play a game. The buffer is

operatively coupled to a random number generator that generates a random number for each player in the buffer. A paytable module in communication with the random number generator determines the outcome associated with the random number generator. The paytable also determines which images are associated with the outcome for each player. Preferably, the images are stored on a mini video server and then cached in a memory module. The images are intelligently buffered for downstream communications. In its preferred embodiment, a plurality of encoders are operatively coupled to the memory module caching the broadcast video streams. The plurality of encoders encode the broadcast downstream images according the requirements for each network access device. Each encoder is operatively coupled to an encryption module that encrypts the broadcast. A modulation module is operatively coupled to the encryption module and modulates encrypted images for downstream transmission. Each network access device includes a tuner, a demodulation module, and a decryption module that permits an image to be viewed by the network access device.

A transactional system and method that ensures secure communications occur in the verification system and the broadband gaming system is described. The transactional system also performs accounting, bonusing, tracking, and other such functions. Preferably, the transactional system is capable of receiving a plurality of funds from a financial account and converting them to credits that are used in the broadband gaming system.

The above description sets forth, rather broadly, the more important features of the present disclosure so that the detailed description of the preferred embodiment that follows may be better understood and contributions of the present disclosure to the art may be better appreciated. There are, of course, additional features of the disclosure that will be described below and will form the subject matter of claims. In this respect, before explaining at least one preferred embodiment of the disclosure in detail, it is to be understood that the disclosure is not limited in its application to the details of the construction and to the arrangement of the components set forth in the following description or as illustrated in the drawings. The disclosure is capable of other embodiments and of being practiced and carried out in various ways. Also, it is to be understood that the phraseology and terminology employed herein are for the purpose of description and should not be regarded as limiting.

In the following detailed description of the preferred embodiments, reference is made to the accompanying drawings, which form a part of this application. The drawings show, by way of illustration, specific embodiments in which the disclosure may be practiced. It is to be understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present disclosure.

Network Access Devices

Referring to FIG. **1***a* through FIG. **1***d*, there is shown a plurality of illustrative network access devices. Each of the network access devices is configured to be capable of running a gaming application. For illustrative purposes the gaming application shown simulates the spinning reels of a slot machine.

The network access device in FIG. **1***a* is a personal computer **10** having a network interface card (not shown) that may be operatively coupled to a modem (not shown). Another network access device shown in FIG. **1***b* includes a television **12** operatively coupled to an interactive set-top box **14** that is operatively coupled to a cable network (not shown). The other network access device shown in FIG. **1***c* is a wireless device **16** such as a digital phone or personal digital system (PDA) or other such wireless device which is configured to communicate with a network using wireless networking protocols. Yet another network access device is shown in FIG. **1***d* and includes a gaming terminal **18** such as a slot machine on a casino floor that is operatively coupled to a plurality of other gaming terminals. It shall be appreciated by those skilled in the art of networking that the distinguishing feature between each of these network access devices is the type of communications protocols used by each device to enable communications between similar network access devices.

Each of the network access devices either includes a biometric input module operatively coupled to the network access device or includes a biometric input module communicatively coupled to the network access device. A biometric is a measurable psychological and/or behavioral trait that can be captured and subsequently compared with another instance at the time of verification. This definition includes the matching of fingerprints, voice patterns, hand geometry, iris and retina scans, vein patterns, and other such methodologies. For purposes of the disclosure described heretofore, the definition of biometrics also includes signature verification, keystroke patterns, and other methodologies weighted towards individual behavior.

In one illustrative embodiment, the biometric input module is a fingerprint scanner **20** resident on the gaming terminal **18** wherein the biometric input is a fingerprint. In another illustrative embodiment, the biometric input module is the screen **22** of wireless device **16** wherein the screen is configured to receive a biometric input such as a user signature. In yet another illustrative embodiment, the biometric input module is a telephone **24** that is configured to receive a voice pattern from a user prior to engaging communications with the interactive set-top box **14**. In yet another illustrative embodiment the biometric input module is a keyboard **26** operatively coupled to computer **10** wherein the user is requested to input a keystroke pattern. An illustrative example of a biometric input module operatively coupled to the network access device is shown in FIG. **1***d* having the fingerprint scanner **20** on the gaming terminal **18**. An illustrative example of a biometric input module, e.g. the telephone **24**, communicatively coupled to the network access device, e.g. the interactive set-top box **14**, is shown in FIG. **1***b*.

The biometric input is used to prevent unauthorized gaming activity and efficiently store credits on the user's behalf. By way of example and not of limitation, unauthorized gaming activity includes preventing underage gaming and prohibiting players with histories of gambling addiction. Additionally, player credits may be stored on a network so that the player does not need to carry coins, paper currency, coupons, credit cards, or debits cards to play a game. It shall be appreciated by those skilled in the art having the benefit of this disclosure that different biometric input modules may be used in conjunction with different network access devices.

Gaming System

Referring to FIG. **2** there is shown a high level block diagram of a gaming system **30** in communication with a plurality of network access devices coupled to a network **32**. The gaming system includes a verification system **34**, a broadband gaming system **36**, and a transactional system **38**. The verification system **34** verifies that a user operating a network access device is a registered player. The broadband gaming system **36** performs the function of generating a game and broadcasting the game results to each of the

network access devices. The transactional system **38** performs a plurality of functions including tracking each transaction performed by both the verification system and the broadband gaming system and conducting electronic fund transfers.

Verification System

The verification system **34** verifies that a user desiring to play the game is a registered player. The verification system **34** communicates with the biometric input module and a network access device to generate user identification information. The user identification information includes information such as cryptographic keys that are necessary to securely identify the network access device. The user identification information also includes media access control (MAC) identification and confirmation of the user Internet Protocol (IP) address. The user identification information is compared to information in a registration database **40** by a verification server **42**. If an acceptable match is made between the user identification information and the information in the registration database, the user is designated as a player. The player then has access to either the broadband gaming system **36** or the transactional system **38**.

In an alternative embodiment the user identification information is housed in a smart card (not shown) that is in communication with the verification system **34**. The smart card includes a stored biometric which is used to identify the user as a player. Cryptographic keys are then exchanged between the verification system **34** and the smart card to provide the player access to either the broadband gaming system or the transactional system **38**.

Referring to FIG. **3** there is shown an illustrative biometric input module **50**. By way of example, the illustrative biometric input module **50** is a fingerprint scanner. It shall be appreciated by those skilled in the art having the benefit of this disclosure that the use of the fingerprint scanner as the illustrative biometric input module is not restrictive. A scanned fingerprint image is collected by the biometric input **52**. After the scanned fingerprint image is collected, the fingerprint image is compressed by the compression module **54**. A memory module **56** provides fast memory resources for the compression of the fingerprint image. After compression, the fingerprint image is encrypted by the encryption module **58** for downstream transmission. The encryption module **58** also includes a memory module **60** that provides fast memory resources for the encryption of the compressed fingerprint image. An encrypted compressed fingerprint image is then communicated to network **32** (see FIG. **2**) using the network interface module **62**.

Referring to FIG. **4** there is shown a block diagram of the verification system **34**. The verification system is operatively coupled to network **32** with network interface module **64**. The network interface module **64** is configured to receive user identification information generated by the network access devices and from the biometric input module. Preferably, the biometric and other user identification information received by the verification system is an encrypted biometric that is decrypted by decryption module **66**. A memory module **68** is preferably a fast memory that expedites the decryption process. After decryption the biometric and remaining user identification information is processed by the verification server. It shall be appreciated by those skilled in the art that the verification server **42** may house the network interface module **64**, decryption module **66** and the memory module **68**. The verification server **42** is also in operative communication with a registration database **40**. The verification server **42** performs the function of matching the user identification information collected from the network access device with the player information in the registration database **40**. Additionally, the verification server **42** performs the caching functions needed to ensure that once a player has been identified during an initial game, subsequent usage by the same player proceeds quickly.

Preferably, the verification server **42** identifies registered players using a biometric template of the registered player residing on the registration database **40**. The registered players are referenced with personal ID numbers. When a transaction is undertaken, the user firstly calls up the particular template from the registration database **40** by inputting a personal ID. The personal ID includes a particular number, user ID, password, or other such identification techniques. The inputting of the personal ID is accomplished with a familiar numeric keypad, keyboard, magstripe card, or smart card. The correct template is called and held in memory ready for comparison with the biometric sample provided by the user. A comparison takes place that results in a binary true or false condition as to the identity of the user. The user is in effect claiming an identity by inputting the personal ID and the system is subsequently verifying that the claim is genuine according to the matching criteria setup within the system.

Referring to FIG. **5** there is shown the registration data fields **70** and user submitted data fields **72**. The registration data fields **70** include data fields that comprise the user identification information. The registration data fields include user identification information such as player name, address, user name, password, credit card information, and the date and time of the registration. The player biometric and personal ID also comprises the user identification information and provides unique information about the player. The personal ID may be the same as the user name or password. It shall be appreciated by those skilled in the art that some biometric information may be compressed. Furthermore, the user identification information includes data about the network access device and the network connection such as MAC ID, IP addresses, browser type, any cookies resident on the network access device, etc. Finally, the user identification system includes cryptographic keys which are used to encrypt and decrypt the communications between the verification system and each of the network access devices.

The user submitted data fields **72** mirror the registration data fields **70**. The user submitted data fields receive data generated by a user that is attempting to access the broadband gaming system **36**. The user submitted information is carefully analyzed to ensure that a valid user is being identified. It is well known that the connection of one network access device to another network access device generates security concerns. Preferably, the present verification system operates using a fast hardware-type firewall that performs a stateful multilayer inspection. In its preferred embodiment the firewall provides packet filtering using a secure protocol such as IPSec. This protocol provides encryption of the data at the packet level as well as at the source address level. Without access to the encryption keys, a potential intruder would have difficulty penetrating the firewall. Additionally, it would be preferable to provide a circuit level gateway and an application level gateway. The circuit level gateway works on the session layer of the OSI model or the TCP layer of the TCP/IP model, and monitors TCP handshaking between packets to determine whether a requested session is legitimate. The application level gateway filters data packets at the application layer of the OSI

model. A stateful multilayer inspection firewall offers a high level of security, good performance, and transparency to end users.

Referring to FIG. **6** there is shown the player data fields **74** that are generated by the broadband gaming system and the transactional system after the user has been verified to be a registered player. The player data fields **74** are used to generate a player matrix which is used as an additional internal security measure. The player data fields **74** include a player ID that identifies the player, and a timestamp that provides the date, time in, and time out by the player during the game. Additionally, the type of game, credits played, and credits remaining are monitored. Based on the level of player activity a bonus is provided to the player. Further still the session time for each type of game and the amount played during the session is monitored to better define the type of games the player likes. Transactional information is also monitored and updated, preferably, by the transactional system **38**. The transactional information includes credit card information, transaction requests, transaction approval, conversion of monetary funds to credits for playing the game, any transfers of credits for playing the game, and conversions from credits to monetary funds that are credited to the player's financial account. Preferably, communications between the transactional system and the broadband gaming system are conducted in a secure environment using cryptographic keys. Although the use of cryptography within the private network may appear excessive, one of the greatest security threats within a private network comes from its own employees. Therefore, it is preferable to use internal firewalls for communications between the broadband gaming system, the transactional system and the verification system.

Broadband Gaming System

A more detailed drawing of the broadband gaming system is provided in FIG. **7**. The dashed boundary in FIG. **7** defines the broadband gaming system **36**. After player verification is completed at the verification system **36**, the broadband gaming system **36** is engaged. The broadband gaming system **34** includes a player buffer **80** configured to receive the players who will be playing the game. The player buffer **80** generates an initial player matrix with player data fields **74** (shown on FIG. **6**).

A countdown timer **82** is coupled to the player buffer **80**. Preferably, the countdown timer **82** is also displayed to the player. The countdown timer **82** provides a window of time within which players may join the game. The players that have joined the game before the end of the timing period are stored in the buffer. When the timing period reaches zero the initial player matrix is communicated to the transactional system **38** and to the gaming module **84**.

The gaming module **84** provides a game that is played by the plurality of players. The game may include a plurality of different games and the type of game is not restrictive to this disclosure. Preferably, the gaming module **84** includes at least one random number generator **86** and a paytable module **88**.

The random number generator **86** is operatively coupled to the player buffer. The random number generator **86** generates at least one random number that is stored in the player matrix. In one embodiment, at least one random number is generated for the plurality of players playing the game. In an alternative embodiment, at least one random number is generated for each player. In yet another embodiment, a plurality of random numbers are generated that are applied to the plurality of players playing the game. Preferably, the random number generator **86** is a fast hardware module.

A paytable module **88** is operatively coupled to the random number generator **86**. The paytable module **88** is a programmable module that determines the type of prize awarded to the player based on the random number generated by the random number generator **86**. In one embodiment, the paytable module **88** is a field programmable gate array. Preferably, the paytable module **88** also includes an image ID that is associated with the outcome determined by the paytable module **88**.

A gaming output module **90** revises the player matrix to include the outcome for each player. Additionally, the gaming output module **90** groups the players according to the image ID. Based on the results generated by the gaming module **84**, the gaming output module **90** generates a final player matrix that is communicated to the transactional server **38** and to a memory module **92**.

Preferably, the memory module **92** has stored a plurality of images in a fast memory by the time the final player matrix is communicated to the memory module **92**. In operation, the memory module **92** is enabled before the final matrix is communicated to the memory module **92**. By way of example, when the game is engaged the memory module **92** begins the process of finding the applicable images associated with the image IDs in the mini-video server **94** and transfers the images to the fast memory module **92**. Thus, when the gaming output is received by the memory, the images are stored in the fast memory module **92**. In one embodiment, the memory module **92** then broadcasts the images to encoders **96** and **98**. In an alternative embodiment, the memory module **92** is operatively coupled to an intelligent router (not shown) that routes the images to the appropriate encoders **96** and **98**.

The appropriate encoder then receives the images and converts them to a format which meets the requirements for the appropriate network access device. By way of example, an IP encoder **96** encodes a plurality of JPEG images for viewing on a conventional web browser, and an MPEG encoder **98** encodes the plurality of JPEG images into an MPEG stream that is viewed on a television via an interactive set-top box.

Encryption modules **100***a* and **100***b* are operatively coupled to encoders **96** and **98**, respectively, and receive the encoded images and encrypt the encoded images in manner well known to those skilled in the art. Modulation modules **102***a* and **102***b* are operatively coupled to encryption modules **100***a* and **100***b*, respectively, and modulate encrypted encoded images for downstream transmission in a manner well known to those skilled in the art.

Preferably, the broadband gaming system occupies one downstream band, i.e. one 6 or 8 MHz band, in the interactive set-top-box environment. In the web-based broadcast environment, the broadband gaming system occupies a downstream channel much like a standard streaming media website.

It shall be appreciated by those skilled in the art having the benefit of this disclosure that the broadband gaming system can play more than one game at a time. The system may be designed to operate in a multi-tasking mode where more than one game is played at a time. Additionally, the system may be designed to operate in a fast serial mode in which a game is played while the countdown timer is waiting for the next queue to be filled.

Transactional System

Referring back to FIG. **2**, there is shown the transactional system **38** which comprises a transactional server **110** and a transactional database **112**. The transactional system **38** performs a plurality of functions including tracking each transaction performed by both the verification system and the broadband gaming system. Additionally, the transactional system **38** is configured to authorize and conduct electronic fund transfers. Furthermore, the transactional system **38** performs such operations as player tracking, managing loyalty programs, engaging bonus games, determining bonus prizes and interfacing with accounting programs.

Method for Registering a Player

Referring to FIG. **8** there is shown a flowchart of the registration method for the gaming system **30**. The registration method **150** begins when a prospective player first accesses a website, channel, kiosk or other such registration terminals as described in block **152**. The method then proceeds to block **153**.

At block **153**, the registration process is initiated. By way of example and not of limitation, a registration terminal may provide a hyperlink to a registration window that prompts the prospective player for information. The method then proceeds to block **154**.

At block **154**, the prospective player provides registration identification information such as name, address, credit card number, and other information necessary to create a registration file for the prospective player. The method then proceeds to block **156**.

At block **156**, the prospective player is prompted for a personal ID. The personal ID may be a user ID, a password, a numeric combination, or any other such identification information. The personal ID is used during the verification process to identify a biometric template for the prospective player. The method then proceeds to block **158**.

At block **158**, the prospective player submits a biometric to the registration terminal. By way of example and not of limitation the biometric is a fingerprint. Any other biometric may also be used. The method then proceeds to block **160** or **162**.

At block **160**, the biometric input is compressed and encrypted. It is preferable for certain biometric inputs to be compressed such as fingerprint scans, retinal scans, and other such scanning techniques. Other biometric inputs such as voice patterns and signatures do not have to be compressed. The process of encrypting biometric inputs is necessary in an open network environment. The process of encrypting may not be necessary on a private proprietary network. Therefore, it shall be appreciated by those skilled in the art having the benefit of this disclosure that the compression and encryption processes in block **160** may not be necessary for every biometric input.

At block **162**, the prospective player information is stored in the verification system and a player profile is updated accordingly. Alternatively, the prospective player information is stored on a smart card. The method then proceeds to block **164**.

At block **164**, security information about the registration terminal is collected. The registration information identifies the registration terminal as being a secure terminal. The registration terminal provides information such as the MAC ID for the biometric input module, the IP address for the server communicating with the registration terminal, and the cryptographic keys associated with the registration terminal. The registration terminal includes the network access devices described in FIG. **1***a* through FIG. **1***d*, as well as kiosks and other such registration terminals.

At block **166**, the prospective player is identified as a registered player and the registration database **40** is updated accordingly. The registration process is broken out into separate components for security purposes. Once a validly registered player is identified by the verification system, the registration process is completed.

Method for Player Verification

Referring to FIG. **9** there is shown a method **170** for player verification used by the verification system **34**. The player verification process includes receiving user identification information from a network access device. The method is initiated at block **174** when a user accesses a website or channel displaying the game. The method then proceeds to block **176**.

At block **176**, the personal ID is provided by the user. The personal ID is used by the verification system to find a biometric template for determining whether the user is a registered player. The method then proceeds to block **178**.

At block **178**, the biometric input module of the network access device receives a biometric from the user. As previously described the biometric input module can be one of plurality of biometric inputs. Depending on the type of biometric, the biometric may be compressed as described by block **180** and encrypted as described by block **182**. At block **184**, the biometric and the personal ID is then communicated through a network **32** to the verification system **34**. Alternatively, the biometric and personal ID are communicated to a smart card for verification.

At block **186**, the verification system **34** requests security information from the network access devices. The security information identifies the network access devices as being a valid network access device. The method then proceeds to block **188**.

At block **188**, the verification system **34** processes the security information to ensure that the security information is generated by the appropriate network access device, and to ensure that the security information has not been compromised. Preferably, the verification system **34** performs a stateful multilayer inspection as described above. The method then proceeds to block **190**.

At block **190**, the user submitted player information is compared to the registered player information. If a determination is made at decision diamond **192** that the submitted player information is not a valid, registered player the method proceeds to block **194**. At block **194**, the user is requested to re-input the biometric. If the biometric is input more than three times, as provided by decision diamond **196**, the user is requested to contact customer service.

If a match is found at decision diamond **192** between the user submitted information and the registered player information, the user is identified as a valid player then the player proceeds to the broadband gaming system **36**.

Method for Operation of Broadband Gaming System

Referring to FIG. **10** and FIG. **11**, there is shown a flowchart **200** of the information processed by the broadband gaming system **36**. The process is engaged by performing the verification process in which the verification system identifies a player as in block **201**. After the verification process has been completed the method proceeds to block **202**.

At block **202**, the players who desire to play a particular game are stored in a buffer until the particular game is engaged. The method then proceeds to decision diamond **204**.

At decision diamond **204**, the countdown timer **82** determines if the period during which the game is open has been closed. If the game remains open, additional players may be received by the broadband gaming system. If the game is closed because the period during which the game is open has expired, then the method proceeds to block **206**.

At block **206**, the initial player matrix described above is generated. The initial player matrix includes information about the player, the type of game, and other such information about the game as described by the player data fields **74** shown in FIG. **6**. The initial player matrix is then communicated to block **208** which transmits initial player matrix to the transactional system for validation. Additionally, the initial player matrix is communicated to the next block **210** in the broadband gaming system which starts the gaming module.

At block **210**, the initial player matrix is received by the gaming module **84** and the gaming module **84** is engaged. At a minimum the gaming module **84** comprises a random number generator **86** and a paytable module **88**. The random number generator generates at least one random number that is used during the game. The paytable module **88** is used to determine the prize associated with the at least one random number.

Referring to FIG. **11**, a continuation of the broadband gaming system method is shown. By way of example, the gaming module may comprise a plurality of different random number generators. The blocks **214** and **216** describe the processes performed by a random number generator and a paytable module, respectively. The random number generator **86** of block **214** determines the winning combination of numbers for the game. At block **216**, the paytable module **88** is used to determine the prize awarded to the player. Preferably, the paytable module **88** is also configured to provide image IDs that identify the images associated with the prize. Preferably, the paytable module **88** is resident in both the broadband gaming system and the transactional system. The purpose for this redundancy is as a security check for output generated by the gaming module. The method then proceeds to block **218**.

At block **218** the player outputs with the same image IDs are grouped together. The grouping process is performed to simplify the broadcasting of the images to the plurality of players. By grouping the players according to the same image ID and having identified the network access device used by the player, a dynamic broadcasting method is created which occupies minimal downstream bandwidth. The method then proceeds to block **220**.

At block **220** a final player matrix is completed. The final player matrix includes the same data fields as the initial player matrix. Additionally, the final player matrix includes the random number output and the paytable output. The final player matrix is then communicated to the transactional system as described in block **222**. The method then proceeds to decision diamond **224**.

At decision diamond **224**, a validation procedure is conducted. The validation procedure essentially compares the transactional system's reverse calculation of the random numbers with the random numbers generated by the gaming module. If the random numbers in the transactional system are not the same or similar to the random numbers generated by the random number generator, a system failure or security breach is detected. If a security breach or system failure is detected, the method then proceeds to process block **226**, which initiates diagnostic procedures. If the random numbers match, then the method proceeds to block **228**.

At block **228**, the plurality of images are broadcast. The images are preferably broadcast along one downstream channel for each network access device. However, traffic considerations may require the use of a plurality of downstream channels. By way of example, for DOCSIS and DSL type downstream transmissions, the streaming video preferably occupies a portion of the bandwidth available for a cable modem or DSL modem, respectively. In an alternative example, for an interactive set-top box environment, the downstream channel preferably occupies one 6 MHz or 8 MHz band or a portion of the 6 MHz or 8 MHz band. The method then proceeds to the next block **230**.

At block **230**, the broadcast images are encoded for downstream transmission. It shall be appreciated by those skilled in the art having the benefit of this disclosure that downstream transmission systems are well known and can be easily integrated into the systems and method described in this patent. The method then proceeds to block **232**.

At block **232**, the broadcast images are encrypted for downstream transmission. The purpose for downstream encryption is to prevent unauthorized access to the downstream signal. It shall be appreciated by those skilled in the art that various secure systems and methods for downstream transmission of images are well known.

It shall be appreciated by those skilled in the art having the benefit of this disclosure that a plurality of games may be played simultaneously. The games may be played in a distributed/parallel manner or in serial manner.

An Illustrative Game

An illustrative game is described to show how the system and method described above operates. The illustrative game described herein is a progressive slot machine. It is well known that in the United States many states have legalized lottery games even though other games of chance, such as progressive slot machines, have not been legalized. It is also well known that in casino gaming floors the most popular games are progressive slot machines. The present illustrative game operates on the system and method described above and provides an output similar to a progressive slot machine with a lottery type input.

The illustrative game includes first having a player provide a plurality of letters or numbers that are either generated by the player or are selected in a random manner. The random number generator of the gaming module is then engaged and a gaming module random number is generated. Preferably, the order that the random numbers were generated is used to determine the prize awarded to the player. A programmed paytable is then used to compare the player selected numbers to the gaming module random numbers according to the rules programmed into the paytable module. Based on the results of this comparison, a prize is awarded to the player. An image ID is associated with the prize awarded. The plurality of players are then grouped according to their respective image IDs. A broadcast stream for the plurality of images associated with each image ID is broadcast to each player.

A more concrete example includes having a player select a plurality of numbers, such as the numbers below:

25 35 8 15 42

The random number generator of the gaming module is then engaged. By way of example the random number results are:

56 2 3 8 42

The paytable module is then programmed to interpret the random numbers generating by the gaming module according to the following illustrative rules:

1. If a match between one number is achieved, then a prize of I× the initial bet credit is awarded and an image ID XQ23-1396 is used. Image ID XQ23-1396 is an animated plurality of images representing three cherries.

2. If a match between one number at the same location is achieved, then a prize of 2× the initial bet credit is awarded and an image ID XQ23-1397 is used. Image ID XQ23-1397 is an animated plurality of images representing four cherries.

3. If a match between a first number is achieved and a match between a second number is achieved, then a prize of 5× the initial credit is awarded and an image ID XQ23-1998 is used. Image ID XQ23-1998 is an animated plurality of images representing 3 oranges.

4. If a match between a first number at the same location is achieved and a match between a second number is achieved, than a prize of 7× the initial credit is awarded and an image ID XQ23-1999 is used. Image ID XQ23-1999 is an animated plurality of images representing 4 oranges.

Thus, for the illustrative example provided above, the player having selected the numbers: 23, 35, 8, 15 and 42 is entitled to a prize of 7× the initial credit for a random number: 56, 2, 3, 8, and 42. The associated images displayed on the network access device are an animated plurality of images representing 4 oranges.

The scope of the invention should be determined by the appended claims and their legal equivalents rather than by the examples given.

What is claimed is:

1. A networked gaming system comprising:

a user identification received by at least one network access device that is compared with registration data in a registration database, wherein a player is provided access to a game when the user identification matches the registered player data;

a transactional component that charges the registered player at least one credit for a game outcome;

a centralized networked gaming module that performs game operations and generates at least one random game output by random generation at the networked gaming module;

the networked gaming module associates the at least one random game output with an image ID; and

the networked gaming module communicates one or more images corresponding to the image ID to the network access device.

2. The networked gaming system of claim **1** further comprising a countdown timer that provides a window of time for other players to join the game.

3. The networked gaming system of claim **1** further comprising an encryption module, the encryption module configured to encrypt the plurality of images communicated to each network access device.

4. The networked gaming system of claim **1**, wherein the images communicated to the network access device are viewable on a browser.

5. The networked gaming system of claim **1**, wherein the network access device includes a gaming terminal.

6. The networked gaming system of claim **1**, wherein the network access device includes a wireless device.

7. The networked gaming system of claim **1**, wherein the one or more images communicated to the network access device game include a slot machine game outcome.

8. The networked gaming system of claim **7**, wherein the networked gaming module generates the random game output with a lottery game.

9. A networked gaming system comprising:

a registration database that includes a registered player biometric;

an input player biometric that is received by at least one network access device, wherein a player is provided access to a game when the input player biometric matches the registered player biometric;

a transactional component that charges the registered player at least one credit for a game outcome;

a centralized networked gaming module that performs game operations and generates at least one random game output by random generation at the networked gaming module;

the networked gaming module associates the at least one random game output with an image ID; and

the networked gaming module communicates one or more images corresponding to the image ID to the network access device.

10. The networked gaming system of claim **9** further comprising a countdown timer that provides a window of time for other players to join the game.

11. The networked gaming system of claim **9** further comprising an encryption module, the encryption module configured to encrypt the plurality of images communicated to each network access device.

12. The networked gaming system of claim **9**, wherein the images communicated to the network access device are viewable on a browser.

13. The networked gaming system of claim **9**, wherein the network access device includes a gaming terminal.

14. The networked gaming system of claim **9**, wherein the network access device includes a wireless device.

15. The networked gaming system of claim **9**, wherein the one or more images communicated to the network access device game include a slot machine outcome.

16. The networked gaming system of claim **15**, wherein the networked gaming module generates the random game output with a lottery game.

17. A networked gaming method comprising:

receiving a user identification from at least one network access device, wherein the user identification is compared with registration data in a registration database;

providing a player with access to a game when the user identification matches the registered player data;

charging the registered player at least one credit for a game outcome;

enabling a centralized networked gaming module to perform the game operations and generate at least one random game output by random generation at the networked gaming module;

enabling the networked gaming module to associate the at east one random game output with an image ID; and

enabling the networked gaming module to communicate one or more Images corresponding to the image ID to the network access device.

18. The networked gaming method of claim **17** further comprising:

receiving a registered player biometric associated with the player and storing the registered player biometric in the registration database;

receiving an input player biometric from the network access device; and

providing access to the game when the input player biometric matches the registered player biometric.

19. The networked gaming method of claim **18** further comprising enabling a countdown timer to provide a window of time for other players to join the game.

20. The networked gaming method of claim **18** further comprising encrypting the plurality of images communicated from the networked gaming module to each network access device.

21. The networked gaming method of claim **18**, wherein the images communicated to the network access device are viewable on a browser.

22. The networked gaming method of claim **18**, wherein the network access device includes a gaming terminal.

23. The networked gaming method of claim **18**, wherein the network access device includes a wireless device.

24. The networked gaming method of claim **18**, wherein the one or more images communicated to the network access device game include a slot machine game outcome.

25. The networked gaming system of claim **24**, wherein the networked gaming module generates the random game output with a lottery game.

26. The networked gaming system of claim **1**, the networked gaming module communicating a plurality of images corresponding to the image ID to the network access device.

27. The networked gaming system of claim **9**, the networked gaming module communicating a plurality of images corresponding to the image ID to the network access device.

28. The networked gaming method of claim **18**, further comprising enabling the networked gaming module to communicate a plurality of images corresponding to the image ID to the network access device.

* * * * *

US008506407B2

(12) **United States Patent**
Kerr

(10) **Patent No.: US 8,506,407 B2**
(45) **Date of Patent: *Aug. 13, 2013**

(54) **GAMING SYSTEM NETWORK AND METHOD FOR DELIVERING GAMING MEDIA**

(75) Inventor: **Michael A. Kerr**, Reno, NV (US)

(73) Assignee: **NexRF, Corp.**

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 117 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **12/982,656**

(22) Filed: **Dec. 30, 2010**

(65) **Prior Publication Data**

US 2011/0165936 A1 Jul. 7, 2011

Related U.S. Application Data

(63) Continuation of application No. 10/681,034, filed on Oct. 8, 2003, now Pat. No. 8,403,755, which is a continuation of application No. 09/899,559, filed on Jul. 5, 2001, now abandoned.

(60) Provisional application No. 60/266,956, filed on Feb. 6, 2001.

(51) **Int. Cl.**
A63F 9/24 (2006.01)

(52) **U.S. Cl.**
USPC **463/42**; 705/44; 463/20; 463/16

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,339,798	A	7/1982	Hedges et al.
4,856,787	A	8/1989	Itkis
5,586,937	A	12/1996	Menashe
5,594,491	A	1/1997	Hodge et al.
5,630,757	A	5/1997	Gagin et al.
5,643,086	A	7/1997	Alcorn et al.
5,738,583	A	4/1998	Comas et al.
5,761,416	A	6/1998	Mandal et al.
5,762,552	A	6/1998	Vuong et al.
5,768,382	A	6/1998	Schneier et al.
5,779,545	A	7/1998	Berg et al.
5,800,268	A	9/1998	Molnick

(Continued)

OTHER PUBLICATIONS

"Internet Industry Interacting Gambling Code: A Code for Industry Co-Regulation in the Area of Internet Gambling Content Pursuant to the Requirements of the Interactive Gaming Act of 2001". Internet Industry Association. Dec. 2001.

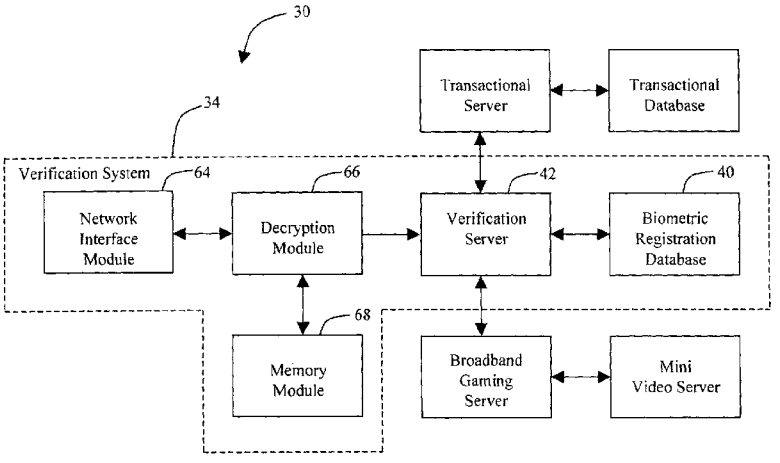
(Continued)

Primary Examiner — Paul A D'Agostino
(74) *Attorney, Agent, or Firm* — Michael A. Kerr; Kerr IP Group, LLC

(57) **ABSTRACT**

A gaming system network and gaming method are described. The network includes at least one network access device, a registration database configured to store registration data associated with each user, a verification system communicatively connected with the at least one network access device and the registration database, a video server, and a gaming system. The verification system verifies that the user associated with the network access device is a registered user and verifies security information received from the network access device. The video server stores a plurality of images corresponding to at least one game type. The gaming system generates at least one random game output associated with at least one game outcome, and communicates the plurality of images corresponding to the at least one game outcome to the at least one network access device.

21 Claims, 9 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

5,851,149	A		12/1998	Xidos et al.
5,871,398	A		2/1999	Schneier et al.
5,902,983	A		5/1999	Crevalt et al.
5,971,849	A	*	10/1999	Falciglia 463/16
6,001,016	A	*	12/1999	Walker et al. 463/42
6,010,404	A		1/2000	Walker et al.
6,106,396	A		8/2000	Alcorn et al.
6,142,876	A		11/2000	Cumbers
6,178,510	B1		1/2001	O'Connor et al.
6,409,602	B1		6/2002	Wiltshire et al.
6,500,068	B2		12/2002	Walker et al.
6,508,709	B1	*	1/2003	Karmarkar 463/42
6,508,710	B1		1/2003	Paravia et al.
6,527,638	B1		3/2003	Walker et al.
6,575,834	B1		6/2003	Lindo
6,612,928	B1		9/2003	Bradford et al.
6,628,939	B2		9/2003	Paulsen
6,676,522	B2		1/2004	Rowe
6,682,421	B1		1/2004	Rowe et al.
6,709,333	B1		3/2004	Bradford et al.
6,709,631	B2		3/2004	Mori et al.
6,719,631	B1	*	4/2004	Tulley et al. 463/17
6,749,512	B2		6/2004	MacGregor et al.
6,875,110	B1	*	4/2005	Crumby 463/42
6,884,162	B2		4/2005	Raverdy et al.
6,942,574	B1	*	9/2005	LeMay et al. 463/41
7,107,245	B1	*	9/2006	Kowalick 705/44
7,338,372	B2		3/2008	Morrow et al.
7,341,522	B2		3/2008	Yamagishi
7,534,169	B2		5/2009	Amaitis et al.
7,611,407	B1		11/2009	Itkis et al.
7,753,772	B1	*	7/2010	Walker et al. 463/17
8,029,349	B2		10/2011	Lind
2001/0004768	A1		6/2001	Hodge et al.
2001/0005908	A1		6/2001	Hodge et al.
2002/0002073	A1	*	1/2002	Montgomery et al. 463/13
2002/0007494	A1		1/2002	Hodge
2002/0056125	A1		5/2002	Hodge et al.
2002/0056143	A1		5/2002	Hodge et al.
2002/0077167	A1	*	6/2002	Merari 463/13
2002/0142815	A1	*	10/2002	Candelore 463/1
2002/0142844	A1		10/2002	Kerr
2006/0189382	A1		8/2006	Muir et al.
2007/0087834	A1		4/2007	Moser et al.
2007/0270212	A1		11/2007	Cockerille et al.
2008/0026844	A1		1/2008	Wells
2008/0057894	A1		3/2008	Aleksic et al.
2008/0097858	A1		4/2008	Vucina et al.

OTHER PUBLICATIONS

Wirelss Network. Wikipedia. http://en.wikipedia.org/wiki/Wireless_network. Nov. 17, 2008.

"Tracking Cookie." Wikipedia. http://en.wikipedia.org/wiki/Tracking_cookie. May 24, 2009.

* cited by examiner

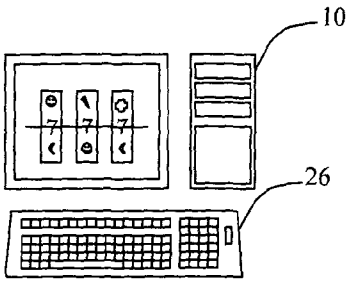


FIG. 1a

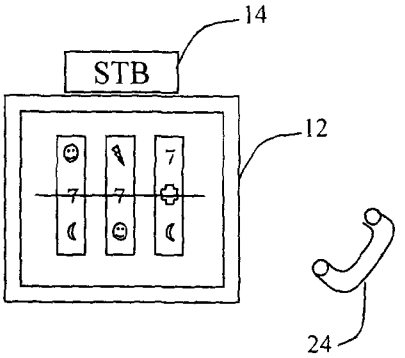


FIG. 1b

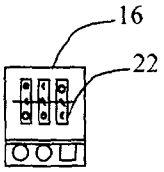


FIG. 1c

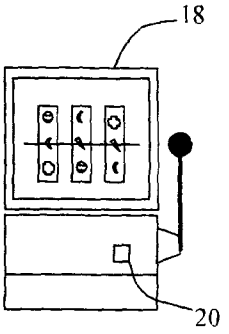
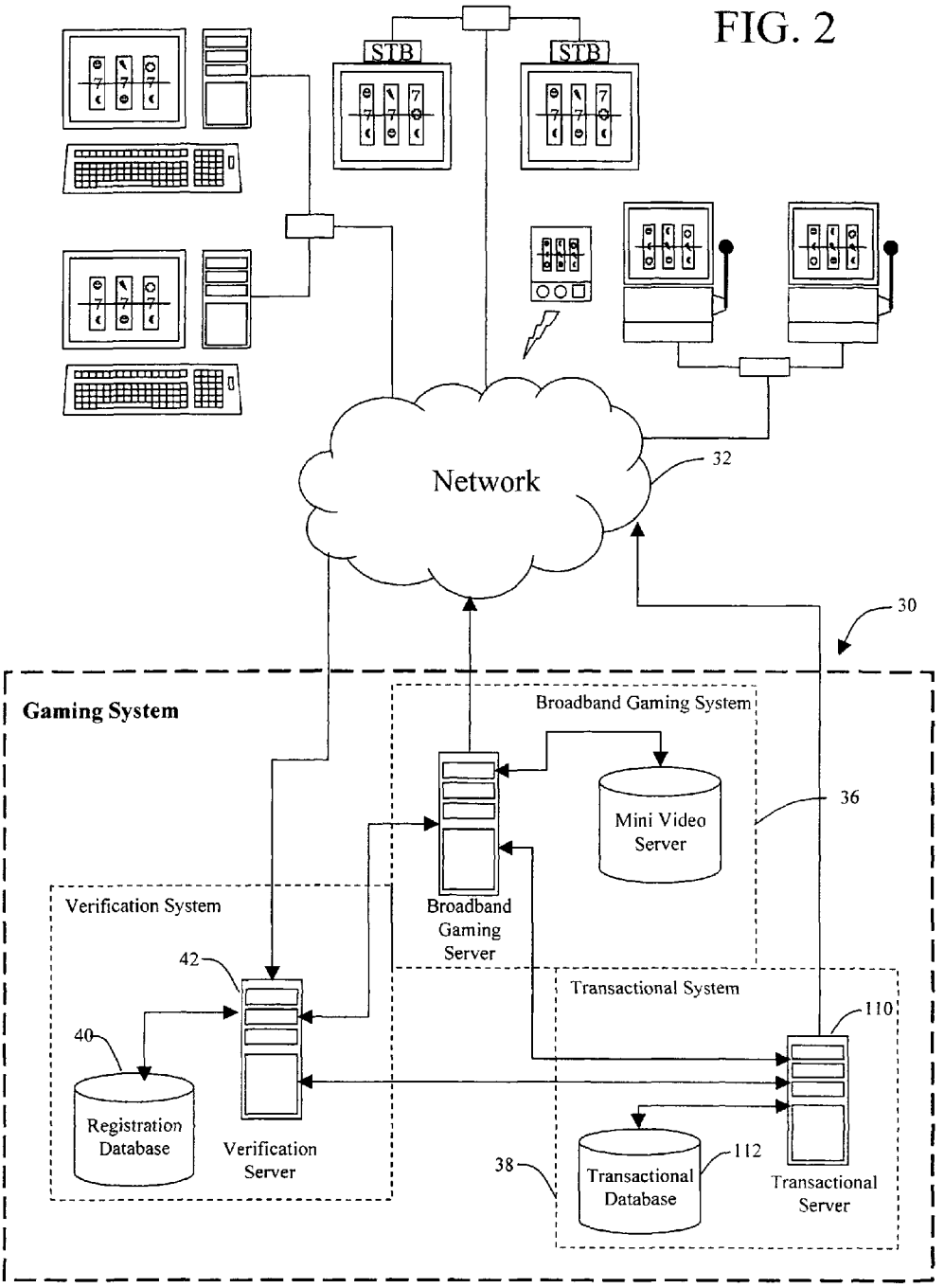


FIG. 1d

FIG. 2


STB
STB
Network
32
30
Gaming System
Broadband Gaming System
Mini Video Server
36
Broadband Gaming Server
Verification System
42
40
Registration Database
Verification Server
Transactional System
110
38
Transactional Database
112
Transactional Server

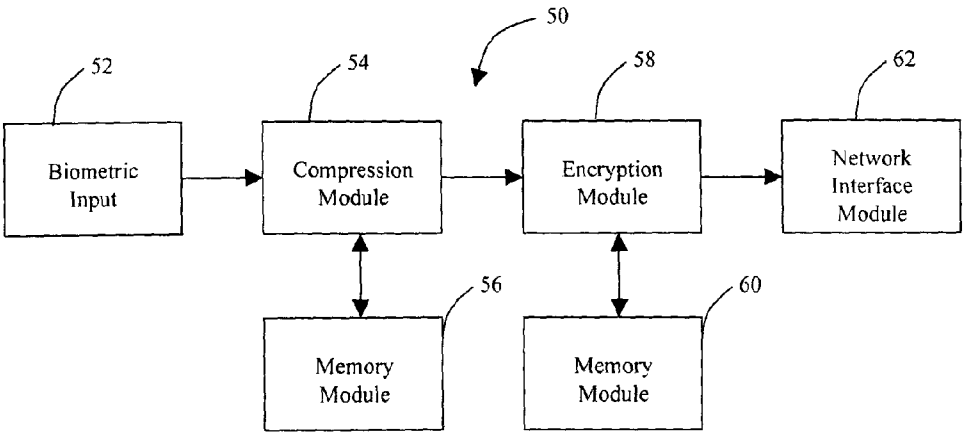

50
52
54
58
62
Biometric Input
Compression Module
Encryption Module
Network Interface Module
56
60
Memory Module
Memory Module

FIG. 3

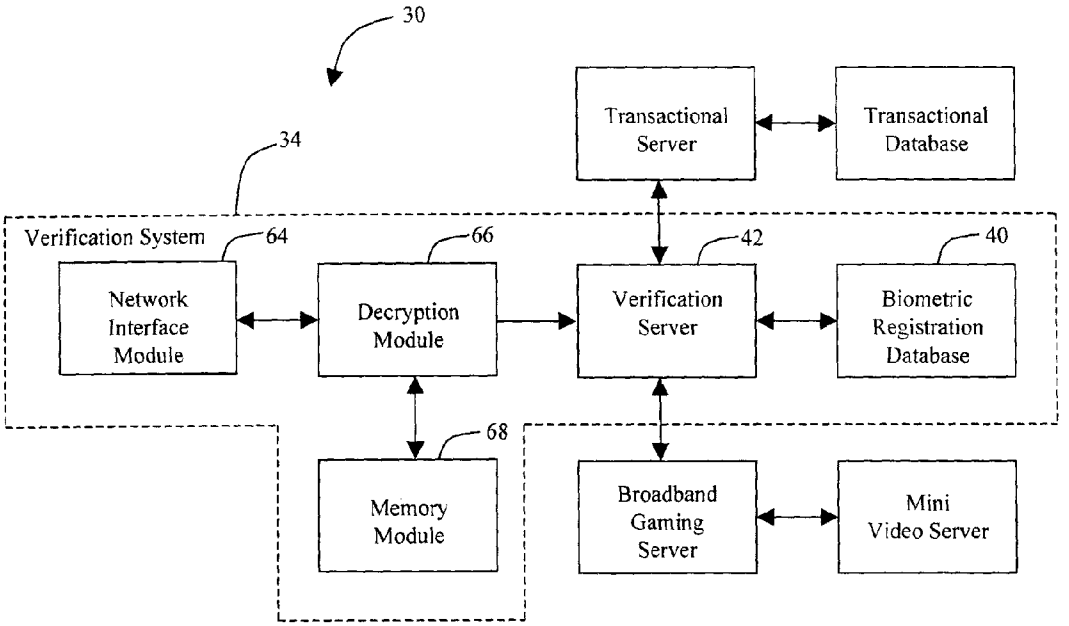

30
34
Transactional Server
Transactional Database
Verification System
64
66
42
40
Network Interface Module
Decryption Module
Verification Server
Biometric Registration Database
68
Memory Module
Broadband Gaming Server
Mini Video Server

FIG. 4

70

REGISTRATION DATA FIELDS	
NAME	BIOMETRIC
ADDRESS	PLAYER ID
USER NAME	MAC ID
PASSWORD	IP ADDRESS
CREDIT CARD	BROWSER
DATE	COOKIES
TIME	CRYPTO KEYS

72

USER SUBMITTED DATA	
NAME	BIOMETRIC
ADDRESS	PLAYER ID
USER NAME	MAC ID
PASSWORD	IP ADDRESS
CREDIT CARD	BROWSER
DATE	COOKIES
TIME	CRYPTO KEYS

FIG. 5

74

PLAYER DATA FIELDS	
PLAYER ID	SESSION TIME FOR TYPE OF GAME
DATE	AMOUNT PLAYED DURING SESSION
TIME IN	CREDIT CARD INFORMATION
TIME OUT	TRANSACTION REQUEST
TYPE GAME	TRANSACTION APPROVAL
CREDITS IN	TRANSFER OF CREDITS
CREDITS OUT	TRANSFER TO PLAYER CREDIT CRD
BONUS	CRYPTO KEYS

FIG. 6

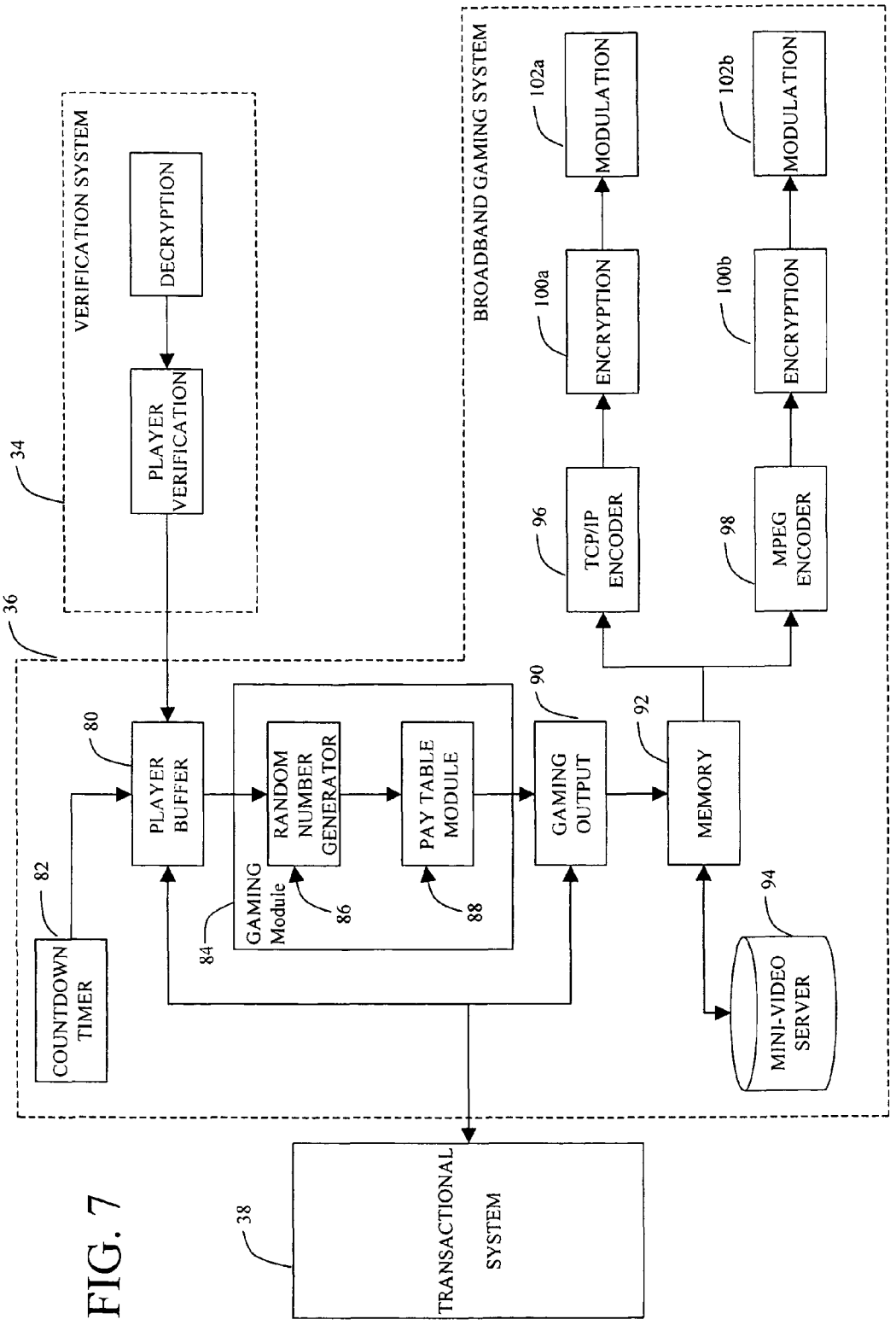

VERIFICATION SYSTEM
DECRYPTION
PLAYER VERIFICATION
34
36
BROADBAND GAMING SYSTEM
102a
MODULATION
102b
MODULATION
100a
ENCRYPTION
100b
ENCRYPTION
96
TCP/IP ENCODER
98
MPEG ENCODER
80
PLAYER BUFFER
RANDOM NUMBER GENERATOR
PAY TABLE MODULE
90
GAMING OUTPUT
92
MEMORY
GAMING Module
84
86
88
82
COUNTDOWN TIMER
94
MINI-VIDEO SERVER
38
TRANSACTIONAL SYSTEM

FIG. 7

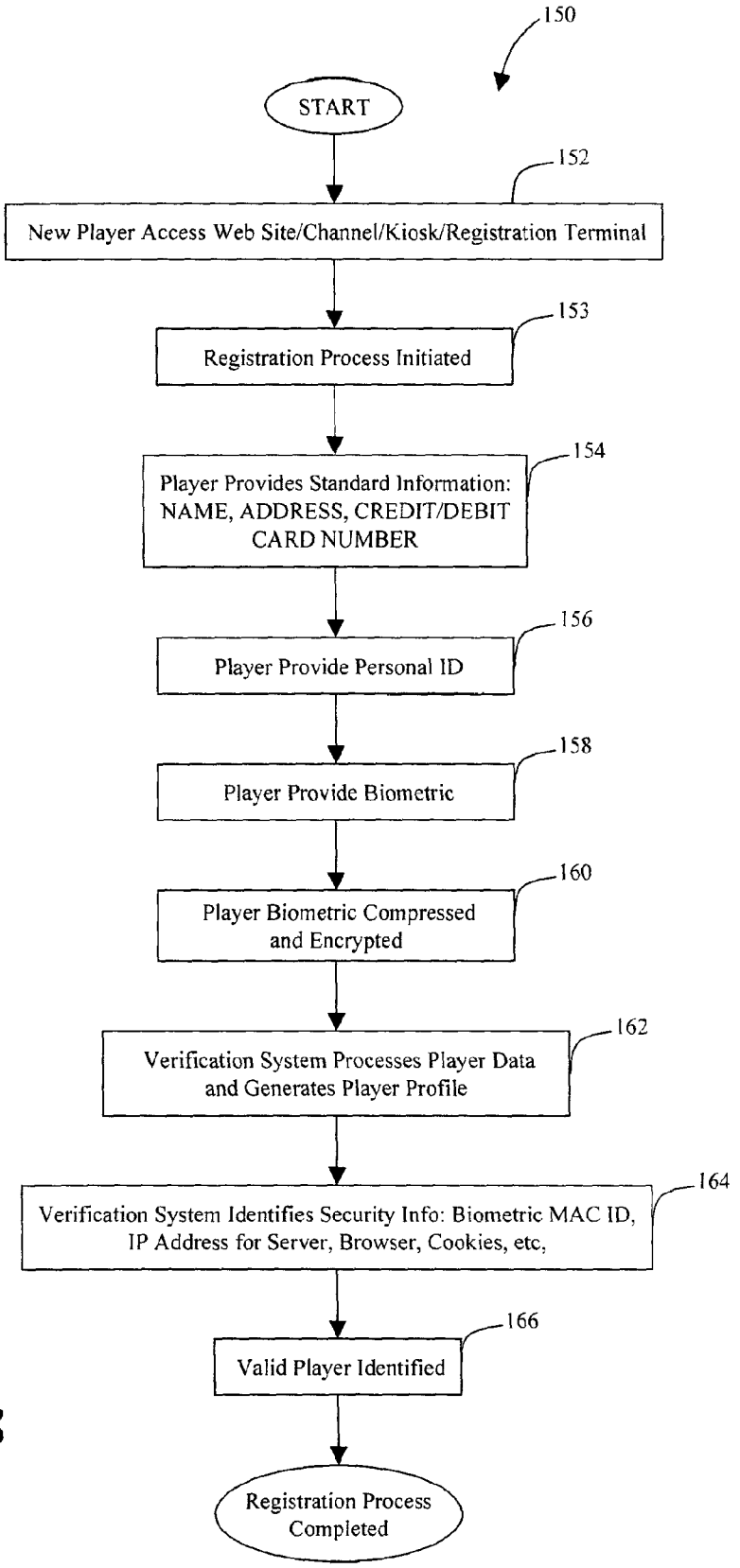

150
START
152
New Player Access Web Site/Channel/Kiosk/Registration Terminal
153
Registration Process Initiated
154
Player Provides Standard Information: NAME, ADDRESS, CREDIT/DEBIT CARD NUMBER
156
Player Provide Personal ID
158
Player Provide Biometric
160
Player Biometric Compressed and Encrypted
162
Verification System Processes Player Data and Generates Player Profile
164
Verification System Identifies Security Info: Biometric MAC ID, IP Address for Server, Browser, Cookies, etc,
166
Valid Player Identified
Registration Process Completed

FIG. 8

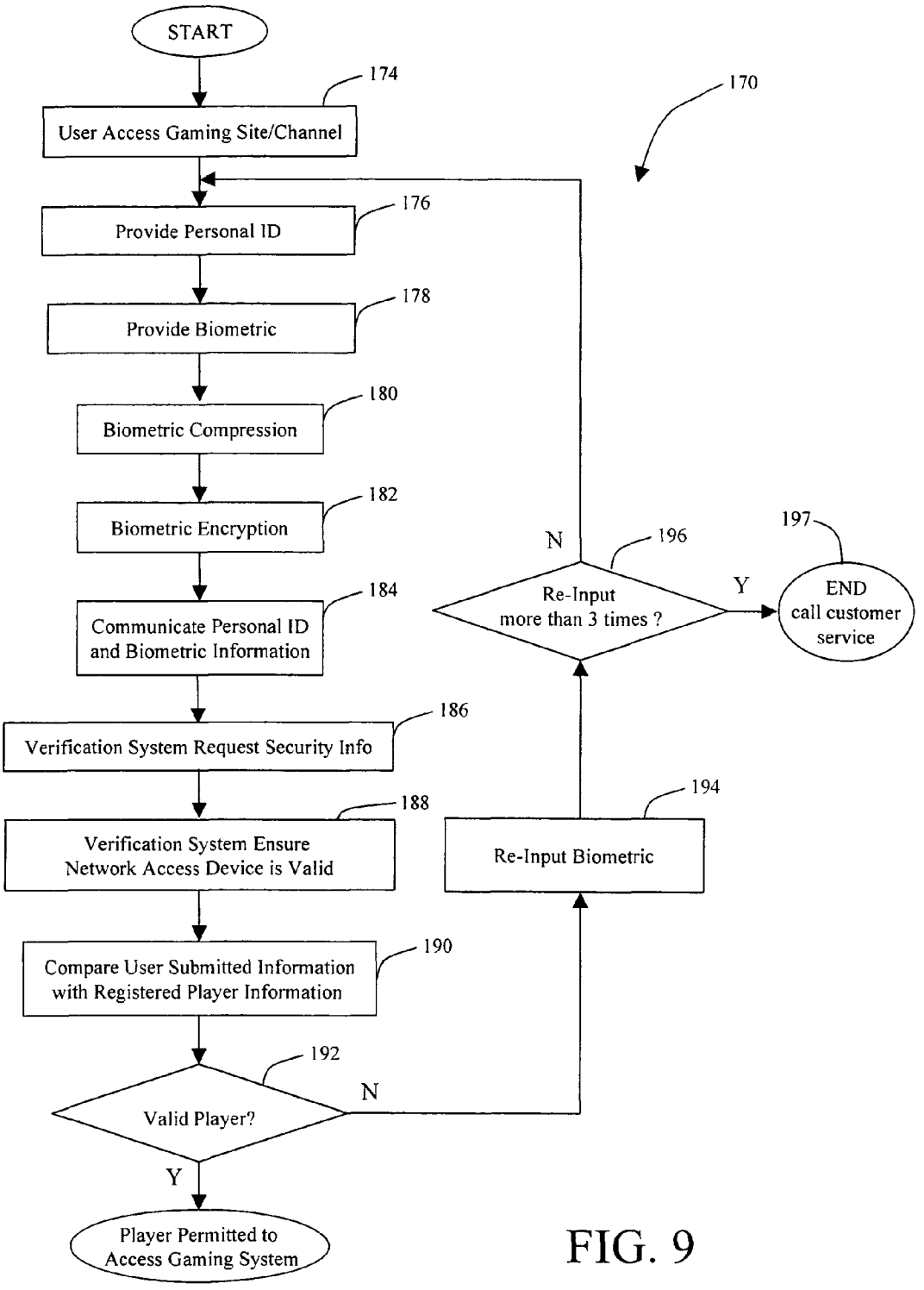

START
174
User Access Gaming Site/Channel
170
176
Provide Personal ID
178
Provide Biometric
180
Biometric Compression
182
Biometric Encryption
184
Communicate Personal ID and Biometric Information
186
Verification System Request Security Info
188
Verification System Ensure Network Access Device is Valid
190
Compare User Submitted Information with Registered Player Information
192
Valid Player?
N
Y
Player Permitted to Access Gaming System
194
Re-Input Biometric
196
Re-Input more than 3 times ?
N
Y
197
END call customer service

FIG. 9

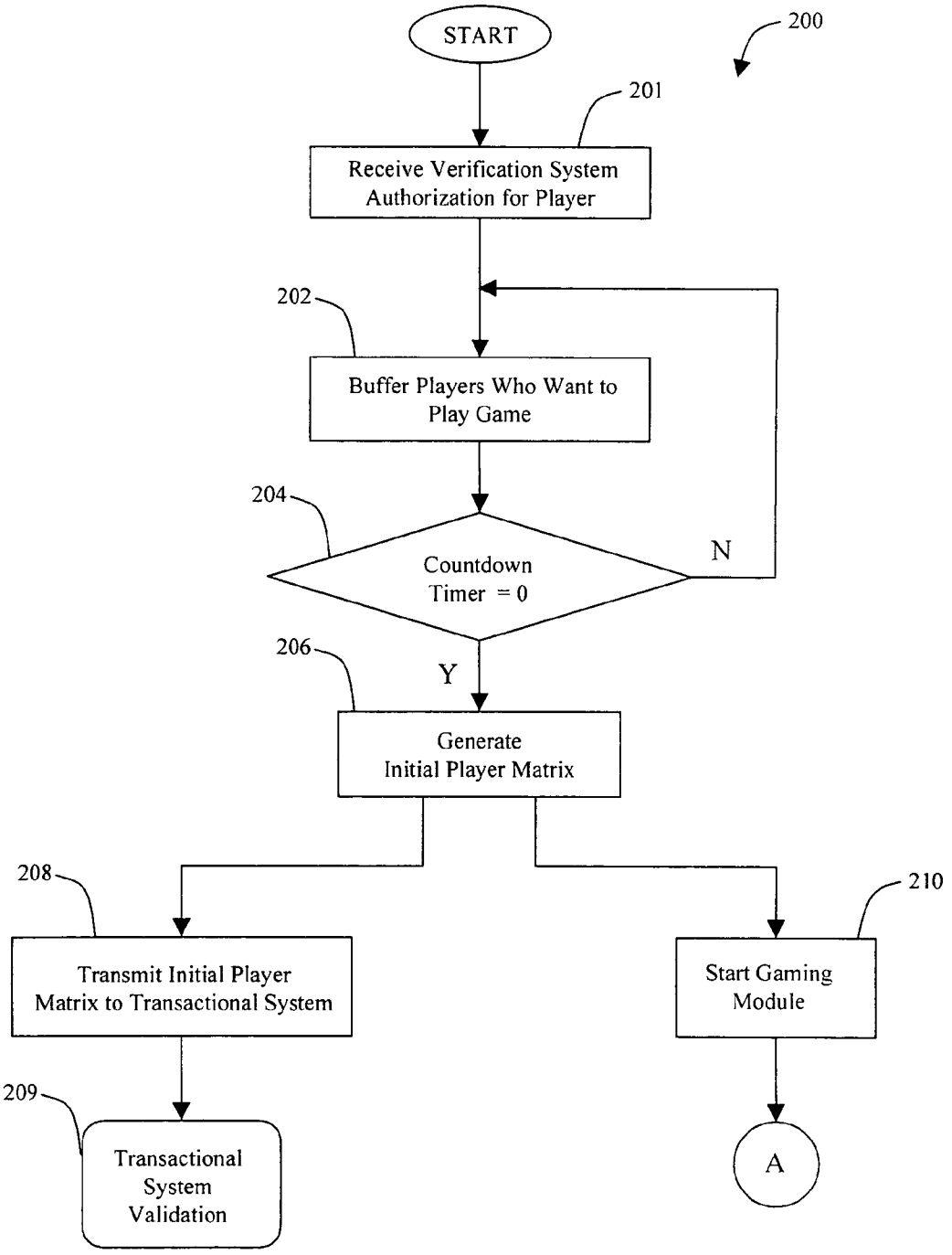

START
200
201
Receive Verification System Authorization for Player
202
Buffer Players Who Want to Play Game
204
Countdown Timer = 0
N
Y
206
Generate Initial Player Matrix
208
Transmit Initial Player Matrix to Transactional System
209
Transactional System Validation
210
Start Gaming Module
A

FIG. 10

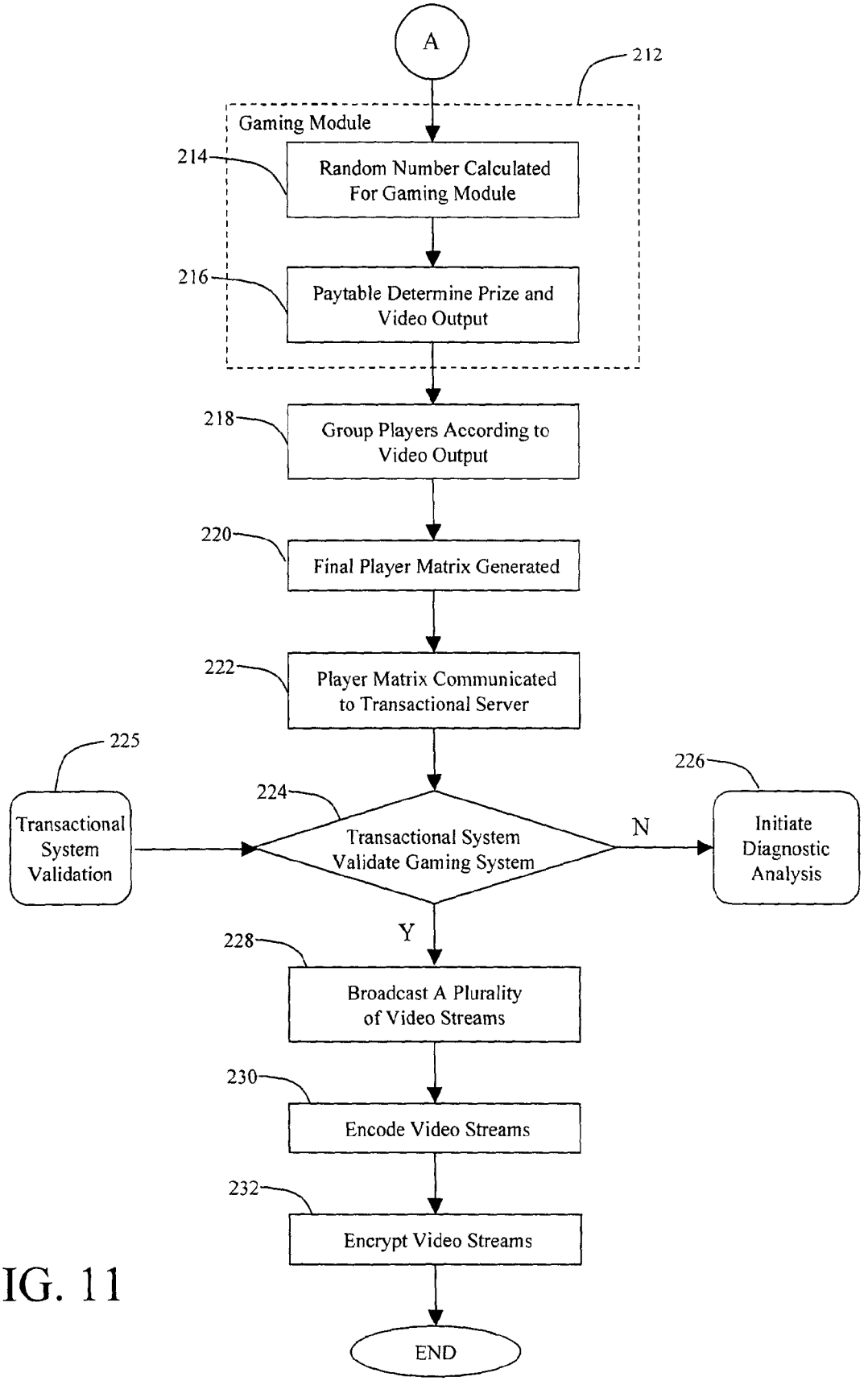

A
212
Gaming Module
214
Random Number Calculated For Gaming Module
216
Paytable Determine Prize and Video Output
218
Group Players According to Video Output
220
Final Player Matrix Generated
222
Player Matrix Communicated to Transactional Server
225
Transactional System Validation
224
Transactional System Validate Gaming System
N
226
Initiate Diagnostic Analysis
Y
228
Broadcast A Plurality of Video Streams
230
Encode Video Streams
232
Encrypt Video Streams
END

FIG. 11

GAMING SYSTEM NETWORK AND METHOD FOR DELIVERING GAMING MEDIA

CROSS REFERENCES TO RELATED APPLICATIONS

This patent application is a continuation of Ser. No. 10/681,034, filed Oct. 8, 2003 now U.S. Pat. No. 8,403,755 which is a continuation of patent application Ser. No. 09/899,559 having a filing date of Jul. 5, 2001, now abandoned, which claims the benefit of provisional patent application 60/266,956 filed Feb. 6, 2001.

BACKGROUND

1. Field

The present invention is an interactive gaming system network and method for delivering gaming media. More particularly, the interactive gaming system and method operates in a networked environment that interfaces with a gaming server and a video server.

2. Description of Related Art

The related art includes gaming devices, on-line gaming, networked interactive gaming, and biometrics.

Gaming Devices

For purposes of this patent, the term "gaming" shall refer to either gambling and/or gaming applications. Gaming devices include games of skill and games of chance. Games of chance include many casino-type gaming devices in which the outcome of the game depends, at least in part, on a randomly generated event. For example, a game of chance may use a random number generator to generate a random or pseudo-random number. The random number may then be compared to a predefined table to determine the outcome of the event. If the random number falls within a certain range of numbers on the table, the player may win a predefined prize. The table may also contain display information that allows the gaming device to generate a display that corresponds to the outcome of the game. The gaming device may present the outcome of the game on a large variety of display devices, such as mechanical spinning reels or video screens.

Games of skill comprise a skill component in which a player combines letters or words (word puzzles), answers questions (trivia), overcomes challenges (video games), competes with other players (networked video games), and the like. Generally, a game of skill is a game requiring a level of skill which does not rely solely on chance. Some games of skill require a high degree of expertise and knowledge and other games of skill require very limited expertise or knowledge.

On-Line Gaming

In June 2001, Nevada signed a bill that could result in Nevada being the first state to offer legalized gambling over the Internet. The new law authorizes state gaming regulators to set up an infrastructure to license and oversee online gaming in Nevada when such gaming becomes legal. Online gaming is a federal issue whose legality is unclear at present.

A variety of technological limitations have been asserted as preventing Congress's endorsement of on-line gaming. These technological limitations are related to the prevention of underage gambling, controlling of gambling addiction, and ensuring the security and reliability of on-line gaming.

To prevent underage gambling prior art systems and methods use passwords, user IDs, credit cards and "click-through" agreements that ask the player to agree to being of legal gambling age by clicking on a button. Presently, there are no

systems and methods to control on-line gambling addiction. With respect to ensuring that on-line gaming is secure and reliable, prior art systems and methods use various cryptographic techniques such as RSA encryption, digital certificates, or other similar well known cryptographic methods. These cryptographic methods are helpful in ensuring secure communications, however these cryptographic methods do not ensure that the individual accessing the on-line game is a valid user.

In view of the prior art systems, a minor or other unauthorized individual simply needs a user ID and a corresponding password to access a gaming site. The obtaining of a user ID and password is a relatively simple task as this information is generally not modified. Commonly the user ID information is acquired by identifying the web site's naming convention for the player. The player password can be easily determined by remembering the pattern of keys typed by the player during the log-on procedures or by simply requesting the password from the player as part of a diagnostic procedure. The latter is a trick commonly used by hackers to access a system. The password problem may be overcome by modifying the password on a regular basis, however the player must then remember the modified password. Should the player forget the password a new password is mailed. During the mailing process it is common for e-mail to be easily intercepted in cyberspace. Additionally, it is common for unauthorized users to simulate being at a certain location by submitting an IP address that identifies an authorized user.

Therefore, a better system and method for identifying a valid user is needed. Additionally, it would be beneficial to provide a gaming system and method that would prevent underage gambling, be simple to implement, prevent gambling addiction, and provide a higher degree of security and reliability from unauthorized users.

Networked Interactive Gaming

Networked interactive gaming in an open networked environment such as the Internet is well-known. However, interactive gaming in an open network such as the Internet is confined to communicating with other devices using the same TCP/IP protocols. Currently networked interactive gaming systems using the TCP/IP protocol are not configured to communicate with interactive set-top boxes using MPEG protocols.

Networked interactive gaming in an open networked environment using traditional security methods such as secure socket layers and digital certificates are well known. However, networked interactive gaming in an open networked environment using traditional security methods does not prevent gambling from a minor having acquired a parent's user ID and password without the parent's consent.

Networked interactive gaming using LANs and WANs for progressive slot machines having large jackpots are also well-known. However, networked interactive systems using LANs and WANs for progressive slot machines generally exist in a highly secure proprietary network environment. Thus, the creation of a progressive slot machine with a large jackpot in an open network environment is not well known.

Biometrics

A biometric is a measurable psychological and/or behavioral trait that can be captured and subsequently compared with another instance at the time of verification. This definition includes the matching of fingerprints, voice patterns, hand geometry, iris and retina scans, vein patterns and other such methodologies. For purposes of the invention described heretofore, the definition of biometrics also includes signature verification, keystroke patterns and other methodologies weighted towards individual behavior.

Biometric applications for games of skill and games of chance are limited. For example biometric gaming applications are taught in U.S. Pat. No. 6,010,404 granted to Walker et al. teaches a method and apparatus for using player input codes (e.g., numeric, biometric or physical) to affect the outcomes of electronic gambling devices, such as slot machines. Additionally, U.S. Pat. No. 6,142,876 granted to Cumbers teaches a system and method for passively tracking the play of players playing gaming devices such as slot machines. Players provide identification information and facial recognition data is acquired by a digital or video camera. For each player an account file and a file of the facial image data is stored. When the player plays the slot machine, a camera scans the player and acquires facial image data which is compared to stored data to identify the player. Furthermore, U.S. Pat. No. 5,902,983 granted to Crevelt et al. teaches a gaming machine configured to perform EFT transactions which are limited to preset amounts. The patent teaches the use of a fingerprint imaging device, and retinal scans for verifying a player's identity.

Although biometric applications for gaming applications are known, biometric applications for on-line gaming systems are not known. Furthermore, the managing of biometric information and gaming information in an open network environment are not known. Additionally, the use of biometrics in a gaming system and method to prevent underage gambling and prevent gambling addiction is not known.

SUMMARY

A gaming system network is described. The network comprises at least one network access device. The network further comprises a registration database configured to store registration data associated with each user registered to use the gaming system. A verification system is communicatively connected with the at least one network access device and the registration database. The verification system is configured to receive user identification information from the at least one network access device, receive security information from the at least one network access device, verify that the user associated with the network access device is a registered user by comparing the user identification information to the registration data, and verify the security information received from the network access device. The network also has a video server configured to store a plurality of images corresponding to at least one game type. A gaming system of the network is configured to generate at least one random game output. The at least one random game output is associated with at least one game outcome. The gaming system is also configured to communicate the plurality of images corresponding to the at least one game outcome to the at least one network access device.

In another embodiment, the gaming system network is described. The network comprises a means for generating at least one game outcome and communicating a game output corresponding to the game outcome to the at least one network access device.

A gaming method is also described. The method comprises receiving user identification information associated with at least one network access device at a verification system. The method further comprises receiving security information associated with the at least one network access device at a verification system. The verification system verifies that the at least one network access device user is a registered user by comparing the user identification information to registration data stored in a registration database. The verification system also verifies the security information received from the at least one network access device. The at least one network access device is permitted to communicate with the gaming system when user identification information is successfully matched to the stored registration data and security information is successfully verified. The method further comprises storing in a video server a plurality of images corresponding to at least one game. The method also comprises generating with a gaming system at least one random game output. The at least one random game output is associated with at least one game outcome. The gaming system communicates the plurality of images corresponding to the at least one game outcome from the gaming system to the at least one network access device.

One advantage of the present invention is that it provides a system and method to prevent underage gambling.

A further advantage of the present invention is that it provides a more secure and reliable and secure gaming system and method.

Another advantage of the present invention is that it provides a system and method for managing biometric information and gaming information in an open network environment.

Another advantage of the present invention is that it permits a plurality of users in a geographically broad area to play the same game.

A further advantage of the present invention is that it provides a pseudo-real time gaming system and method.

Another advantage of the present invention is that it simulates a game of chance such as a slot machine in an on-line environment.

An additional advantage of the present invention is that it provides a networked jackpot.

BRIEF DESCRIPTION

A networked gaming system that comprises a verification system, a broadband gaming system and a transactional system is described. The verification system operations include ensuring that a user is a registered player by using a biometric input. The broadband gaming system operations include managing and performing at least one game. The transactional system operations include providing oversight for each transaction conducted by the verification system and the broadband gaming system.

A verification system for playing the networked gaming system is described. The networked games include games of chance and games of skill. The verification system communicates with a biometric input module and a network access device to generate a user identification information. The user identification information is compared to information in a registration database. If an acceptable match is made between the user identification information and the information in the registration database, the user is designated as a player. The player then has access to both the broadband gaming system and the transactional system.

A broadband gaming system which is in communication with the verification system is described. The broadband gaming system includes a buffer which stores information about players who desire to play a game. The buffer is operatively coupled to a random number generator that generates a random number for each player in the buffer. A paytable module in communication with the random number generator determines the outcome associated with the random number generator. The paytable also determines which images are associated with the outcome for each player. Preferably, the images are stored on a mini video server and then cached in a memory module. The images are intelligently buffered for

downstream communications. In its preferred embodiment, a plurality of encoders are operatively coupled to the memory module caching the broadcast video streams. The plurality of encoders encode the broadcast downstream images according the requirements for each network access device. Each encoder is operatively coupled to an encryption module that encrypts the broadcast. A modulation module is operatively coupled to the encryption module and modulates encrypted images for downstream transmission. Each network access device includes a tuner, a demodulation module, and a decryption module that permits an image to be viewed by the network access device.

A transactional system and method that ensures secure communications occur in the verification system and the broadband gaming system is described. The transactional system also performs accounting, bonusing, tracking and other such functions. Preferably, the transactional system is capable of receiving a plurality of funds from a financial account and converting them to credits that are used in the broadband gaming system.

The above description sets forth, rather broadly, the more important features of the present invention so that the detailed description of the preferred embodiment that follows may be better understood and contributions of the present invention to the art may be better appreciated. There are, of course, additional features of the invention that will be described below and will form the subject matter of claims. In this respect, before explaining at least one preferred embodiment of the invention in detail, it is to be understood that the invention is not limited in its application to the details of the construction and to the arrangement of the components set forth in the following description or as illustrated in the drawings. The invention is capable of other embodiments and of being practiced and carried out in various ways. Also, it is to be understood that the phraseology and terminology employed herein are for the purpose of description and should not be regarded as limiting.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the present invention are shown in the accompanying drawings wherein:

FIG. **1***a* through FIG. **1***d* provide diagrams of a plurality of network access devices.

FIG. **2** is a high level diagram of a gaming system networked to a plurality of network access devices.

FIG. **3** is a block diagram of an illustrative biometric input module.

FIG. **4** is a block diagram of a gaming system configured to receive a biometric input from a network access device.

FIG. **5** is a table of the data fields in a verification system.

FIG. **6** is a table of the data fields in a broadband gaming system and in a transactional system.

FIG. **7** is a block diagram of a broadband gaming system.

FIG. **8** is a flowchart of the registration method for the gaming system.

FIG. **9** is a flowchart of the verification method for the gaming system.

FIG. **10** is a flowchart of the information processed by the gaming system.

FIG. **11** is a continuation of the flowchart of the information processed by the gaming system in FIG. **10**.

DETAILED DESCRIPTION

In the following detailed description of the preferred embodiments, reference is made to the accompanying drawings, which form a part of this application. The drawings show, by way of illustration, specific embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

Network Access Devices

Referring to FIG. **1***a* through FIG. **1***d* there is shown a plurality of illustrative network access devices. Each of the network access devices is configured to be capable of running a gaming application. For illustrative purposes the gaming application shown simulates the spinning reels of a slot machine.

The network access device in FIG. **1***a* is a personal computer **10** having a network interface card (not shown) that may be operatively coupled to a modem (not shown). Another network access device shown in FIG. **1***b* includes a television **12** operatively coupled to an interactive set-top box **14** that is operatively coupled to a cable network (not shown). The other network access device shown in FIG. **1***c* is a wireless device **16** such as a digital phone or personal digital system (PDA) or other such wireless device which is configured to communicate with a network using wireless networking protocols. Yet another network access device is shown in FIG. **1***d* and includes a gaming terminal **18** such as a slot machine on a casino floor that is operatively coupled to a plurality of other gaming terminals. It shall be appreciated by those skilled in the art of networking that the distinguishing feature between each of these network access devices is the type of communications protocols used by each device to enable communications between similar network access devices.

Each of the network access devices either includes a biometric input module operatively coupled to the network access device or includes a biometric input module communicatively coupled to the network access device. A biometric is a measurable psychological and/or behavioral trait that can be captured and subsequently compared with another instance at the time of verification. This definition includes the matching of fingerprints, voice patterns, hand geometry, iris and retina scans, vein patterns and other such methodologies. For purposes of the invention described heretofore, the definition of biometrics also includes signature verification, keystroke patterns and other methodologies weighted towards individual behavior.

In one illustrative embodiment, the biometric input module is a fingerprint scanner **20** resident on the gaming terminal **18** wherein the biometric input is a fingerprint. In another illustrative embodiment, the biometric input module is the screen **22** of wireless device **16** wherein the screen is configured to receive a biometric input such as a user signature. In yet another illustrative embodiment, the biometric input module is a telephone **24** that is configured to receive a voice pattern from a user prior to engaging communications with the interactive set-top box **14**. In yet another illustrative embodiment the biometric input module is a keyboard **26** operatively coupled to computer **10** wherein the user is requested to input a keystroke pattern. An illustrative example of a biometric input module operatively coupled to the network access device is shown in FIG. **1***d* having the fingerprint scanner **20** on the gaming terminal **18**. An illustrative example of a biometric input module, e.g. the telephone **24**, communicatively coupled to the network access device, e.g. the interactive set-top box **14**, is shown in FIG. **1***b*.

The biometric input is used to prevent unauthorized gaming activity and efficiently store credits on the user's behalf. By way of example and not of limitation, unauthorized gaming activity includes preventing underage gaming and prohib-

iting players with histories of gambling addiction. Additionally, player credits may be stored on a network so that the player does not need to carry coins, paper currency, coupons, credit cards or debits cards to play a game. It shall be appreciated by those skilled in the art having the benefit of this disclosure that different biometric input modules may be used in conjunction with different network access devices.

Gaming System

Referring to FIG. **2** there is shown a high level block diagram of a gaming system **30** in communication with a plurality of network access devices coupled to a network **32**. The gaming system includes a verification system **34**, a broadband gaming system **36** and a transactional system **38**. The verification system **34** verifies that a user operating a network access device is a registered player. The broadband gaming system **36** performs the function of generating a game and broadcasting the game results to each of the network access devices. The transactional system **38** performs a plurality of functions including tracking each transaction performed by both the verification system and the broadband gaming system and conducting electronic fund transfers.

Verification System

The verification system **34** verifies that a user desiring to play the game is a registered player. The verification system **34** communicates with the biometric input module and a network access device to generate user identification information. The user identification information includes information such as cryptographic keys that are necessary to securely identify the network access device. The user identification information also includes media access control (MAC) identification and confirmation of the user Internet Protocol (IP) address. The user identification information is compared to information in a registration database **40** by a verification server **42**. If an acceptable match is made between the user identification information and the information in the registration database, the user is designated as a player. The player then has access to either the broadband gaming system **36** or the transactional system **38**.

In an alternative embodiment the user identification information is housed in a smart card (not shown) that is in communication with the verification system **34**. The smart card includes a stored biometric which is used to identify the user as a player. Cryptographic keys are then exchanged between the verification system **34** and the smart card to provide the player access to either the broadband gaming system or the transactional system **38**.

Referring to FIG. **3** there is shown an illustrative biometric input module **50**. By way of example, the illustrative biometric input module **50** is a fingerprint scanner. It shall be appreciated by those skilled in the art having the benefit of this disclosure that the use of the fingerprint scanner as the illustrative biometric input module is not restrictive. A scanned fingerprint image is collected by the biometric input **52**. After the scanned fingerprint image is collected, the fingerprint image is compressed by the compression module **54**. A memory module **56** provides fast memory resources for the compression of the fingerprint image. After compression, the fingerprint image is encrypted by the encryption module **58** for downstream transmission. The encryption module **58** also includes a memory module **60** that provides fast memory resources for the encryption of the compressed fingerprint image. An encrypted compressed fingerprint image is then communicated to network **32** (see FIG. **2**) using the network interface module **62**.

Referring to FIG. **4** there is shown a block diagram of the verification system **34**. The verification system is operatively coupled to network **32** with network interface module **64**. The network interface module **64** is configured to receive user identification information generated by the network access devices and from the biometric input module. Preferably, the biometric and other user identification information received by the verification system is an encrypted biometric that is decrypted by decryption module **66**. A memory module **68** is preferably a fast memory that expedites the decryption process. After decryption the biometric and remaining user identification information is processed by the verification server. It shall be appreciated by those skilled in the art that the verification server **42** may house the network interface module **64**, decryption module **66** and the memory module **68**. The verification server **42** is also in operative communication with a registration database **40**. The verification server **42** performs the function of matching the user identification information collected from the network access device with the player information in the registration database **40**. Additionally, the verification server **42** performs the caching functions needed to ensure that once a player has been identified during an initial game, subsequent usage by the same player proceeds quickly.

Preferably, the verification server **42** identifies registered players using a biometric template of the registered player residing on the registration database **40**. The registered players are referenced with Personal ID numbers. When a transaction is undertaken the user firstly calls up the particular template from the registration database **40** by inputting a Personal ID. The Personal ID includes a particular number, user ID, password or other such identification techniques. The inputting of the Personal ID is accomplished with a familiar numeric keypad, keyboard, magstripe card or smart card. The correct template is called and held in memory ready for comparison with the biometric sample provided by the user. A comparison takes place that results in a binary true or false condition as to the identity of the user. The user is in effect claiming an identity by inputting the Personal ID and the system is subsequently verifying that the claim is genuine according to the matching criteria setup within the system.

Referring to FIG. **5** there is shown the registration data fields **70** and user submitted data fields **72**. The registration data fields **70** include data fields that comprise the user identification information. The registration data fields include user identification information such as player name, address, user name, password, credit card information, and the date and time of the registration. The player biometric and Personal ID also comprises the user identification information and provides unique information about the player. The Personal ID may be the same as the user name or password. It shall be appreciated by those skilled in the art that some biometric information may be compressed. Furthermore, the user identification information includes data about the network access device and the network connection such as MAC ID, IP addresses, browser type, any cookies resident on the network access device, etc. Finally, the user identification system includes cryptographic keys which are used to encrypt and decrypt the communications between the verification system and each of the network access devices.

The user submitted data fields **72** mirror the registration data fields **70**. The user submitted data fields receive data generated by a user that is attempting to access the broadband gaming system **36**. The user submitted information is carefully analyzed to ensure that a valid user is being identified. It is well known that the connection of one network access device to another network access device generates security concerns. Preferably, the present verification system operates using a fast hardware-type firewall that performs a stateful multilayer inspection. In its preferred embodiment the fire-

wall provides packet filtering using a secure protocol such as IPSec. This protocol provides encryption of the data at the packet level as well as at the source address level. Without access to the encryption keys, a potential intruder would have difficulty penetrating the firewall. Additionally, it would be preferable to provide a circuit level gateway and an application level gateway. The circuit level gateway works on the session layer of the OSI model or the TCP layer of the TCP/IP model and monitors TCP handshaking between packets to determine whether a requested session is legitimate. The application level gateway filters data packets at the application layer of the OSI model. A stateful multilayer inspection firewall offers a high level of security, good performance and transparency to end users.

Referring to FIG. **6** there is shown the player data fields **74** that are generated by the broadband gaming system and the transactional system after the user has been verified to be a registered player. The player data fields **74** are used to generate a player matrix which is used as an additional internal security measure. The player data fields **74** include a Player ID that identifies the player, a timestamp that provides the date, time in and time out by the player during the game. Additionally, the type of game, credits played, and credits remaining are monitored. Based on the level of player activity a bonus is provided to the player. Further still the session time for each type of game and the amount played during the session is monitored to better define the type of games the players' like. Transactional information is also monitored and updated, preferably, by the transactional system **38**. The transactional information includes credit card information, transaction requests, transaction approval, conversion of monetary funds to credits for playing the game, any transfers of credits for playing the game, and conversions from credits to monetary funds that are credited to the player's financial account. Preferably, communications between the transactional system and the broadband gaming system are conducted in a secure environment using cryptographic keys. Although the use of cryptography within the private network may appear excessive one of the greatest security threats within a private network comes from its own employees. Therefore, it is preferable to use internal firewalls for communications between the broadband gaming system, the transactional system and the verification system.

Broadband Gaming System

A more detailed drawing of the broadband gaming system is provided in FIG. **7**. The dashed boundary in FIG. **7** defines the broadband gaming system **36**. After player verification is completed at the verification system **34**, the broadband gaming system **34** is engaged. The broadband gaming system **34** includes a player buffer **84** configured to receive the players who will be playing the game. The player buffer **84** generates an initial player matrix with player data fields **74**.

A countdown timer **82** is coupled to the player buffer **80**. Preferably, the countdown timer **82** is also displayed to the player. The countdown timer **82** provides a window of time within which players may join the game. The players that have joined the game before the end of the timing period are stored in the buffer. When the timing period reaches zero the initial player matrix is communicated to the transactional system **38** and to the gaming module **84**.

The gaming module **84** provides a game that is played by the plurality of players. The game may include a plurality of different games and the type of game is not restrictive to this invention. Preferably, the gaming module **84** includes at least one random number generator **86** and a paytable module **88**.

The random number generator **86** is operatively coupled to the player buffer. The random number generator **86** generates at least one random number that is stored in the player matrix. In one embodiment, at least one random number is generated for the plurality of players playing the game. In an alternative embodiment, at least one random number is generated for each player. In yet another embodiment, a plurality of random numbers are generated that are applied to the plurality of players playing the game. Preferably, the random number generator **86** is a fast hardware module.

A paytable module **88** is operatively coupled to the random number generator **86**. The paytable module **88** is a programmable module that determines the type of prize awarded to the player based on the random number generated by the random number generator **86**. In one embodiment, the paytable module **88** is a field programmable gate array. Preferably, the paytable module **88** also includes an image ID that is associated with the outcome determined by the paytable module **88**.

A gaming output module **90** revises the player matrix to include the outcome for each player. Additionally, the gaming output module **90** groups the players according to the image ID. Based on the results generated by the gaming module **84**, the gaming output module **84** generates a final player matrix that is communicated to the transactional server **38** and to a memory module **92**.

Preferably, the memory module **92** has stored a plurality of images in a fast memory by the time the final player matrix is communicated to the memory module **92**. In operation, the memory module **92** is enabled before the final matrix is communicated to the memory module **92**. By way of example, when the game is engaged the memory module **92** begins the process of finding the applicable images associated with the image IDs in the mini-video server **94** and transferring the images to the fast memory module **92**. Thus, when the gaming output is received by the memory, the images are stored in the fast memory module **92**. In one embodiment, the memory module **92** then broadcasts the images to encoders **96** and **98**. In an alternative embodiment, the memory module **92** is operatively coupled to an intelligent router (not shown) that routes the images to the appropriate encoders **96** and **98**.

The appropriate encoder then receives the images and converts them to a format which meets the requirements for the appropriate network access device. By way of example, an IP encoder **96** encodes a plurality of JPEG images for viewing on a conventional web browser, and an MPEG encoder **98** encodes the plurality of JPEG images into an MPEG stream that is viewed on a television via an interactive set-top box.

An encryption module **100***a* and **100***b* operatively coupled to encoder **96** and **98**, respectively, then receives the encoded images and encrypts the encoded images in manner well known to those skilled in the art. A modulation module **102***a* and **102***b* is operatively coupled to encryption modules **100***a* and **100***b*, respectively, then modulates encrypted encoded images for downstream transmission in a manner well known to those skilled in the art.

Preferably, the broadband gaming system occupies one downstream band, i.e. one 6 or 8 MHz band, in the interactive set-top-box environment. In the web based broadcast environment, the broadband gaming system occupies a downstream channel much like a standard streaming media website.

It shall be appreciated by those skilled in the art having the benefit of this disclosure that the broadband gaming system can play more than one game at a time. The system may be designed to operate in a multi-tasking mode where more than one game is played at a time. Additionally, the system may be designed to operate in a fast serial mode in which a game is played while the countdown timer is waiting for the next queue to be filled.

Transactional System

Referring back to FIG. **2**, there is shown the transactional system **38** which comprises a transactional server **110** and a transactional database **112**. The transactional system **38** performs a plurality of functions including tracking each transaction performed by both the verification system and the broadband gaming system. Additionally, the transactional system **38** is configured to authorize and conduct electronic fund transfers. Furthermore, the transactional system **38** performs such operations as player tracking, managing loyalty programs, engaging bonus games, determining bonus prizes and interfacing with accounting programs.

Method for Registering a Player

Referring to FIG. **8** there is shown a flowchart of the registration method for the gaming system **30**. The registration method **150** begins when a prospective player first accesses a website, channel, kiosk or other such registration terminals as described in block **152**. The method then proceeds to block **153**.

At block **153**, the registration process is initiated. By way of example and not of limitation, a registration terminal may provide a hyperlink to a registration window that prompts the prospective player for information. The method then proceeds to block **154**.

At block **154**, the prospective player provides registration identification information such as name, address, credit card number and other information necessary to create a registration file for the prospective player. The method then proceeds to block **156**.

At block **156**, the prospective player is prompted for a personal ID. The personal ID may be a user ID, a password, a numeric combination, or any other such identification information. The personal ID is used during the verification process to identify a biometric template for the prospective player. The method then proceeds to block **158**.

At block **158**, the prospective player submits a biometric to the registration terminal. By way of example and not of limitation the biometric is a fingerprint. Any other biometric may also be used. The method then proceeds to block **160** or **162**.

At block **160**, the biometric input is compressed and encrypted. It is preferable for certain biometric inputs to be compressed such as fingerprint scans, retinal scans and other such scanning techniques. Other biometric inputs such as voice patterns and signatures do not have to be compressed. The process of encrypting biometric inputs is necessary in an open network environment. The process of encrypting may not be necessary on a private proprietary network. Therefore, it shall be appreciated by those skilled in the art having the benefit of this disclosure that the compression and encryption processes in block **160** may not be necessary for every biometric input.

At block **162**, the prospective player information is stored in the verification system and a player profile is updated accordingly. Alternatively, the prospective player information is stored on a smart card. The method then proceeds to block **164**.

At block **164**, security information about the registration terminal is collected. The registration information identifies the registration terminal as being a secure terminal. The registration terminal provides information such as the MAC ID for the biometric input module, the IP address for the server communicating with the registration terminal, and the cryptographic keys associated with the registration terminal. The registration terminal includes the network access devices described in FIG. **1***a* through FIG. **1***d* as well as kiosks and other such registration terminals.

At block **166**, the prospective player is identified as a registered player and the registration database **40** is updated accordingly. The registration process is broken out into separate components for security purposes. Once a validly registered player is identified by the verification system, the registration process is completed.

Method for Player Verification

Referring to FIG. **9** there is shown a method **170** for player verification used by the verification system **34**. The player verification process includes receiving user identification information from a network access device. The method is initiated at block **174** when a user accesses a website or channel displaying the game. The method then proceeds to block **176**.

At block **176**, the personal ID is provided by the user. The personal ID is used by the verification system to find a biometric template for determining whether the user is a registered player. The method then proceeds to block **178**.

At block **178**, the biometric input module of the network access device receives a biometric from the user. As previously described the biometric input module can be one of plurality of biometric inputs. Depending on the type of biometric, the biometric may be compressed as described by block **180** and encrypted as described by block **182**. At block **184**, the biometric and the personal ID is then communicated through a network **32** to the verification system **34**. Alternatively, the biometric and Personal ID is communicated to a smart card for verification.

At block **186**, the verification system **34** requests security information from the network access devices. The security information identifies the network access devices as being a valid network access device. The method then proceeds to block **188**.

At block **188**, the verification system **34** processes the security information to ensure that the security information is generated by the appropriate network access device, and to ensure that the security information has not been compromised. Preferably, the verification system **34** performs a stateful multilayer inspection as described above. The method then proceeds to block **190**.

At block **190**, the user submitted player information is compared to the registered player information. If a determination is made at decision diamond **192** that the submitted player information is not a valid registered player the method proceeds to block **194**. At block **194**, the user is requested to re-input the biometric. If the biometric is input more than three times, as provided by decision diamond **196**, the user is requested to contact customer service.

If a match is found at decision diamond **192** between the user submitted information and the registered player information, the user is identified as a valid player then the player proceeds to the broadband gaming system **36**.

Method for Operation of Broadband Gaming System

Referring to FIG. **10** and FIG. **11** there is shown a flowchart **200** of the information processed by the broadband gaming system **34**. The process is engaged by performing the verification process in which the verification system identifies a player as in block **201**. After the verification process has been completed the method proceeds to block **202**.

At block **202**, the players who desire to play a particular game are stored in a buffer until the particular game is engaged. The method then proceeds to decision diamond **204**.

At decision diamond **204**, the countdown timer **82** determines if the period during which the game is open has been closed. If the game remains open, additional players may be received by the broadband gaming system. If the game is

closed because the period during which the game is open has expired, then the method proceeds to block **206**.

At block **206**, the initial player matrix described above is generated. The initial player matrix includes information about the player, the type of game, and other such information about the game as described by the player data fields **74** shown in FIG. **6**. The initial player matrix is then communicated to block **208** which transmits the initial player matrix to the transactional system for validation. Additionally, the initial player matrix is communicated to the next block **210** in the broadband gaming system which starts the gaming module.

At block **210**, the initial player matrix is received by the gaming module **84** and the gaming module **84** is engaged. At a minimum the gaming module **84** comprises a random number generator **86** and a paytable module **88**. The random number generator generates at least one random number that is used during the game. The paytable module **88** is used to determine the prize associated with the at least one random number.

Referring to FIG. **11**, a continuation of the broadband gaming system method is shown. By way of example, the gaming module may comprise a plurality of different random number generators. The blocks **214** and **216** describe the processes performed by a random number generator and a paytable module, respectively. The random number generator **86** of block **214** determines the winning combination of numbers for the game. At block **216**, the paytable module **88** is used to determine the prize awarded to the player. Preferably, the paytable module **88** is also configured to provide image IDs that identify the images associated with the prize. Preferably, the paytable module **88** is resident in both the broadband gaming system and the transactional system. The purpose for this redundancy is as a security check for output generated by the gaming module. The method then proceeds to block **218**.

At block **218** the player outputs with the same image IDs are grouped together. The grouping process is performed to simplify the broadcasting of the images to the plurality of players. By grouping the players according to the same image ID and having identified the network access device used by the player, a dynamic broadcasting method is created which occupies minimal downstream bandwidth. The method then proceeds to block **220**.

At block **220** a final player matrix is completed. The final player matrix includes the same data fields as the initial player matrix. Additionally, the final player matrix includes the random number output and the paytable output. The final player matrix is then communicated to the transactional system as described in block **222**. The method then proceeds to decision diamond **224**.

At decision diamond **224**, a validation procedure is conducted. The validation procedure essentially compares the transactional system's reverse calculation of the random numbers with the random numbers generated by the gaming module. If the random numbers in the transactional system are not the same or similar to the random numbers generated by the random number generator, a system failure or security breach is detected. If a security breach or system failure is detected, the method then proceeds to process block **226**, which initiates diagnostic procedures. If the random numbers match, then the method proceeds to block **228**.

At block **228**, the plurality of images is broadcast. The images are preferably broadcast along one downstream channel for each network access device. However, traffic considerations may require the use of a plurality of downstream channels. By way of example, for DOCSIS and DSL type downstream transmissions, the streaming video preferably occupies a portion of the bandwidth available for a cable modem or DSL modem, respectively. In an alternative example, for an interactive set-top box environment, the downstream channel preferably occupies one 6 MHz or 8 MHz band or a portion of the 6 MHz or 8 MHz band. The method then proceeds to the next block **230**.

At block **230**, the broadcast images are encoded for downstream transmission. It shall be appreciated by those skilled in the art having the benefit of this disclosure that downstream transmission systems are well known and can be easily integrated into the systems and method described in this patent. The method then proceeds to block **232**.

At block **232**, the broadcast images are encrypted for downstream transmission. The purpose for downstream encryption is to prevent unauthorized access to the downstream signal. It shall be appreciated by those skilled in the art that various secure systems and methods for downstream transmission of images are well known.

It shall be appreciated by those skilled in the art having the benefit of this disclosure that a plurality of games may be played simultaneously. The games may be played in a distributed/parallel manner or in serial manner.

An Illustrative Game

An illustrative game is described to show how the system and method described above operates. The illustrative game described herein is a progressive slot machine. It is well-known that in the United States many states have legalized lottery games even though other games of chance such as progressive slot machines have not been legalized. It is also well-known that in casino gaming floors the most popular games are progressive slot machines. The present illustrative game operates on the system and method described above and provides an output similar to a progressive slot machine with a lottery type input.

The illustrative game includes first having a player provide a plurality of letters or numbers that are either generated by the player or are selected in a random manner. The random number generator of the gaming module is then engaged and a gaming module random number is generated. Preferably, the order that the random numbers were generated is used to determine the prize awarded to the player. A programmed paytable is then used to compare the player selected numbers to the gaming module random numbers according to the rules programmed into the paytable module. Based on the results of this comparison a prize is awarded to the player. An image ID is associated with the prize awarded. The plurality of players are then grouped according to their respective image IDs. A broadcast stream for the plurality of images associated with each image ID is broadcast to each player.

A more concrete example includes having a player select a plurality of numbers, such as the numbers below:

25	35	8	15	42

The random number generator of the gaming module is then engaged. By way of example the random number results are:

56	2	3	8	42

The paytable module is then programmed to interpret the random numbers generated by the gaming module according to the following illustrative rules:

1. If a match between one number is achieved, then a prize of I× the initial bet credit is awarded and an image ID X023-1396 is used. Image ID X023-1396 is an animated plurality of images representing three cherries.

2. If a match between one number at the same location is achieved, then a prize of 2× the initial bet credit is awarded and an image ID X023-1397 is used. Image ID X023-1397 is an animated plurality of images representing four cherries.

3. If a match between a first number is achieved and a match between a second number is achieved, then a prize of 5× the initial credit is awarded and an image ID X023-1998 is used. Image ID X023-1998 is an animated plurality of images representing 3 oranges.

4. If a match between a first number at the same location is achieved and a match between a second number is achieved, than a prize of 7× the initial credit is awarded and an image ID X023-1999 is used. Image ID X023-1999 is an animated plurality of images representing 4 oranges.

Thus, for the illustrative example provided above, the player having selected the numbers: 23, 35, 8, 15 and 42 is entitled to a prize of 7× the initial credit for a random number: 56, 2, 3, 8, and 42. The associated images displayed on the network access device is an animated plurality of images representing 4 oranges.

The scope of the invention should be determined by the appended claims and their legal equivalents rather than by the examples given.

What is claimed is:

1. A gaming system network, comprising:

a verification system configured to verify that a user attempting to access the gaming system network is a registered player, the user operating a network access device communicating with the gaming system network;

a gaming system configured to generate at least one random game output, the gaming system configured to associate an image ID with the at least one random game output;

a video server configured to store a plurality of images corresponding to at least one game, the video server configured to retrieve one or more images associated with the image ID, wherein the one or more images are representative of a game output, the video server configured to communicate the one or more images to the network access device; and

a transactional system configured to credit monetary funds to a financial account of the user based on the at least one random game output.

2. The gaming system network of claim **1**, wherein the one or more images communicated to the network access device are viewable on a web browser.

3. The gaming system network of claim **1**, wherein the one or more images communicated to the network access device are encrypted.

4. The gaming system network of claim **1**, wherein the transactional system is further configured to track each transaction performed by the gaming system.

5. The gaming system network of claim **1**, wherein the network access device is a gaming terminal.

6. The gaming system network of claim **1**, wherein the network access device is a wireless device.

7. The gaming system network of claim **1**, wherein the network access device is a display operatively coupled to an interactive set-top box.

8. The gaming system network of claim **1**, wherein the gaming system is further configured to allow a first game type to be played on a first network access device and a second game type to be simultaneously played on a second network access device.

9. A gaming system network, comprising:

a verification system configured to verify that a user attempting to access the gaming system network is a registered player, the user operating a network access device communicating with the gaming system network;

a means for generating at least one random game output and associating an image ID with the at least one random game output;

a video server configured to store a plurality of images corresponding to at least one game, the video server configured to retrieve one or more images associated with the image ID, wherein the one or more images are representative of a game output, the video server configured to communicate the one or more images to the network access device; and

a transactional system configure to credit monetary funds to a financial account of the user based on the at least one random game output.

10. The gaming system network of claim **9**, wherein the one or more images communicated to the network access device are viewable on a web browser.

11. The gaming system network of claim **9**, wherein the one or more images communicated to the network access device are encrypted.

12. The gaming system network of claim **9**, wherein the network access device is a gaming terminal.

13. The gaming system network of claim **9**, wherein the network access device is a wireless device.

14. The gaming system network of claim **9**, wherein the network access device is a display operatively coupled to an interactive set-top box.

15. The gaming system network of claim **9**, wherein the means for generating the at least one random game output include means for allowing a first game type to be played on a first network access device and a second game type to be simultaneously played on a second network access device.

16. A gaming method, comprising the steps of:

verifying that a user operating a network access device is a registered player, the network access device communicating with a gaming system network;

generating at least one random game output with a gaming system;

associating an image ID with the at least one random game output;

retrieving one or more images associated with the image ID;

communicating the one or more images to the network access device; and

crediting monetary funds to a financial account of the user based on the at least one random game output.

17. The method of claim **16**, wherein the one or more images are viewable on a web browser.

18. The method of claim **16**, further comprising the step of encrypting the one or more images prior to communicating the one or more images to the network access device.

19. The method of claim **16**, wherein the network access device includes a gaming terminal, a wireless device, and a display operatively coupled to an interactive set-top box.

20. The method of claim **16**, further comprising the step of tracking each transaction performed by the gaming system.

21. The method of claim **16**, further comprising the step of enabling a first game type to be played on a first network access device and a second game type to be simultaneously played on a second network access device.

* * * * *

US009373116B1

(12) **United States Patent**
Kerr

(10) **Patent No.: US 9,373,116 B1**
(45) **Date of Patent: Jun. 21, 2016**

(54) **PLAYER TRACKING USING A WIRELESS DEVICE FOR A CASINO PROPERTY**

(75) Inventor: **Michael A. Kerr**, Carson City, NV (US)

(73) Assignee: **NexRF Corporation**, Reno, NV (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1329 days.

(21) Appl. No.: **11/948,007**

(22) Filed: **Nov. 30, 2007**

Related U.S. Application Data

(63) Continuation-in-part of application No. 10/681,034, filed on Oct. 8, 2003, now Pat. No. 8,403,755, which is a continuation of application No. 09/899,559, filed on Jul. 5, 2001, now abandoned.

(60) Provisional application No. 60/872,351, filed on Nov. 30, 2006, provisional application No. 60/266,956, filed on Feb. 6, 2011.

(51) **Int. Cl.**
G06Q 30/00 (2012.01)

(52) **U.S. Cl.**
CPC ***G06Q 30/00*** (2013.01)

(58) **Field of Classification Search**
USPC 463/10, 29, 40, 42
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,339,798	A	7/1982	Hedges et al.	
4,856,787	A	8/1989	Itkis	
5,586,937	A	12/1996	Menashe	
5,594,491	A	1/1997	Hodge et al.	
5,630,757	A	5/1997	Gagin et al.	
5,643,086	A	7/1997	Alcorn et al.	
5,738,583	A *	4/1998	Comas et al.	463/40
5,761,416	A	6/1998	Mandal et al.	
5,761,647	A *	6/1998	Boushy	705/10
5,762,552	A	6/1998	Vuong et al.	
5,768,382	A	6/1998	Schneier et al.	
5,779,545	A *	7/1998	Berg et al.	463/22
5,795,228	A	8/1998	Trumbull et al.	
5,800,268	A	9/1998	Molnick	
5,851,149	A	12/1998	Xidos et al.	

(Continued)

FOREIGN PATENT DOCUMENTS

WO	2008065257	A1	6/2008

OTHER PUBLICATIONS

"Internet Industry Interacting Gambling Code: A Code for Industry Co-Regulation in the Area of Internet Gambling Content Pursuant to the Requirements of the Interactive Gambling Act 2001." Internet Industry Association. Dec. 2001.

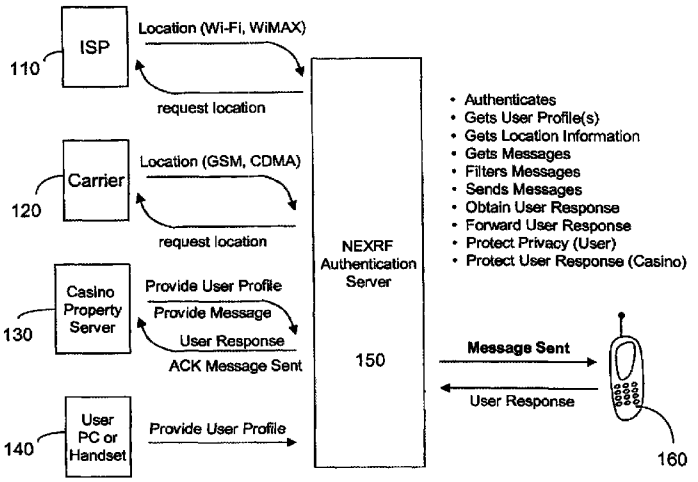
(Continued)

Primary Examiner — Paul A D'Agostino
Assistant Examiner — Brandon Gray
(74) *Attorney, Agent, or Firm* — Michael A. Kerr; Kerr IP Group, LLC

(57) **ABSTRACT**

A method for tracking patronage of a customer in at least one casino property is described. The method comprises monitoring a wireless handset that determines the location of the customer. The method then proceeds to generate a user profile that comprises user preferences and monitored betting activity associated with the customer and accumulated points stored in a customer account according to a monetary value of the monitored betting activity. Complementary goods or services are determined based on the accumulated points associated with the customer account. A message is sent to the wireless handset associated with the complementary goods or services that is consistent with the user preferences.

20 Claims, 2 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

5,871,398	A	2/1999	Schneier et al.	
5,902,983	A	5/1999	Crevelt et al.	
5,947,821	A	9/1999	Stone	
5,970,143	A	10/1999	Schneier et al.	
5,971,849	A	10/1999	Falciglia	
6,001,016	A	12/1999	Walker et al.	
6,010,404	A	1/2000	Walker et al.	
6,106,396	A	8/2000	Alcorn et al.	
6,142,876	A	11/2000	Cumbers	
6,159,095	A	12/2000	Frohm et al.	
6,178,510	B1	1/2001	O'Connor et al.	
6,203,428	B1	3/2001	Giobbi et al.	
6,217,447	B1	4/2001	Lofink et al.	
6,220,961	B1	4/2001	Keane et al.	
6,259,405	B1	7/2001	Stewart et al.	
6,322,446	B1	11/2001	Yacenda	
6,327,535	B1	12/2001	Evans et al.	
6,409,602	B1	6/2002	Wiltshire et al.	
6,500,068	B2	12/2002	Walker et al.	
6,508,709	B1	1/2003	Karmarkar	
6,508,710	B1	1/2003	Paravia et al.	
6,527,638	B1	3/2003	Walker et al.	
6,554,705	B1	4/2003	Cumbers	
6,575,834	B1	6/2003	Lindo	
6,612,928	B1 *	9/2003	Bradford et al.	463/29
6,628,939	B2	9/2003	Paulsen	
6,638,170	B1	10/2003	Crumby	
6,640,218	B1	10/2003	Golding et al.	
6,676,522	B2	1/2004	Rowe	
6,682,421	B1	1/2004	Rowe et al.	
6,702,672	B1	3/2004	Angell et al.	
6,709,333	B1	3/2004	Bradford et al.	
6,709,631	B2	3/2004	Mori et al.	
6,719,631	B1	4/2004	Tulley et al.	
6,749,512	B2	6/2004	MacGregor et al.	
6,782,253	B1	8/2004	Shteyn et al.	
6,834,195	B2	12/2004	Brandenberg et al.	
6,875,110	B1	4/2005	Crumby	
6,879,838	B2	4/2005	Rankin et al.	
6,884,162	B2	4/2005	Raverdy et al.	
6,942,574	B1	9/2005	LeMay et al.	
7,035,651	B2	4/2006	Schreiner et al.	
7,076,243	B2	7/2006	Parupudi et al.	
7,107,245	B1	9/2006	Kowalick	
7,136,915	B2	11/2006	Rieger, III	
7,196,662	B2	3/2007	Misikangas et al.	
7,209,752	B2	4/2007	Myllymaki et al.	
7,218,941	B1	5/2007	Kubo et al.	
7,228,136	B2	6/2007	Myllymaki et al.	
7,299,059	B2	11/2007	Misikangas et al.	
7,338,372	B2	3/2008	Morrow et al.	
7,341,522	B2	3/2008	Yamagishi	
7,349,683	B2	3/2008	Misikangas	
7,359,714	B2	4/2008	Parupudi et al.	
7,397,424	B2	7/2008	Houri	
7,450,954	B2	11/2008	Randall	
7,493,565	B2	2/2009	Parupudi et al.	
7,529,639	B2	5/2009	Kikta et al.	
7,534,169	B2	5/2009	Amaitis et al.	
7,611,407	B1	11/2009	Itkis et al.	
7,753,772	B1	7/2010	Walker et al.	
8,002,617	B1	8/2011	Uskela et al.	
8,029,349	B2	10/2011	Lind	
2001/0004768	A1	6/2001	Hodge et al.	
2001/0005908	A1	6/2001	Hodge et al.	
2001/0031654	A1	10/2001	Walker et al.	
2001/0031656	A1	10/2001	Marshall et al.	
2001/0036224	A1	11/2001	Demello et al.	
2001/0039210	A1	11/2001	ST-Denis	
2001/0044337	A1 *	11/2001	Rowe et al.	463/29
2002/0002073	A1	1/2002	Montgomery et al.	
2002/0007494	A1	1/2002	Hodge	
2002/0056125	A1	5/2002	Hodge et al.	
2002/0056143	A1	5/2002	Hodge et al.	
2002/0061778	A1	5/2002	Acres	
2002/0069105	A1	6/2002	Botelho et al.	
2002/0077130	A1	6/2002	Owensby	
2002/0077167	A1	6/2002	Merari	
2002/0091568	A1	7/2002	Kraft et al.	
2002/0103028	A1	8/2002	Carter et al.	
2002/0111210	A1	8/2002	Luciano et al.	
2002/0111907	A1 *	8/2002	Ling	705/41
2002/0133707	A1	9/2002	Newcombe	
2002/0142815	A1	10/2002	Candelore	
2002/0142844	A1	10/2002	Kerr	
2002/0142846	A1 *	10/2002	Paulsen	463/43
2002/0144151	A1	10/2002	Shell et al.	
2002/0174436	A1	11/2002	Wu et al.	
2002/0198775	A1	12/2002	Ryan	
2003/0009385	A1	1/2003	Tucciarone et al.	
2003/0030666	A1	2/2003	Najmi et al.	
2003/0032409	A1	2/2003	Hutcheson et al.	
2003/0064805	A1	4/2003	Wells	
2003/0119578	A1	6/2003	Newson	
2003/0144017	A1	7/2003	Inselberg	
2004/0023721	A1	2/2004	Giobbi	
2004/0192438	A1	9/2004	Wells et al.	
2004/0224757	A1	11/2004	Yamamura et al.	
2005/0046608	A1	3/2005	Schantz et al.	
2005/0048990	A1	3/2005	Lauriol	
2005/0085257	A1	4/2005	Laird et al.	
2005/0114212	A1	5/2005	Carrez et al.	
2005/0136949	A1	6/2005	Barnes	
2005/0154646	A1	7/2005	Chermesino	
2005/0159883	A1	7/2005	Humphries et al.	
2005/0181804	A1	8/2005	Misikangas et al.	
2005/0246334	A1	11/2005	Tao et al.	
2005/0261063	A1	11/2005	Boyd et al.	
2006/0003830	A1	1/2006	Walker et al.	
2006/0004627	A1	1/2006	Baluja	
2006/0058102	A1	3/2006	Nguyen et al.	
2006/0063575	A1	3/2006	Gatto et al.	
2006/0125693	A1	6/2006	Recker	
2006/0181411	A1	8/2006	Fast et al.	
2006/0189382	A1 *	8/2006	Muir et al.	463/29
2006/0194633	A1	8/2006	Paulsen	
2006/0238382	A1	10/2006	Kimchi et al.	
2006/0240891	A1	10/2006	Klinkhammer et al.	
2006/0287810	A1	12/2006	Sadri et al.	
2007/0024580	A1	2/2007	Sands et al.	
2007/0025265	A1	2/2007	Porras et al.	
2007/0060306	A1	3/2007	Amaitis et al.	
2007/0061229	A1	3/2007	Ramer et al.	
2007/0087834	A1	4/2007	Moser et al.	
2007/0100963	A1	5/2007	Ban et al.	
2007/0136132	A1	6/2007	Weiser et al.	
2007/0149215	A1	6/2007	Misikangas	
2007/0149216	A1	6/2007	Misikangas	
2007/0167210	A1 *	7/2007	Kelly et al.	463/16
2007/0168127	A1	7/2007	Zaruba et al.	
2007/0184852	A1	8/2007	Johnson et al.	
2007/0218975	A1	9/2007	Iddings et al.	
2007/0243925	A1	10/2007	LeMay et al.	
2007/0244633	A1	10/2007	Phillips et al.	
2007/0257831	A1	11/2007	Mathews et al.	
2007/0270212	A1	11/2007	Cockerille et al.	
2007/0281692	A1	12/2007	Bucher et al.	
2008/0026844	A1	1/2008	Wells	
2008/0032705	A1	2/2008	Patel et al.	
2008/0039192	A1	2/2008	Laut	
2008/0057894	A1	3/2008	Aleksic et al.	
2008/0085692	A1	4/2008	Hart et al.	
2008/0096659	A1 *	4/2008	Kreloff et al.	463/39
2008/0097858	A1	4/2008	Vucina et al.	
2008/0102947	A1	5/2008	Hays et al.	
2008/0108430	A1	5/2008	Evans	
2008/0162037	A1	7/2008	Mahmoud	
2008/0166973	A1	7/2008	Hart et al.	
2008/0186234	A1	8/2008	Alles et al.	
2008/0189360	A1	8/2008	Kiley et al.	
2008/0227473	A1	9/2008	Haney	
2010/0022308	A1 *	1/2010	Hartmann et al.	463/42
2010/0027521	A1	2/2010	Huber et al.	
2010/0039929	A1	2/2010	Cho et al.	

(56) **References Cited**

U.S. PATENT DOCUMENTS

2010/0121567	A1	5/2010	Mendelson
2010/0167771	A1	7/2010	Raghothaman et al.
2010/0305855	A1	12/2010	Dutton et al.
2010/0331016	A1	12/2010	Dutton et al.
2011/0103360	A1	5/2011	Ku et al.
2012/0115512	A1	5/2012	Grainger et al.
2012/0122476	A1	5/2012	Lee et al.
2013/0003572	A1	1/2013	Kim et al.

OTHER PUBLICATIONS

"Wireless Network." Wikipedia. http://en.wikipedia.org/wiki/Wireless_network. Nov. 17, 2008.
"Tracking Cookie." Wikipedia. http://en.wikipedia.org/wiki/Tracking_cookie. May 24, 2009.
"Ekahau Positioning Engine 4.2." 2008. http://www.nowire.se/images/produktblad/ekahau/datasheetsub.--epesub.---42.sub.--en.sub.--11022008.sub.--lo.pdf. Sep. 29, 2008.
"Location in SIP/LP Core Architecture." Open Mobile Alliance. Sep. 4, 2008. Accessed Dec. 2008. http://www.openmobilealliance.org/technical/release.sub.--program/locsip.- sub.--archive.aspx.
"The New Normal of Retailing: The Rise of the Mobile Shopper." Next Generation Retail Summit. 2010. http://www.ngrsummit.com/media/whitepapers/Microsoft.sub.--NGRUS.pdf.
"Tracking Cookie," Wikipedia. http://en.wikipedia.org/wiki/Tracking.sub.--cookie. May 24, 2009.
"Wireless Network." Wikipedia. http://en.wikipedia.org/wiki/Wireless.sub.--network. Nov. 17, 2008.
Vegni et al. "Local Positioning Services on IEEE 802.11 Networks," Radio Engineering, pp. 42-47, vol. 17, No. 2, Jun . 2008.
Wirelss Network. Wikipedia. http://en.wikipedia.org/wiki/Wireless.sub.--network. Nov. 17, 2008.
Lafargue, Edouard. "Wireless Network Audits using Open Source Tools". SANS Institute 2003. Accessed Dec. 2008. http://www.sans.org/reading.sub.--room/whitepapers/auditing/wireless-netw- ork-audits-open-source-tools.sub.--1235.

* cited by examiner

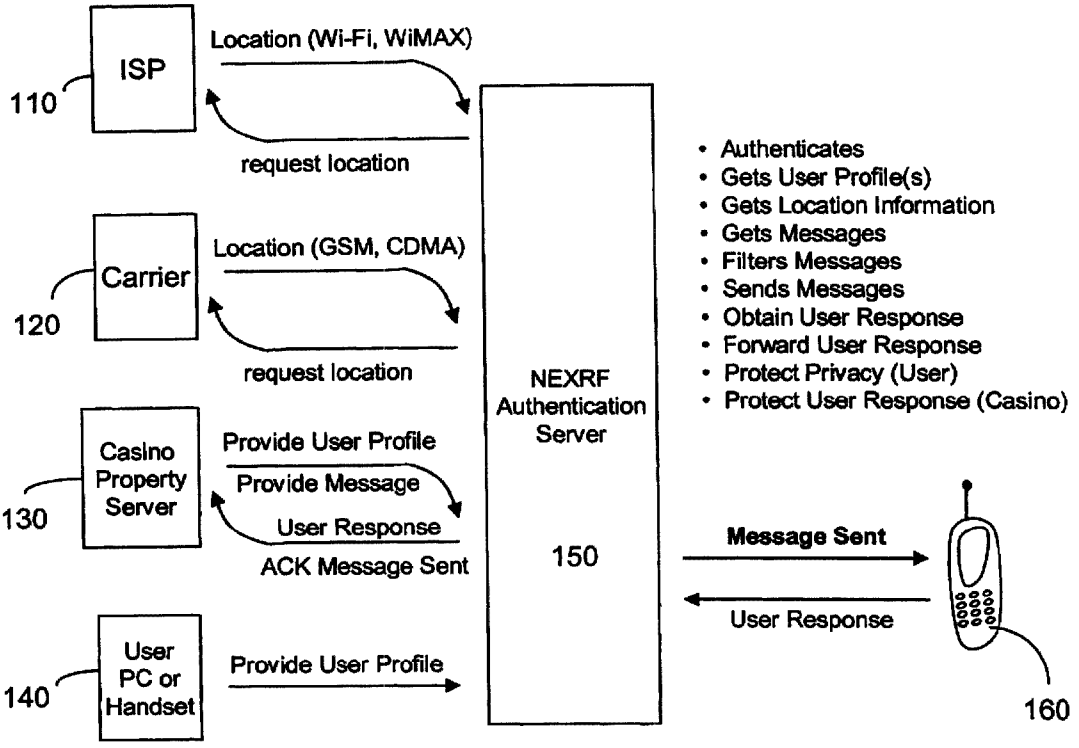

ISP
110
Location (Wi-Fi, WiMAX)
request location
Carrier
120
Location (GSM, CDMA)
request location
Casino Property Server
130
Provide User Profile
Provide Message
User Response
ACK Message Sent
User PC or Handset
140
Provide User Profile
NEXRF Authentication Server
150
• Authenticates
• Gets User Profile(s)
• Gets Location Information
• Gets Messages
• Filters Messages
• Sends Messages
• Obtain User Response
• Forward User Response
• Protect Privacy (User)
• Protect User Response (Casino)
Message Sent
User Response
160

Figure 1

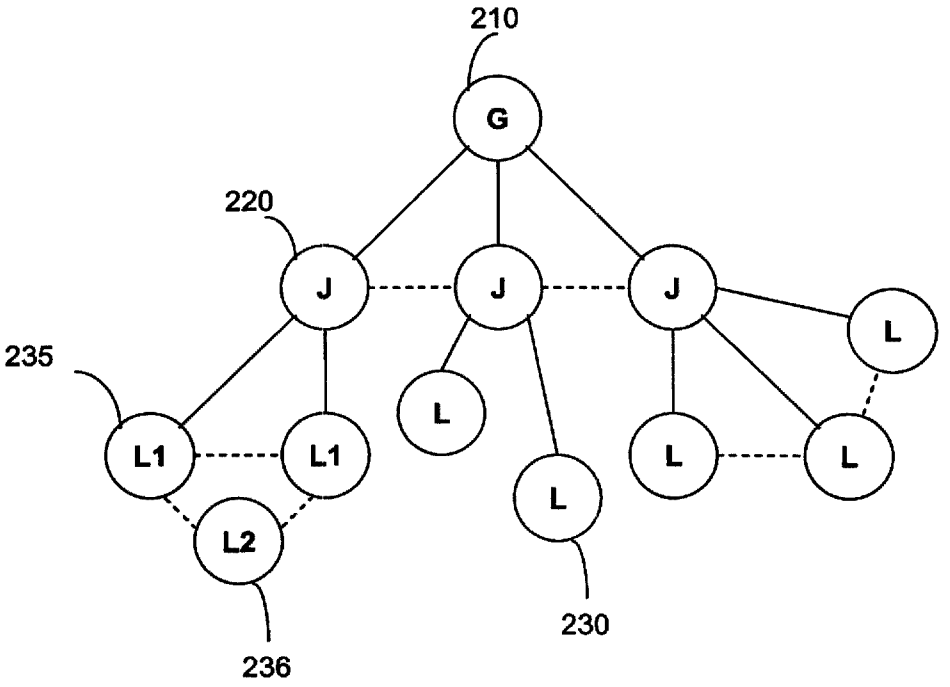


Figure 2

PLAYER TRACKING USING A WIRELESS DEVICE FOR A CASINO PROPERTY

CROSS REFERENCE

This patent application is related to provisional patent application 60/872,351 filed on Nov. 30, 2006, and is a continuation-in-part of patent application Ser. No. 10/681,034 filed on Oct. 8, 2003, which is a continuation of patent application Ser. No. 09/899,559 having a filed date of Jul. 5, 2001, that is related to provisional patent application 60/266,956 filed on Feb. 6, 2001, all of which are hereby incorporated by reference.

FIELD OF THE INVENTION

This invention relates to player tracking using a wireless communication device for a casino property. More particularly, the invention relates to sending messages to wireless devices based on user preferences, location, and player tracking information.

BACKGROUND

Generally, present day player tracking systems rely on the use of mag stripe cards. Currently, wireless devices are being promoted that perform various player tracking functions. However, these wireless devices are generally limited to being used exclusively on the casino floor for wireless gaming. These wireless devices are not enabled to take advantage of the player's mobility in the casino megaplex or similar large entertainment property.

SUMMARY

A method for tracking patronage of a customer in at least one casino property is described. The method comprises monitoring a wireless handset configured to determine the location of the customer. The wireless handset is configured to communicate with a network using at least one wireless networking protocol. The method then proceeds to generate a user profile associated with the customer that includes user preferences. The user profile also comprises monitored betting activity associated with the customer and accumulated points stored in a customer account according to a monetary value of the monitored betting activity. Complementary goods or services are determined based on the accumulated points associated with the customer account. A message is sent to the wireless handset associated with the complementary goods or services that are consistent with the user profile.

A system for tracking customer activity at a casino property using customer accounts is also described. The system comprises a wireless handset associated with the customer and is configured to determine the location of the customer. The wireless handset is configured to communicate with a network using at least one wireless networking protocol. The system also comprises at least one computer system associated with at least one casino property that monitors the betting activity of the customer. The computer system is configured to generate a user profile that comprises user preferences and tracks accumulated points in a customer account according to the monetary value of the monitored betting activity and determine complimentary goods or services to be provided to the customer based on the accumulated points associated with the customer account and the user profile. Additionally, the system comprises a means for generating a message that is sent to the wireless handset regarding the complementary goods or services that is consistent with the user profile.

A method for communicating a particular message to a wireless handset is also described. The method comprises providing at least one computer system associated with a casino property configured to store a plurality of messages. The computer system is configured to wirelessly communicate at least one message within a geographical area. The method also comprises providing a wireless handset that is configured to receive messages from the at least one computer system associated with the casino property. The method then proceeds to determine an approximate location for the wireless handset. At least one message is transmitted from the computer associated with the casino property to the wireless handset based on the location of the wireless handset. The message is displayed on the wireless handset. A reply generated by the wireless handset is received by the casino computer system.

DRAWINGS

The present invention will be more fully understood by reference to the following drawings which are for illustrative, not limiting, purposes.

FIG. **1** shows an illustrative client-server system for player tracking using a wireless communication device.

FIG. **2** shows an illustrative peer-to-peer system for player tracking using a wireless communication device.

DETAILED DESCRIPTION

Persons of ordinary skill in the art will realize that the following description is illustrative and not in any way limiting. Other embodiments of the claimed subject matter will readily suggest themselves to such skilled persons having the benefit of this disclosure. It shall be appreciated by those of ordinary skill in the art that the systems and apparatus described hereinafter may vary as to configuration and as to details. Additionally, the method may vary as to details, order of the actions, or other variations without departing from the illustrative method disclosed herein.

The conversion of a wireless communication device such as a mobile handset to a software valet that is at the beck and call of the user is described. Note, the terms wireless communication device and mobile handset are used interchangeably. Ideally, the solution is hardware agnostic, so the wireless communication device may be a mobile phone, a mobile Wi-Fi handset, or a WiMAX handset. The goal is to provide an integrated platform that supports the personalization of data flow for a wireless communication device. The illustrative application is targeted messaging as a function of the user profile, user location, and time. The user profile includes a plurality of user preferences such as dining preferences, entertainment preferences, drink preferences, and other such personalized preferences.

The solution supports target advertisements, personalization, and permits a handset to "close the transactional loop" where the mobile handset becomes a Point-of-Sale (POS) device.

The mobile handset which performs the operations described above may be used to support mobile gaming transactions within a casino environment, support secure lottery based transactions, or similar gaming related activities. Thus, the mobile handset can also be converted into a secure gaming device, and the description provided in the patent application entitled BIOMETRIC BROADBAND GAMING SYSTEM AND METHOD filed in 2001 by the same named inventor,

which is hereby incorporated by reference to describe a networked server based gaming system.

The wireless communication device may be a mobile handset, mobile phone, wireless phone, portable cell phone, cellular phone, portable phone, a personal digital assistant (PDA), or any type of mobile terminal which is regularly carried by a user and has all the elements necessary for operation in a wireless communication system. The wireless communications include, by way of example and not of limitation, CDMA, WCDMA, GSM or UMTS or any other wireless communication system such as wireless local area network, WLAN, Wi-Fi or WiMAX. It shall be appreciated by those of ordinary skill in the art that the term wireless communication device, mobile handset, wireless phone, and mobile phone are interchangeable.

The wireless communication device is in communication with an antenna. The antenna may be one of a plurality of base station antennas associated with a cellular phone network, or an antenna associated with wireless local area network access point, and may use Wi-Fi or WiMAX, or other such networking protocols.

The goal of a casino property is to keep players on the property, keep players busy gambling, and get players back on the property. The illustrative service offering is integrated into a wireless communication device that may be provided as a complimentary service to the player. The wireless communication device provides the well-known service offerings of a cell phone. Additionally, the wireless communication device is programmed to receive a variety of messages with user-specific information, such as preferred gaming experience, food preferences, and other specific offerings associated with the individual. Thus, if the prospective player is off the casino property, a targeted desirable message is sent, e.g. "Limo is waiting with front row tickets for Van Morrison. Respond if you want to see show." If the user responds with a "yes," a ticket or other means for authorizing entry to the show is sent to the handset.

Note that the player or player tracking solution can also be used to support wireless gaming such as a sports book, horse racing, bingo, slots, and even table games.

The cross-over applications for the illustrative solution are established by using the illustrative solution to communicate targeted advertising or messages and to facilitate transactions, such as gift card transactions, loyalty transactions, coupon based transactions and similar small transactions, i.e. transactions less than $10. The user profile is used to filter messages and to perform mobile commerce transactions. The location information can be used to detect and prevent fraud, and the transactional size minimizes the impact of fraud.

In the illustrative embodiment, a targeted message is sent to a user, and then a transaction may be facilitated with the message or advertisement. Preferably, the user profile remains secure and in control of the user. The user profile filters information on behalf of the user, so that only desirable content is received. The advertisements are managed and controlled so that they conform to local laws.

For utility and/or process engineering applications, one sample application is securely sending automated messages that are triggered by sensor outputs and location, e.g. wireless telemetry to an affordable wireless communication device. For example, in certain high risk working environments such as nuclear power plants, oil well platforms, or oil refineries, there is a need to provide individuals with real-time alarm data that is location specific. This illustrative solution supports sending these targeted messages as a function of location, time and sensor input to an affordable handset leveraging an existing wireless network infrastructure.

Another industrial application includes regulatory applications such as environmental monitoring. With the described solution all that is needed is a wireless communication device or PC card that is in communication with a sensor network. Data can be securely accessed from any networked device. User profiles can be created that filter content, so a first set of information is available to the regulatory agency, a second set of information is available to off-site personnel or consultants and a third set of information is available to on-site personnel handling day-to-day activities.

Finally, the illustrative solution can support a military application that prevents "friendly fire" casualties because messages can be sent on a real-time basis as function of the user location, regardless of the type of wireless network. The illustrative solution resides on an affordable wireless communication device that securely identifies location, and can be used to validate that a particular user is NOT an enemy combatant.

In a first illustrative embodiment, the solution is embodied in a client-server architecture as described in FIG. **1**. The client-server system model is scalable, and supports multiple clients and servers.

In FIG. **1**, the location information is collected from an ISP **110** and/or a Carrier **120**. The collection of location information is feasible if authorized by the user. If for instance the "user" is a casino property that is loaning the wireless communication device **160** to a casino guest, then the casino property may elect to have the location information for the wireless communication device **160** available to an authorized entity such as the intermediary server **150**. In an alternative embodiment, where the owner of the handset **160** is the casino guest, the casino guest opts-in to provide location information to the intermediary server **150** based on the user profile submitted by the casino guest and downloads the software program that mirrors the operations performed by the casino property's wireless communication device.

The illustrative ISP **110** provides wireless connectivity using one of a plurality of networking standards such as Wi-Fi or WiMAX. The ISP **110** is configured to identify the location of the wireless communication device **160** using well known location based techniques such as triangulation, GPS, and other such methods. The illustrative Carrier **120** that provides wireless services must comply with the E911 regulations and also generates location information. This location information is served by the ISP **110** or Carrier **120** to the intermediary server **150**.

A variety of different user profiles may be collected from different sources. For simplicity, a first user profile is collected from a casino property, and a second user profile is collected directly from the user. In the casino generated user profile, the casino may indicate user preferences such as cocktail preferences and dining preferences. The casino user profile may comprise monitored betting activity associated with the player and accumulated points stored in a player account according to a monetary value of the monitored betting activity. Complementary goods or services are determined based on the accumulated points associated with the player account, and a message may be sent to the wireless communication device **160** associated with the complementary goods or services that are consistent with the user profile. The casino user profile can also be used as a basis to provide mobile concierge services.

The second user profile may be generated separately by a player using a personal computer (PC) **140** and may indicate the user's "comp" preferences where the player may prefer to obtain tickets to a particular Vegas show and to opt-out of receiving comps for a particular dining establishment.

The intermediary server **150** authenticates information that is received from each source. The intermediary server **150** gathers the user profile information including user preferences and obtains the location information. Additionally, the intermediary server **150** receives the messages, which are to be sent to the user as a function of the user profile, location, and time. The illustrative messages are generated by the illustrative casino property; however, the content may be generated by any other entity identified by the user's particular profile. An intelligent agent or "virtual" agent is generated based on the one or more user profiles, and messages are filtered according to the user preferences that are embodied in an agent's requirements. Filtered messages are then sent to the wireless communication device **160**.

The intermediary server **150** then waits for a user response. The user response may be positive and the user may wish to proceed with obtaining more information or acknowledging a particular action. The user may also NOT like the message sent, and the user response may be an opt-out request that states this message is undesirable. Alternatively, the user may provide a "thumbs up" or "thumbs down" feedback. Regardless, the resulting response is sent to the casino server **130**. The user profile resident on the intermediary server **150** is updated based on the user response.

In an alternative embodiment, the functions of the casino property server **130** and the authentication server **150** are performed on a single server for either a brick-and-mortar casino property or for a web-based casino property. If the intermediary server **150** resides on the casino property, privacy laws may be impacted because of perceived overreaching by the casino property because it warehouses location information. However, anonymity may not be an issue in certain foreign jurisdictions.

Although there a numerous benefits in the client-server architecture, there are also limitations associated with the client-server architecture that are not overcome by distributed object computing. These limitations include cost, lack of scalability, a single point of failure, administration difficulties, and the inefficient use of network resources. The peer-to-peer architecture is intended to address the limitations of the client-server solution and a migration from the client-server solution to the P2P solution is anticipated. In a peer-to-peer architecture clients are also servers and routers. Additionally, each node contributes content, storage, memory, and processing resources. The network is dynamic and nodes are free to enter and exit the network. The nodes can also collaborate directly with one another. Furthermore, nodes can have varying capabilities.

The goals and benefits of peer-to-peer systems include efficient use of resources so unused bandwidth, storage, and processing power at the edge of the network can be used efficiently. P2P systems are also scalable because there is no central information, communication and computation bottleneck. The P2P systems are also reliable and provide no single point of failure. There is also an ease of administration because the nodes self-organize and have built-in fault tolerance, replication, and load balancing, resulting in increased autonomy. Since a P2P network is not a centralized system, there a greater degree of anonymity and privacy in a P2P network. Since the P2P environment is highly dynamic, ad-hoc communication and collaboration is supported.

Referring to FIG. **2** there is shown an illustrative hierarchical P2P network which provides a second illustrative embodiment. For the illustrative P2P embodiment, the illustrative embodiment is a hierarchical peer-to-peer network that is comprised of three different types of nodes: Global Node(s) **210**, Jurisdictional Node(s) **220**, and Local Node(s) **230**. There may be different levels or subsets for each type of node, e.g. L**1** **235** and L**2** **236**. The hierarchical peer-to-peer network overlay is highly scalable, robust, and secure. The P2P overlay resides on a group of personal computers or servers, and leverages resources within an existing network infrastructure.

The development of the user profile including the user preferences and monitored betting activity or "personalization" is performed and controlled by the user (or the casino property). Thus, the user profile remains resident on the wireless communication device or personal computer that is used to access the illustrative network. By having users control their own profiles, the user ensures that desirable messages are received.

The Global Node (G) **210** authenticates each node in the network including the Jurisdictional Node **220** and the L**1** **235** and L**2** **236** Local Nodes. Additionally, the Global Node **210** authenticates the user accessing the network. The Global Node **210** provides oversight for the operations performed by each Jurisdictional Node **220**. The Global Node **210** also ensures that the files being shared by each node have the stated content. The Global Node **210** combines the user profile information received from the L**1** nodes **235**, the L**2** nodes **236**, and Jurisdictional Nodes **220** and generates a virtual agent. The virtual agent then filters information, and sends the filtered information to the L**2** node **236**, e.g. the user's wireless communication device **160**.

In one embodiment where the user's privacy concerns are a high priority, the Global Node **210** performs the operations of an anonymizing proxy, so the user, the user profile and the wireless communication device **160** become anonymous. In another embodiment where the systems' security concerns are the highest priority, the Global Node **210** provides oversight for the operations performed by the L**1** **235** and L**2** **236** nodes and anonymizing services are not performed.

In the illustrative P2P embodiment, the user profile is generated from information provided by the store (L**1** node **235**), and the user (L**2** node **236**). Also, information may be provided from the Jurisdictional Node **220**. Additionally, logged user profiles from a search engine may be used to contribute to the user profile. Although information from the Jurisdictional Node **220** and the logged search profiles from the user may contribute to the virtual agent, these contributions may conflict with the expectations of the store (L**1** node **235**) and the user (L**2** node **236**).

For example, a store may not want to enable a user to perform a search for a particular item being sold at a store, thus the store may want to block searches on Google while the user is within the store. The store may achieve this goal if the store can convince the Jurisdictional Node **220** that specific search engines are to be blocked while the user is within the store. Note, the store can itself become a Jurisdictional Node **220** if the store provides in-store Wi-Fi access. The user can elect to circumvent this blocking by using the anonymizing services provided by the Global Node **210**. However, these anonymizing services may not permit the user to obtain the same rebates or coupons as the user could obtain if the user elected not to be anonymous. Regardless of the situation, the user, the store, and possibly even the Carrier **120**/ISP **110** determine the scope of their relationship, and P2P architecture simply facilitates building this relationship.

The illustrative Global Node **210** may also be configured to share transactional revenues with Jurisdictional Nodes **220** and Local Nodes **230** that contribute to the transaction. Completed Point-of-Sale (POS) transactional information may also be shared.

The Jurisdictional Node (J) **220** controls access to the network. The Jurisdictional Node **220** may be associated with an illustrative Carrier **120**, service provider, or casino property. The Jurisdictional Node **220** pushes personalized data to the user based on the user's profile. The Jurisdictional Node **220** also polices the activities of each Local Node **230** within its network, and if a local node **230** is generating inappropriate content, the infected Local Node(s) **230** having the inappropriate content is blocked by the Jurisdictional Node **220**. Additionally, the Jurisdictional Node **220** may have stored or generated user-specific information that it is willing to "share" with the Global Node **210** so that a "better" virtual agent can be generated on behalf of the user.

The Jurisdictional Node (J) **220** controls access to the network. The Jurisdictional Node **220** is associated with an illustrative Carrier **120** or service provider **110**. The Jurisdiction Node **220** pushes personalized data to the user based on the user's profile. The Jurisdictional Node **220** also polices the activities of each Local Node **230** within its network, and if a local node **230** is generating inappropriate content, the infected Local Node(s) **230** having the inappropriate content is blocked by the Jurisdictional Node **220**. Additionally, the Jurisdictional Node **220** may have stored or generated user-specific information that it is willing to "share" with the Global Node **210** so that a "better" virtual agent can be generated on behalf of the user.

Jurisdictional Node **220** tools may be licensed to the Carrier **120** and/or service provider **110**. The tools permit the Jurisdictional Node **220** to generate revenue from sharing user profile information and from converting the wireless communication device to a Point-of-Sale (POS) device.

The Local Node (L) **230** stores the content that is sent via a targeted message. The local nodes **230** either provide or receive location information associated with the wireless communication device **160**. There are two types of local nodes: the L**1** Node **235** is a store-centric node; and the L**2** Node **236** is user-centric.

The L**2** Node **236** (user) is associated with the user and may reside on the users PC **140** and/or the users wireless communication device **160**. The L**2** Node **236** is configured to receive user profile information such as dining preferences, banking preferences, shopping preferences, in-store preferences, and opt-out preferences. For example, an opt-out preference may be "Block ALL Starbucks Messages." Additionally, the L**2** Node **236** (user) may receive location information and permits users to communicate location information.

Additionally, the L**2** Node **236** (user) may convert the wireless communication device **160** to a Point-of-Sale (POS) device that can use coupons, rebates, and gift cards. The L**2** Node **236** (user) is configured to close the transactional loop after receiving a targeted message and completes a transaction associated with the targeted message.

The L**1** Node **235** (store) may also have user profile information that it would like to contribute to generate the localized targeted advertisement. The Local Nodes **230** store content is associated with a particular location. For example, the L**1** Node **235** (store) may store indoor and outdoor advertising messages, so one message is received in a parking lot and another message is received within the store.

The L**1** Node **235** (store) software enables the store to generate mobile advertisements for handsets and to share the store's user profile. Additionally, the software enables the store to convert the wireless communication device to a POS device is also provided.

The L**2** Node **236** (user) software is freely distributed, unless the L**2** Node **236** (user) software is used for industrial and/or military applications. For industrial and/or military applications, the entire hierarchical P2P network overlay will likely operate within a single organizational structure.

Casino Application

The casino application may reside in either the client-server network architecture or the P2P network architecture. However, because of the degree of control need over sensitive player information and because of the progression towards server based gaming, the client-server network architecture is likely the preferred architecture.

Player tracking is an important element of a casino property's goal to retain players and build player goodwill. Player tracking information is information related to how a player wagers in a casino property. Based on the player tracking information, the casino determines how to "comp" the player. Comps are complimentary gifts or services that are provided to the player, e.g. gaming credits, redeemable cash, free rooms, room upgrades, tickets to shows, show upgrades, complimentary restaurant meals, etc. Player tracking information is extremely sensitive and proprietary information that a casino property does NOT share with any competitors. Currently, player tracking is used to track "regular players" and usually a regular player is provided with a mag stripe card that the player swipes into a gaming machine or gives the dealer at a table game their card.

In a first casino property embodiment, the player is provided with a mobile handset that is GPS and/or location enabled. For illustrative purposes only, the player is a "whale" or high roller. The handset may provide local anonymity and the same benefits of an in-room phone. In a second casino property embodiment, the player provides a phone number, and allows one or more software applets to be downloaded to their handset.

Casino properties maintain profiles for their preferred players. These profiles are used to create an experience that keeps the player coming back to the property. The system and method described herein place the casino staff at the beck and call of the player.

For the casino property application, the user profile is provided by the casino property and may be managed by the casino property. The user profile for a particular player may include information such as cocktail preferences, dining preferences, entertainment preferences, gaming preferences, and opt-out preferences. The handset can be used to gain VIP admissions to clubs and shows, and even room access.

In the casino property embodiment, the carriers will need to provide location information. In certain instances, such as within a building, GPS information may be more difficult to obtain, and a Wi-Fi network may be needed within the casino property, e.g. gaming zones and high roller suites.

To accommodate the user, a handset may be loaned to the user. The type of handsets that are loaned must possess a user interface (UI) that is attractive to the user. However, there may be resistance to using a new handset, when the user has invested so much time in understanding the existing UI on the user's current handset. Therefore, to accommodate the type of user not wishing to switch handsets, then the handset must be configured to receive one or more software programs, e.g. Java applets, which reside on the handset, and provide the functionality described above.

For illustrative purposes only, a dual mode handset is selected that includes CDMA, EV-DO and Wi-Fi technology. The handset is GPS enabled. Wi-Fi technology and related triangulation technologies are used in certain locations where GPS may not provide sufficient accuracy. For example, it may desirable to send a high roller a targeted message when the high roller is at the Bar telling them that they qualify for a $500 credit, or they have "won" a free meal or a suite upgrade.

Additionally, the handset may have a large storage component that stores user specific information that is triggered based on location and/or user requests. Thus, a desirable and targeted video message can play after the user has been sitting at the Bar for five minutes, and this message may be pre-loaded on the handset.

The handset may also be programmed in English or the whale's language of origin, e.g. Japanese, Mandarin, Korean, Arabic, Farsi, etc. The interface may be modified to include concierge information, and point of interest (POI) information. Room service and similar casino services can also be programmed into the handheld device.

In the illustrative casino property embodiment, player tracking information is not shared with another casino property and is not used for data mining by the Carrier because this will destroy the trust relationship that is being developed with the player and the casino property. Thus, it is of the utmost importance that this information not be accessible by a competing casino property.

Consumer Application

The consumer application may reside in either the client-server network architecture or the P2P network architecture. However, because of the viral nature of P2P networks and because of the desire for various entities to maintain the confidentiality of their information, a distributed solution such as a P2P is likely the preferred architecture.

In the illustrative consumer oriented embodiment, personalization is performed by the user. Generally, the profile is generated using a browser on a personal computer. With the tools described, each user can create a tailored user profile. The user profile can include information such as preferred dining preferences, hobbies, banking preferences, shopping preferences, and opt-out preferences.

In the consumer oriented embodiment, the user can identify specifics associated with the user's service plan. For example, the user may have disabled web browsing because of the challenges associated with Web surfing on a handset. Thus, the user service plan may only support voice calls, and SMS messages. For this particular user, the user profile may be configured to send targeted SMS messages. Preferably, the advertiser pays for the cost of the SMS message.

For the consumer oriented embodiment, one goal is to minimize the need for network modifications. Our goal is to provide an offering to carrier or service provider in which the user can configure their handset in a manner consistent with the actions performed by a highly targeted Mobile Virtual Network Operator (MVNO), except the embodiment adds a location component, user profiles and virtual agents.

Thus, the illustrative tools are able to simulate providing a user-defined MVNO handset that is adaptable. So, if a user starts with voice and SMS, MMS and obtains targeted messages that are limited by screen resolution and functionality of the handset, the user may wish to upgrade handsets and upgrade service features to obtain the more desirable targeted advertising. For example, coupon promotion may accommodate the advertisers and carriers business model, so a better promotion may be received on a more sophisticated handset.

It is to be understood that the foregoing is a detailed description of illustrative embodiments. The scope of the claims is not limited to these specific embodiments or examples. Therefore, various elements, details, execution of any methods, and uses can differ from those just described, or be expanded on or implemented using technologies not yet commercially viable, and yet still be within the inventive concepts of the present disclosure. The scope of the invention is determined by the following claims and their legal equivalents.

What is claimed is:

1. An interactive gaming system for a casino property, the interactive gaming system comprising:

a wireless device associated with a registered user, wherein the wireless device is used to determine a location of the registered user and the wireless device communicates with a network using at least one wireless networking protocol;

a verification system that accesses a registration database having registration data associated with each registered user;

a centralized gaming server communicatively coupled to the wireless device, the centralized gaming server generates at least one random game outcome;

a memory module that stores a plurality of images corresponding to the at least one game outcome that are communicated to the wireless device;

the centralized gaming server accesses the memory module and communicates the plurality of images corresponding to the random game outcome to the wireless device; and

a casino player tracking system that includes,

a registered user profile that further includes a plurality of user preferences,

a record of a plurality of accumulated points associated with a betting activity of the registered user, wherein the betting activity is associated with the random outcomes generated by the centralized gaming server,

at least one complimentary good or service corresponding to the accumulated points associated with the registered user; and

a plurality of messages generated by the casino player tracking system for the wireless device regarding the complementary goods or services.

2. The interactive gaming system of claim **1** further comprising an intermediary server that is communicatively coupled to the casino player tracking system and the wireless device, the intermediary server determines the location of the registered user and the intermediary server receives a plurality of user profile preferences;

wherein the casino player tracking system is communicatively coupled to at least one of a plurality of slot machines, a plurality of gaming tables, a plurality of restaurants, a plurality of retail sales locations; and

wherein the intermediary server is configured to filter the plurality of messages generated by the casino player tracking system based on the location of the registered user and the user profile preferences.

3. The interactive gaming system of claim **1**, wherein at least one registered user profile includes a biometric.

4. The interactive gaming system of claim **2** wherein the registered user profile comprises a field that permits the location of the registered user to be tracked.

5. The interactive gaming system of claim **4** wherein the message sent to the wireless handset is dependent on the location of the customer.

6. The interactive gaming system of claim **1** further comprising an automated message that is sent when a sensor is triggered.

7. The interactive gaming system of claim **1** further comprising an automated message that is sent when the registered user is in a particular location.

8. An interactive gaming system for a casino property, the interactive gaming comprising:

a wireless device associated with a registered user, wherein the wireless device is used to determine a location of the

registered user and the wireless device communicates with a network using at least one wireless networking protocol;

a verification system that accesses a registration database having registration data associated with each registered user;

a centralized gaming server communicatively coupled to the wireless device, the centralized gaming server generates at least one random game outcome;

a memory module that stores a plurality of images corresponding to the at least one game outcome that are communicated to the wireless device;

the centralized gaming server accesses the memory module and communicates the plurality of images corresponding to the random game outcome to the wireless device;

a casino player tracking server that includes,

a registered user profile that further includes a plurality of user preferences,

a record of a plurality of accumulated points associated with a betting activity of the registered user, wherein the betting activity is associated with the random outcomes generated by the centralized gaming server,

at least one complimentary good or service corresponding to the accumulated points associated with the registered user;

a plurality of messages generated by the casino player tracking server for the wireless device regarding the complementary goods or services;

an intermediary server that is communicatively coupled to the casino player tracking server and the wireless device, wherein the intermediary server determines the location of the registered user and the intermediary server receives a plurality of user profile preferences; and

wherein the intermediary server is configured to filter the plurality of messages generated by the casino player tracking system based on the location of the registered user and the user profile preferences.

9. The interactive gaming system of claim **8** wherein the casino player tracking system is communicatively coupled to at least one of a plurality of slot machines, a plurality of gaming tables, a plurality of restaurants, a plurality of retail sales locations.

10. The interactive gaming system of claim **8**, wherein at least one registered user profile includes a biometric.

11. The interactive gaming system of claim **8** wherein the registered user profile comprises a field that permits the location of the user to be tracked.

12. The interactive gaming system of claim **8** further comprising an automated message that is sent when a sensor is triggered.

13. An interactive gaming method for a casino property, the interactive gaming method comprising:

determining a location of a wireless device associated with a registered user with an intermediary server, wherein the wireless device communicates with a network using at least one wireless networking protocol and the wireless device is communicatively coupled to the intermediary server;

accessing a registration database having registration data associated with each registered user;

generating at least one random game outcome at a centralized gaming server that is communicatively coupled to the wireless device;

storing a plurality of images at a memory module, wherein the plurality of images correspond to the at least one game outcome that is communicated to the wireless device;

communicating the plurality of images corresponding to the random game outcome to the wireless device after the centralized gaming server accesses the memory module; and

generating a plurality of messages with a casino player tracking system that is communicatively coupled to the intermediary server, wherein the messages are associated with the complementary goods or services, the casino player tracking system includes,

a registered user profile that further includes a plurality of user preferences,

a record of a plurality of accumulated points associated with a betting activity of the registered user, wherein the betting activity is associated with the random outcomes generated by the centralized gaming server, and

at least one complimentary good or service corresponding to the accumulated points associated with the registered user; and

receiving a plurality of the user profile preferences at the intermediary server, which is communicatively coupled to the casino player tracking system and the wireless device; and

filtering the plurality of messages generated by the casino player tracking system based on the location of the registered user and the user profile preference with the intermediary server.

14. The interactive gaming method of claim **13** wherein the message generated by the casino player tracking system is communicated by an intermediary server based on the location of the user and the registered user profile, wherein the intermediary server determines the location of the user.

15. The interactive gaming method of claim **13** wherein the casino player tracking system is communicatively coupled to at least one of a plurality of slot machines, a plurality of gaming tables, a plurality of restaurants, a plurality of retail sales locations.

16. The interactive gaming method of claim **13**, wherein each registered user profile includes an activity points field.

17. The interactive gaming method of claim **13** wherein the registered user profile comprises a field that permits the location of the user to be tracked.

18. The interactive gaming method of claim **13** further comprising sending an automated message when a sensor is triggered.

19. The interactive gaming method of claim **13** further comprising verifying the registered user profile with a biometric.

20. The interactive gaming method of claim **13** further comprising sending the message to the wireless handset based on the location, the plurality of accumulated points and the user profile.

* * * * *

PLAY NOW!

Play Free Slot Games Online

When someone mentions the word casino, one of the first words that springs to mind is Caesars. There's a good reason for that. Caesars has become synonymous with slot games because of our long history of providing a premium casino experience. Now, Caesars Games Online lets you experience our epic online slots right from the comfort of your own home.

From mythical creatures to fantastical settings filled with wonder and mystery, Caesars Games Online offers a dose of adventure for everyone. So, get yourself comfortable in your favorite chair, grab some snacks, pour yourself a cup of your favorite beverage, and get ready for some free online slots!

SORT BY: NEW DATE A-Z

Search for games:

Wild Howl

Pink Panther

Scherwood Fortune

New Year's Blast

Moby Dick

Zeus Fortune

Leprechaun Riches Beautiful Bandits Meowza

Cabaret Rouge

Goddess of the Pyramids

Mount Grizzly

Rhino Power

Wild Queens

Tiger Tropics

This is Sparta

Riches of Aladdin

High Class Hogs

Lion's Roar

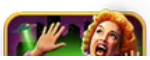
Lucky in Paris

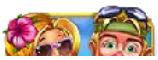
Geisha & Samurai

Kabuki Knockout

Zodiac Ladies

Tropical Fantasy





Lucky Phoenix

Foxtrot Follies

Vegas Zombies

Spin Dragons

Reel Destiny

Diamond Express

Skeleton Bay

Daring Damsels

Ocean Splendor

Cleopatra's Quest

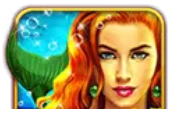
Mighty Musketeers

Buffalo Sunrise

Samba Shake

Midnight Fiesta

Lightning Queen



King of the Grill

Beer Bonanza

The Great Pierre

Dragon Chase

Dr. Jekyll's Jackpot

Diamond Princess

Crazy Goblin Gold

Cheese Heist

Here’s Why You’ll Love Caesars’ Free Slot Games

If you’ve been craving an epic casino experience, you’ve come to the right place. For those of you who crave adventure but can’t drop everything and start trotting across the globe, Caesars free slots online offers the perfect outlet for any craving for exploration and fantasies. Caesars online slot machine games allow you to play our slots online free from anywhere.
Play our legendary casino slots games at any time, whether it’s resting in bed or waiting in line at the grocery store. Escape the stress of your day by taking a dive into one of the many wondrous worlds featured in our free slot machine games roster.

Play Slots for Fun – Caesars Epic Features

Here’s why you don’t want to miss out on our epic slots:

- A Premium Gaming Experience: Caesars Games online offers an online casino experience like none other, with state-of-the-art gaming mechanics and unique game themes designed to transport you into another world.
- High-Class Graphics and Design: Our online slots are designed by world-class graphic designers who know how to create an immersive gaming experience you won’t find for free anywhere else. Simply stated

The Best Way to Enjoy Caesars' Free Casino Slots

Caesars slot machines games offers a variety of easy, flexible, and convenient ways to play. One of the best ways to enjoy our free slots is by logging in through Facebook and playing on your desktop. You can also play free slot games for fun on your phone by downloading the Caesars slot machine app on iOS through Apple's App Store, or on Android through Google Play.

Our phone apps are completely free and can be played from anywhere at any time, offering the ultimate mobile slots experience. Carry your favorite slot games around in your pocket.

Guide for How to Play Free Slots Online

Are you interested in playing free slot games with bonus rounds no download and no strings attached? Here's how to play free slot machines online:

- Visit CaesarsGames.com or search for Caesars slot machines on your mobile device. Once you find our Caesars Slot Machines Games mobile app through your app store of choice, download the game onto your mobile device for free and start spinning the reels!
- Use your free coins to play our free slot machines. When you first start playing you'll get access to dozens of free games to get you started, in addition you'll get hourly surprises, and will never find yourself bored again!
- Play our free casino slot games for fun, zero strings attached! With so many opportunities for playing, you'll never feel forced to buy additional coins, but they'll always there if you want them!

10 Things You Should Know about Free Slot Machines

1. Caesars offers over 50 free casino slot games with bonus rounds. Whether you're in the mood to battle Moby Dick, explore Sherwood Forest, or hang out with the pharaohs in Ancient Egypt, there's always a new immersive theme to experience.

2. There's no need to spend a fortune if you want to win the jackpot. Caesars offers every new player free coins to get you started down your path of riches.

3. Caesars is available on iOS and Android! No matter which platform you prefer, Caesars is there to keep your casino craving satisfied. You can even play our free slots on your preferred tablet, including iPad.

4. Different types of machines means a huge variety of new and exciting wild symbols! Our themed games are designed to offer our users a huge variety of options. Each epic game includes its own unique take on the mobile slots experience.

5. Our mobile apps are absolutely free to download! You can get started right away at no charge!

6. You can sign-in to Caesars using your Facebook account. Connecting your account allows you to pick

8. Everyone is treated like a VIP at Caesars. Unlike some traditional casinos, everyone who plays on the Caesars free slots app is treated like a winner.

9. Learning how to win at slots is easy. Just be lucky! Slots is inherently a skill-less game. Just be smart with your bets and keep your eyes on the prize.

10. The fruit symbols you've come to expect from traditional Vegas slots are a thing of the past. While you can certainly play more traditional games with the Caesars apps, we suggest branching out into one of our epic slot adventures!

FAQ about Free Online Slots

What are free slots?

Caesars offers free slot machines with free slot machine coins, which means you can play at absolutely no cost to you!

Can I win money playing free slots?

While you won't win any real cash playing slots for free, you can earn your riches in Caesars free slot coins! You can then use these coins to play more slots.

Can I play free slots on my mobile device?

Absolutely! Caesars free slot machine app is available through Apple's App Store and Google Play.

Do I need to download anything to play free slots?

Not if you play through your internet browser! Simply visit our site, login, and start spinning!

Are free slot games similar to real money machines?

Not only are they similar, they're exactly the same! The only difference is that you don't have to spend any of your hard-earned cash to play! Enjoy the casino experience without the risk!

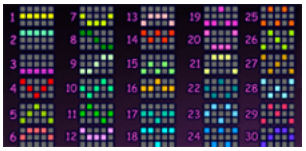
The games do not offer "real money gambling" or an opportunity to win real money or prizes. The games are intended for an adult audience. Practice or success at social casino gaming does not imply future success at "real money gambling"

HOW TO PLAY SLOTS

PLAY NOW!

To start having fun at Slotomania.com, create an account and password by registering with your email address or connecting your account through Facebook.
To start playing, just click SPIN! The reels will begin to spin and then stop one by one to reveal if there's a win! Wins are paid for matching, consecutive symbols that appear on paylines going from left to right across the reels, as described in the pay table.

PAYLINES



A payline represents a path going from left to right across the reels. It may run straight across, diagonally, zig-zag or along any number of routes. When you beton a payline, it becomes active. If the symbols that make up a winning combination appear in the positions represented by an active payline, you win the associated payouts for that symbol, as indicated in the pay table.
Classic slot games used to play one line across the reels. Nowadays, many games let you play as many as 100 lines! You can increase or decrease the number of paylines or click MAX LINES to play all available paylines. The more lines you play, the better your odds at creating a winning combination.

BETS

You can also Increase or decrease your bet per line. Wins are multiplied by the bet per line, so the higher your bet, the higher your win! Your TOTAL BET is the amount that will be deducted from your balance when you click SPIN and is calculated by multiplying the number of lines times the BET. For example, if you are playing 9 lines and your bet per line is 5 Coins, your TOTAL bet is 45 (9 X 5 = 45). With this configuration, every time you click SPIN, 45 Coins will be deducted from your balance.

Now, let's say you spin and 3 cherry symbols appear consecutively on an active payline. The pay table says that 3 cherries pay 100. Because your bet per line is 5, your total win is 500 for those 3 cherries (100 X5 = 500).

Because you can make multiple winning combinations on each spin, the more lines you play, the greater your chances of winning.

PAY TABLE

During a spin, it's possible to win bonus games, free spins and other special prizes on the reels! Check out the pay table for each game to see what special features and prizes can be awarded during a spin. The pay table will also tell how you how much each symbol pays, which reels the special symbols appear on, as well as the specific rules of each game.

SCATTER

Scatter symbols appear in most games. Getting a certain number on the reels may award free spins, more Coins or even a mini game. Scatter symbols are unique in that they are always awarded for appearing anywhere on the reels – they do not have to be on an active payline.

WILD

A Wild symbol may substitute for any other symbol when it appears on the reels, except special symbols, like Scatter and Bonus. Some games offer exciting variations:

- Expanding Wilds stretch to transform a whole reel into Wild symbols.
- Wild Multipliers will multiply your win (x2, x3, x4…) when they appear
- as part of a winning combination.
- Multiplying Wilds will turn other symbols on the reels into Wilds.

BONUS

Bonus symbols appear in many games and are an exciting chance to win big Coin Prizes. Every game has different Bonus Rounds that relate to the story of the game. You might be hunting for treasure with pirates or finding diamonds in Monte Carlo!

JS 44 (Rev. 09/19)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

NEXRF Corp.

(b) County of Residence of First Listed Plaintiff _____
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Adam Yowell, Fisher Broyles, 775-230-7364
59 Damonte Ranch Pkwy, Ste B # 508
Reno NV 89521

DEFENDANTS

Playtika, Ltd., Playtika Holding Corp., Caesars Interactive Entertainment LLC

County of Residence of First Listed Defendant _____
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ❒ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ❒ 2 U.S. Government Defendant
- ❒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	❒ 1	❒ 1	Incorporated *or* Principal Place of Business In This State	❒ 4	❒ 4
Citizen of Another State	❒ 2	❒ 2	Incorporated *and* Principal Place of Business In Another State	❒ 5	❒ 5
Citizen or Subject of a Foreign Country	❒ 3	❒ 3	Foreign Nation	❒ 6	❒ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ❒ 110 Insurance
- ❒ 120 Marine
- ❒ 130 Miller Act
- ❒ 140 Negotiable Instrument
- ❒ 150 Recovery of Overpayment & Enforcement of Judgment
- ❒ 151 Medicare Act
- ❒ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ❒ 153 Recovery of Overpayment of Veteran's Benefits
- ❒ 160 Stockholders' Suits
- ❒ 190 Other Contract
- ❒ 195 Contract Product Liability
- ❒ 196 Franchise

REAL PROPERTY
- ❒ 210 Land Condemnation
- ❒ 220 Foreclosure
- ❒ 230 Rent Lease & Ejectment
- ❒ 240 Torts to Land
- ❒ 245 Tort Product Liability
- ❒ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ❒ 310 Airplane
- ❒ 315 Airplane Product Liability
- ❒ 320 Assault, Libel & Slander
- ❒ 330 Federal Employers' Liability
- ❒ 340 Marine
- ❒ 345 Marine Product Liability
- ❒ 350 Motor Vehicle
- ❒ 355 Motor Vehicle Product Liability
- ❒ 360 Other Personal Injury
- ❒ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ❒ 365 Personal Injury - Product Liability
- ❒ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ❒ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ❒ 370 Other Fraud
- ❒ 371 Truth in Lending
- ❒ 380 Other Personal Property Damage
- ❒ 385 Property Damage Product Liability

CIVIL RIGHTS
- ❒ 440 Other Civil Rights
- ❒ 441 Voting
- ❒ 442 Employment
- ❒ 443 Housing/ Accommodations
- ❒ 445 Amer. w/Disabilities - Employment
- ❒ 446 Amer. w/Disabilities - Other
- ❒ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ❒ 463 Alien Detainee
- ❒ 510 Motions to Vacate Sentence
- ❒ 530 General
- ❒ 535 Death Penalty

Other:
- ❒ 540 Mandamus & Other
- ❒ 550 Civil Rights
- ❒ 555 Prison Condition
- ❒ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ❒ 625 Drug Related Seizure of Property 21 USC 881
- ❒ 690 Other

LABOR
- ❒ 710 Fair Labor Standards Act
- ❒ 720 Labor/Management Relations
- ❒ 740 Railway Labor Act
- ❒ 751 Family and Medical Leave Act
- ❒ 790 Other Labor Litigation
- ❒ 791 Employee Retirement Income Security Act

IMMIGRATION
- ❒ 462 Naturalization Application
- ❒ 465 Other Immigration Actions

BANKRUPTCY
- ❒ 422 Appeal 28 USC 158
- ❒ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ❒ 820 Copyrights
- ☒ 830 Patent
- ❒ 835 Patent - Abbreviated New Drug Application
- ❒ 840 Trademark

SOCIAL SECURITY
- ❒ 861 HIA (1395ff)
- ❒ 862 Black Lung (923)
- ❒ 863 DIWC/DIWW (405(g))
- ❒ 864 SSID Title XVI
- ❒ 865 RSI (405(g))

FEDERAL TAX SUITS
- ❒ 870 Taxes (U.S. Plaintiff or Defendant)
- ❒ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ❒ 375 False Claims Act
- ❒ 376 Qui Tam (31 USC 3729(a))
- ❒ 400 State Reapportionment
- ❒ 410 Antitrust
- ❒ 430 Banks and Banking
- ❒ 450 Commerce
- ❒ 460 Deportation
- ❒ 470 Racketeer Influenced and Corrupt Organizations
- ❒ 480 Consumer Credit (15 USC 1681 or 1692)
- ❒ 485 Telephone Consumer Protection Act
- ❒ 490 Cable/Sat TV
- ❒ 850 Securities/Commodities/ Exchange
- ❒ 890 Other Statutory Actions
- ❒ 891 Agricultural Acts
- ❒ 893 Environmental Matters
- ❒ 895 Freedom of Information Act
- ❒ 896 Arbitration
- ❒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ❒ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ❒ 2 Removed from State Court ❒ 3 Remanded from Appellate Court ❒ 4 Reinstated or Reopened ❒ 5 Transferred from Another District *(specify)* ❒ 6 Multidistrict Litigation - Transfer ❒ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
35 USC Section 271

Brief description of cause:
patent infringement

VII. REQUESTED IN COMPLAINT:

❒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ❒ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE _____ DOCKET NUMBER _____

DATE
10/26/2020

SIGNATURE OF ATTORNEY OF RECORD
/s/ Adam Yowell

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Nevada

NEXRF Corp.

Plaintiff(s)

v.

Playtika Ltd.,
Playtika Holding Corp.,
Caesars Interactive Entertainment LLC

Defendant(s)

Civil Action No. 3:20-cv-00603

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Playtika Ltd.
2225 Village Walk Drive #240
Henderson, Nevada 89052

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Adam Yowell
FisherBroyles LLP
59 Damonte Ranch Pkwy
Ste B #508
Reno, NV 89521
775-230-7364
adam.yowell@fisherbroyles.com

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No. 3:20-cv-00603

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Nevada

NEXRF Corp.

Plaintiff(s)

v.

Playtika Ltd.,
Playtika Holding Corp.,
Caesars Interactive Entertainment LLC

Defendant(s)

Civil Action No. 3:20-cv-00603

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Playtika Holding Corp.
2225 Village Walk Drive #240
Henderson, Nevada 89052

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Adam Yowell
FisherBroyles LLP
59 Damonte Ranch Pkwy
Ste B #508
Reno, NV 89521
775-230-7364
adam.yowell@fisherbroyles.com

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No. 3:20-cv-00603

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Nevada

NEXRF Corp.

Plaintiff(s)

v.

Playtika Ltd.,
Playtika Holding Corp.,
Caesars Interactive Entertainment LLC

Defendant(s)

Civil Action No. 3:20-cv-00603

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Caesars Interactive Entertainment LLC
One Caesars Palace Drive
Las Vegas, Nevada 89109

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Adam Yowell
FisherBroyles LLP
59 Damonte Ranch Pkwy
Ste B #508
Reno, NV 89521
775-230-7364
adam.yowell@fisherbroyles.com

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No. 3:20-cv-00603

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc: