US 20020142844A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2002/0142844 A1

Kerr (43) Pub. Date: Oct. 3, 2002

(54) BIOMETRIC BROADBAND GAMING SYSTEM AND METHOD

(76) Inventor: **Michael A. Kerr**, Stateline, NV (US)

Correspondence Address:
Michael A. Kerr
VIRTUAL LEGAL
777 E. WILLIAM ST.
STE. 211
CARSON CITY, NV 89701 (US)

(21) Appl. No.: **09/899,559**

(22) Filed: **Jul. 5, 2001**

Related U.S. Application Data

(60) Provisional application No. 60/266,856, filed on Feb. 7, 2001.

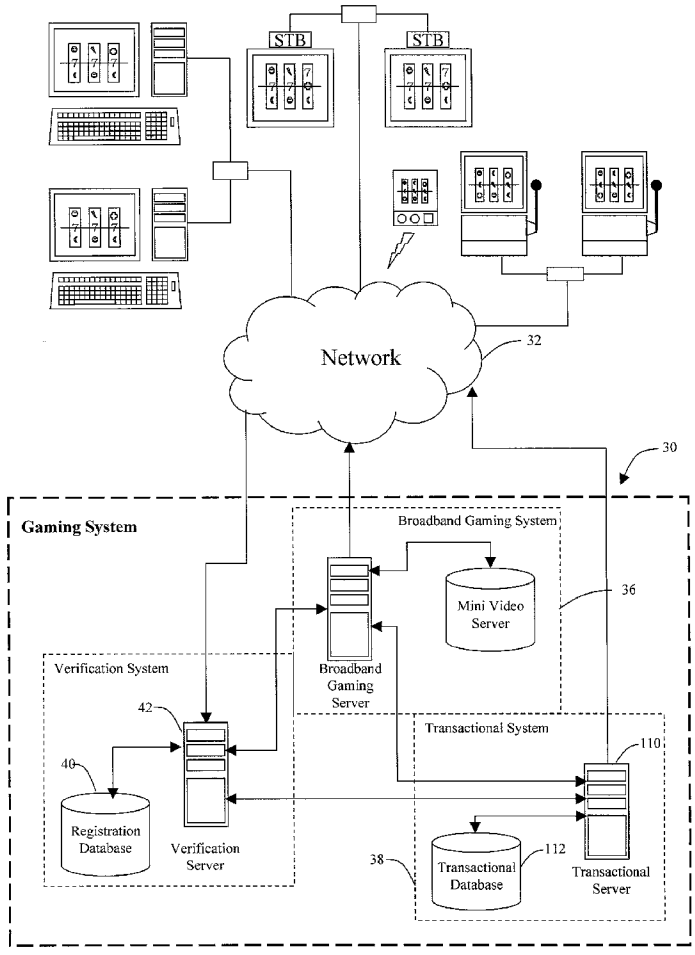
Publication Classification

(51) **Int. Cl.**[7] **G06F 17/00**

(52) **U.S. Cl.** **463/42**

(57) **ABSTRACT**

The present invention is a biometric broadband gaming system and method that comprises a verification system, a broadband gaming system and a transactional system. The verification system operations include receiving a biometric input to ensure that a user is a registered player. The broadband gaming system operations include providing a game of skill or game of chance to a plurality of players communicating via different network access devices. The transactional system operations include managing transactions conducted by the verification system and the broadband gaming system.



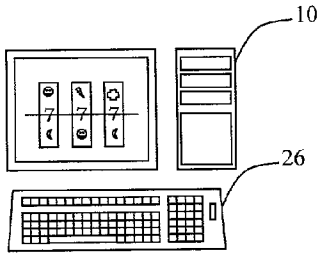


FIG. 1a

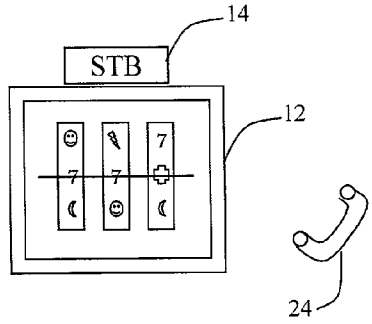


FIG. 1b

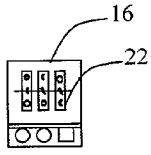


FIG. 1c

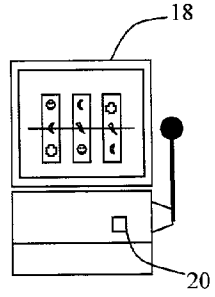
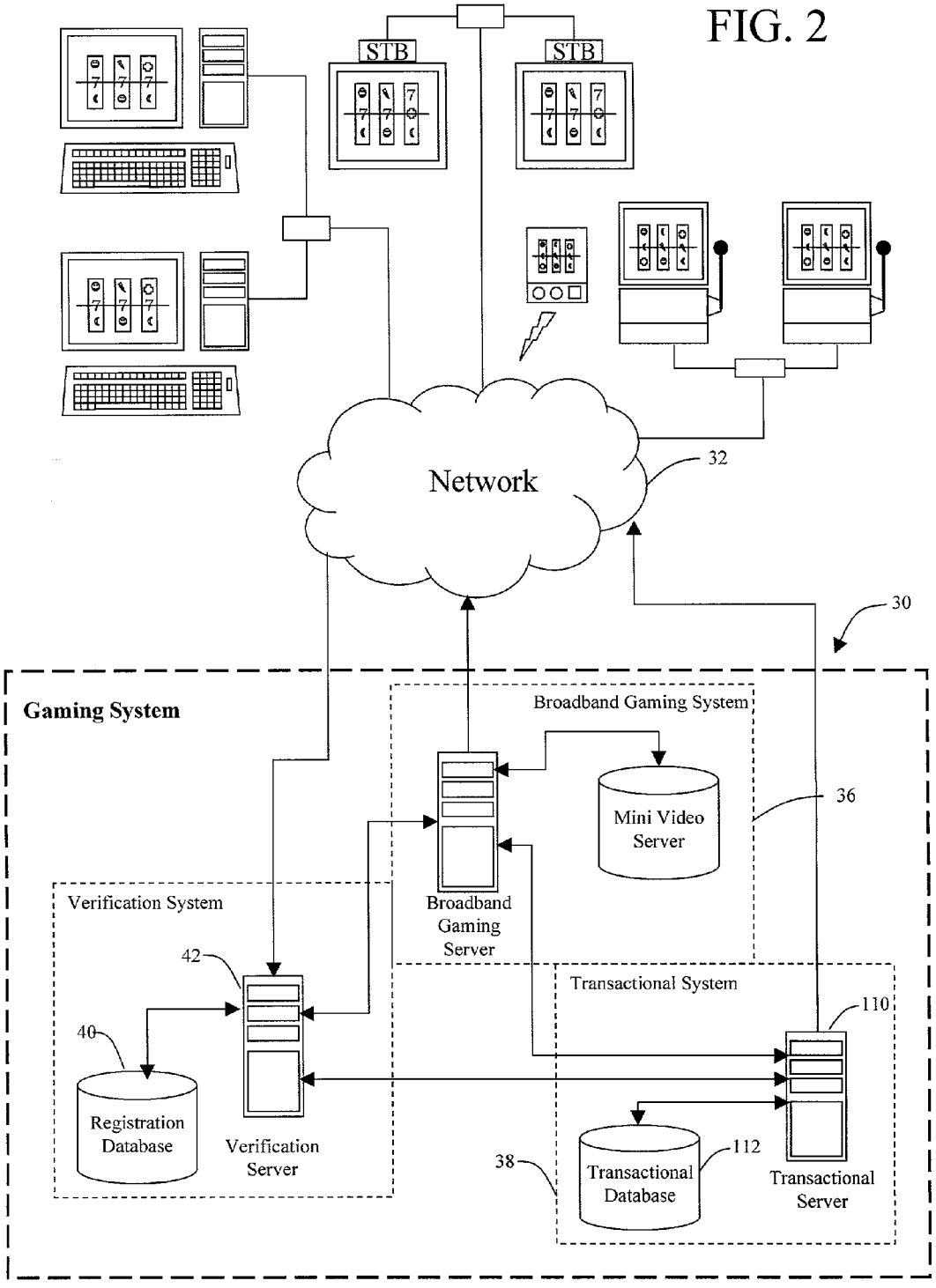


FIG. 1d

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

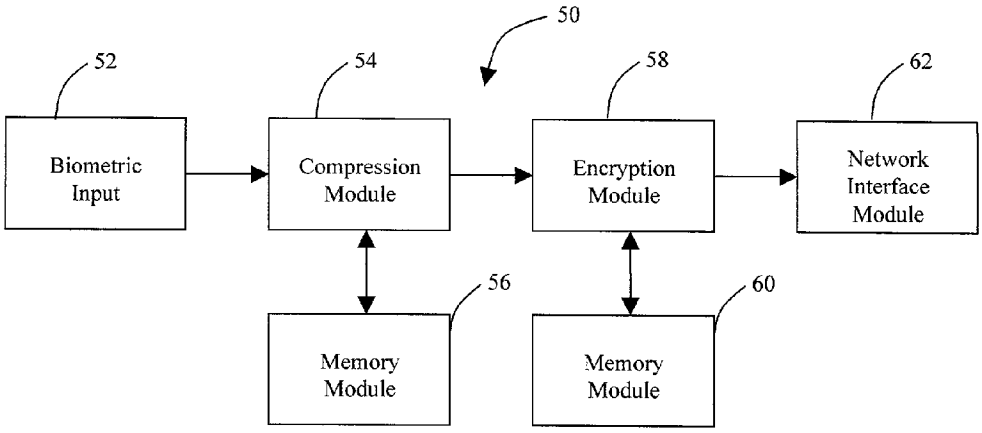

50
52
54
58
62
Biometric Input
Compression Module
Encryption Module
Network Interface Module
56
60
Memory Module
Memory Module

FIG. 3

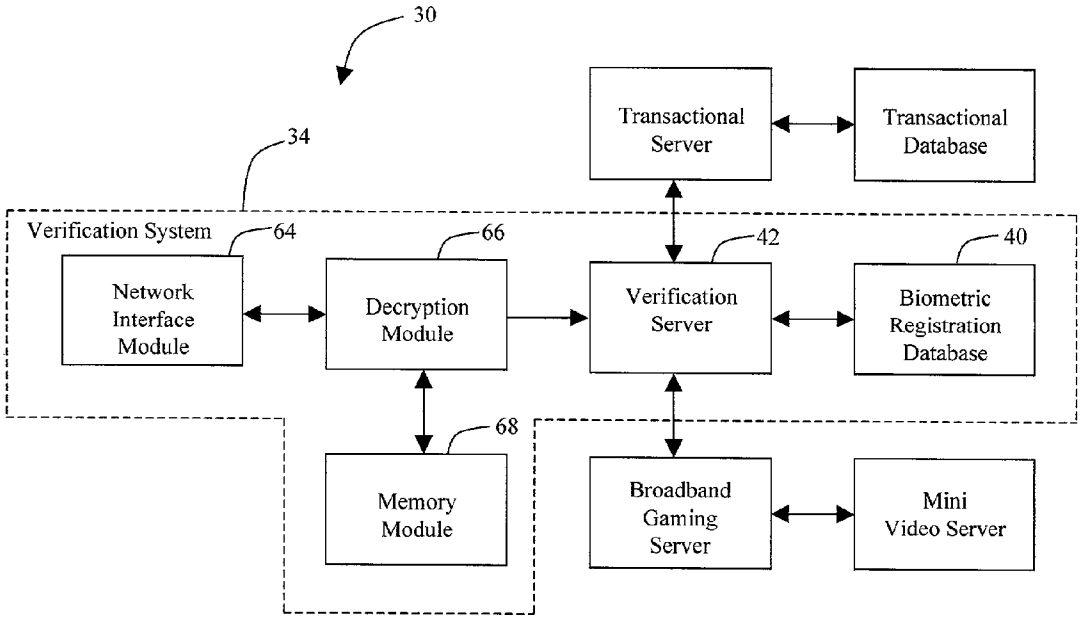

30
34
Transactional Server
Transactional Database
Verification System
64
66
42
40
Network Interface Module
Decryption Module
Verification Server
Biometric Registration Database
68
Memory Module
Broadband Gaming Server
Mini Video Server

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

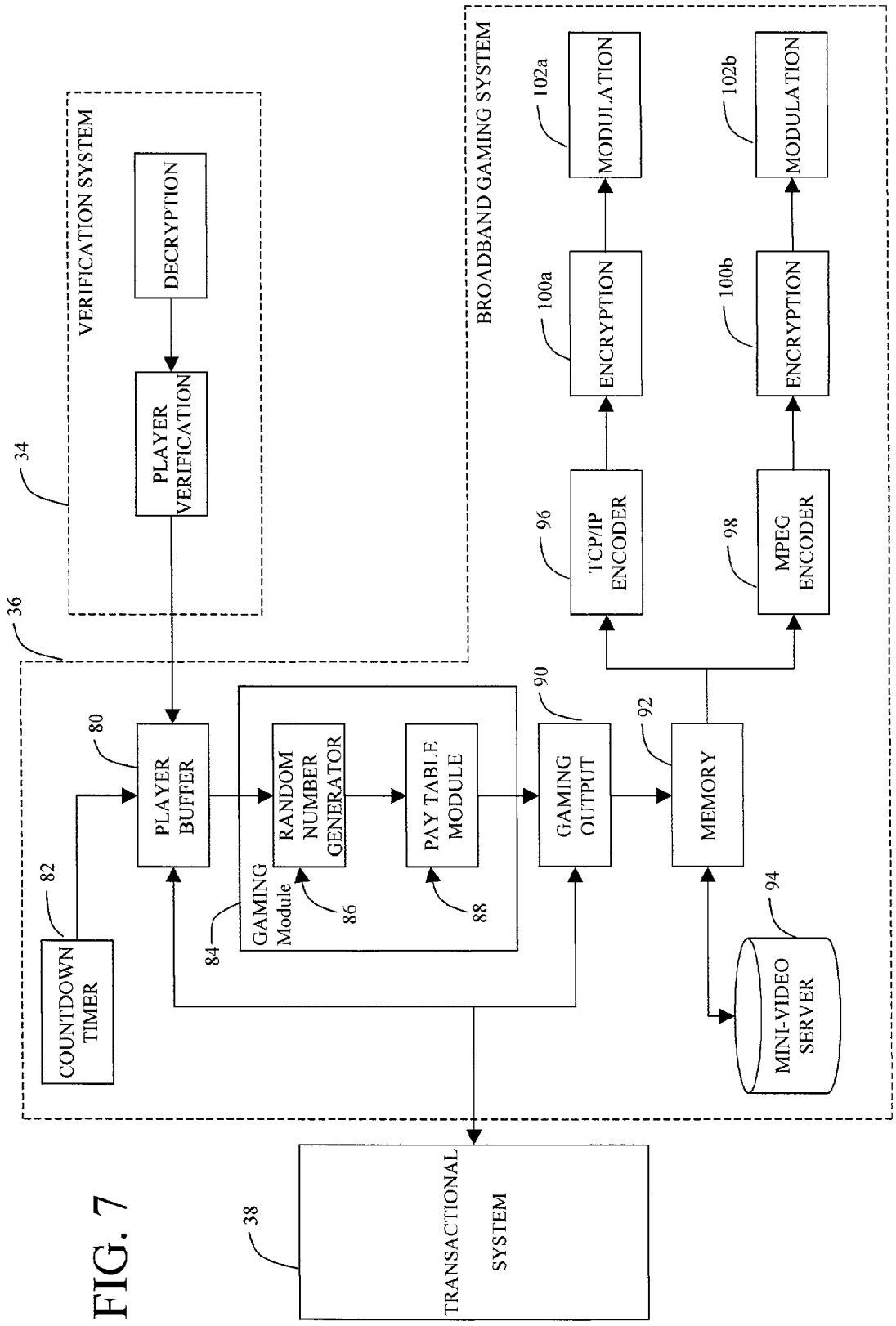

VERIFICATION SYSTEM
DECRYPTION
PLAYER VERIFICATION
34
36
BROADBAND GAMING SYSTEM
102a
MODULATION
102b
MODULATION
100a
ENCRYPTION
100b
ENCRYPTION
96
TCP/IP ENCODER
98
MPEG ENCODER
80
PLAYER BUFFER
RANDOM NUMBER GENERATOR
PAY TABLE MODULE
90
GAMING OUTPUT
92
MEMORY
82
COUNTDOWN TIMER
84
GAMING Module
86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

FIG. 7

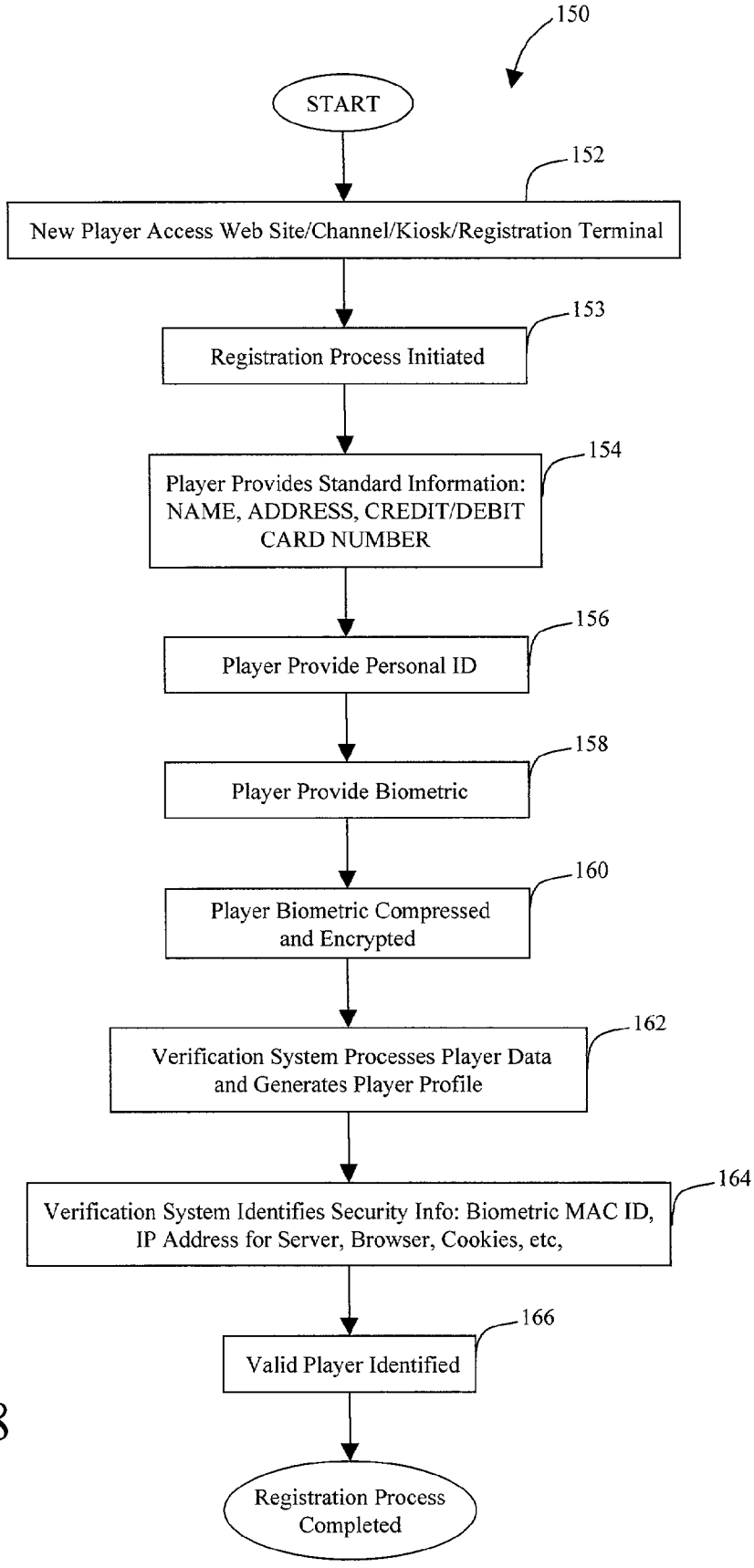

150
START
152
New Player Access Web Site/Channel/Kiosk/Registration Terminal
153
Registration Process Initiated
154
Player Provides Standard Information: NAME, ADDRESS, CREDIT/DEBIT CARD NUMBER
156
Player Provide Personal ID
158
Player Provide Biometric
160
Player Biometric Compressed and Encrypted
162
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

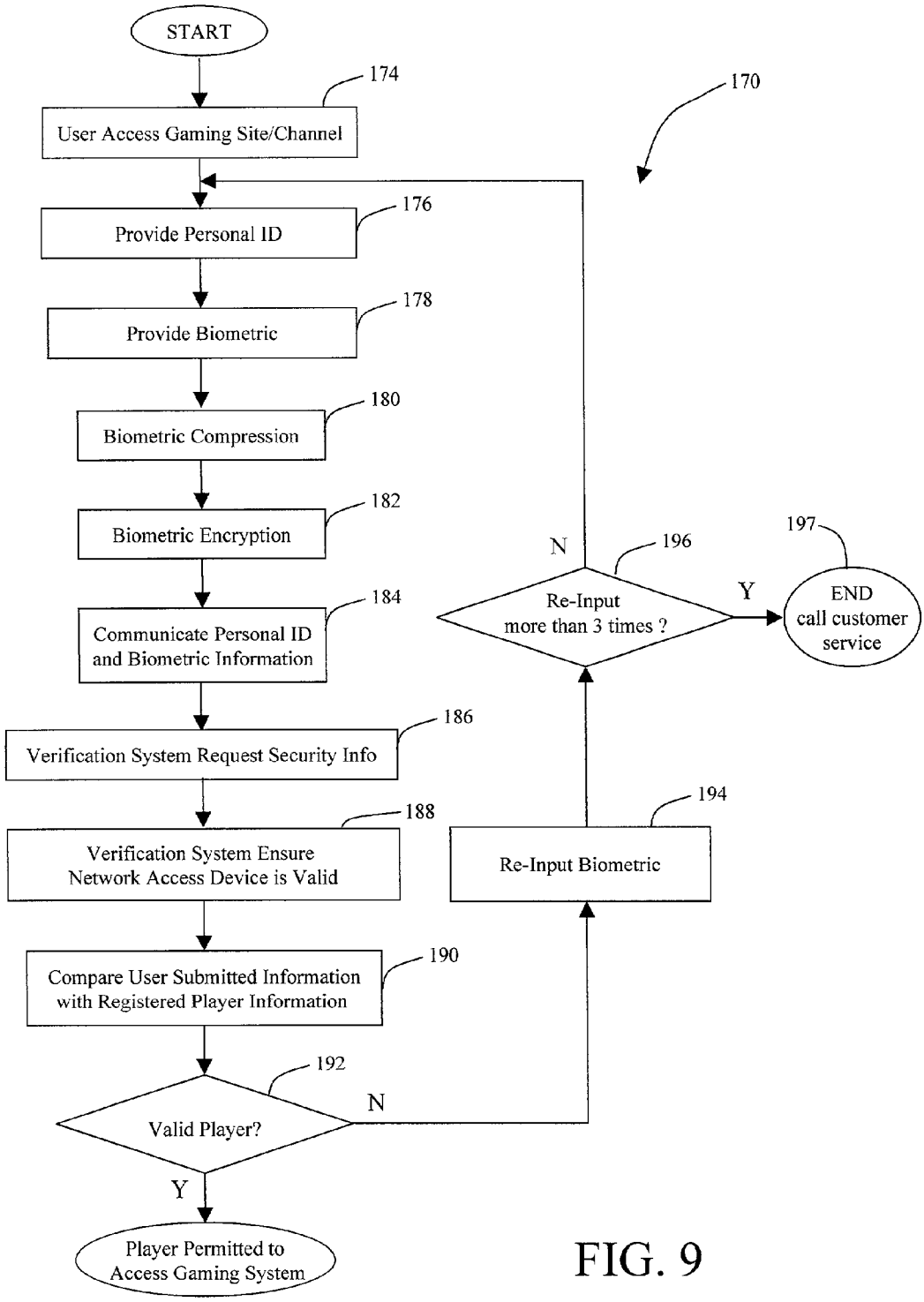

START
174
User Access Gaming Site/Channel
170
176
Provide Personal ID
178
Provide Biometric
180
Biometric Compression
182
Biometric Encryption
184
Communicate Personal ID and Biometric Information
186
Verification System Request Security Info
188
Verification System Ensure Network Access Device is Valid
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

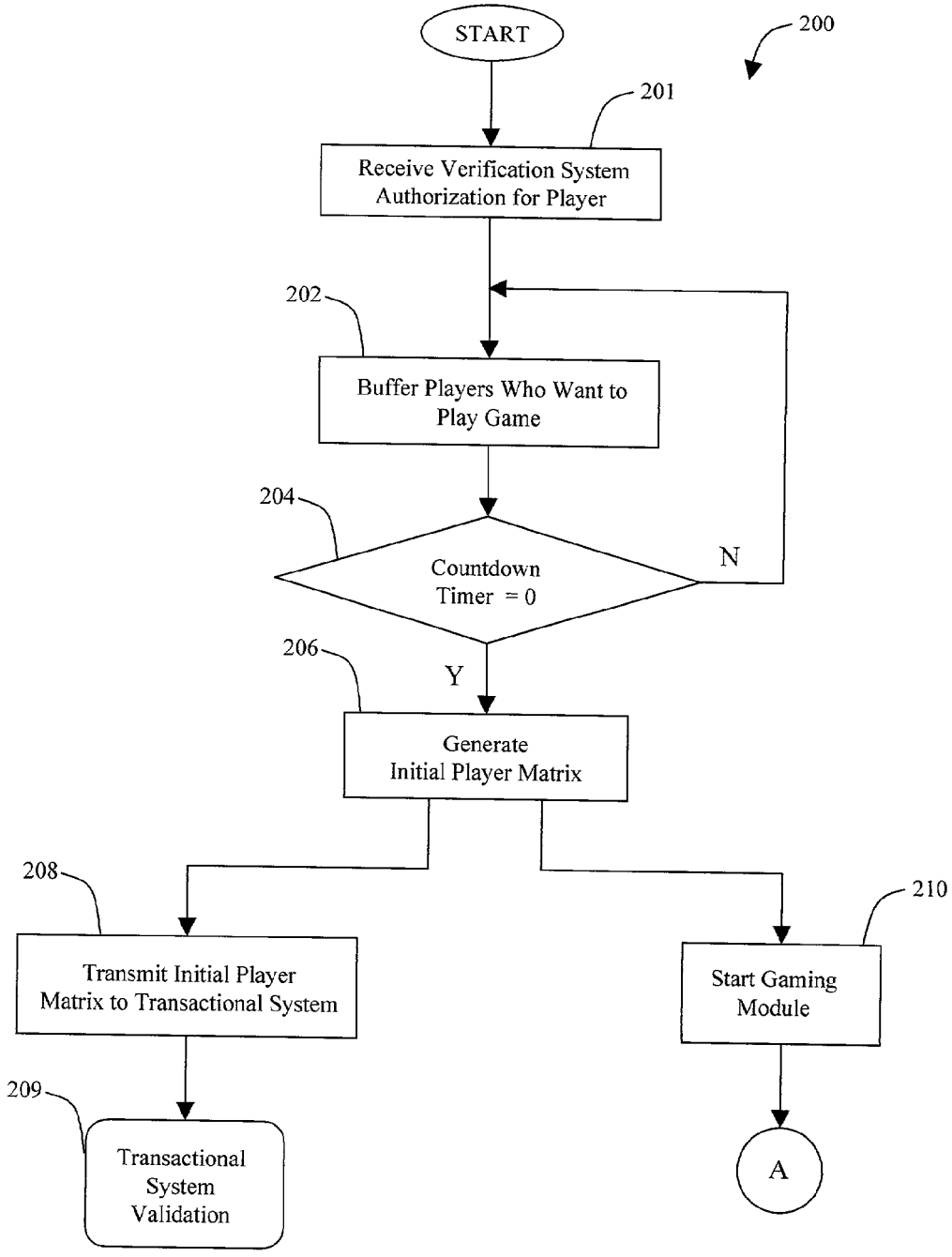

START
200
201
Receive Verification System Authorization for Player
202
Buffer Players Who Want to Play Game
204
Countdown Timer = 0
N
Y
206
Generate Initial Player Matrix
208
Transmit Initial Player Matrix to Transactional System
209
Transactional System Validation
210
Start Gaming Module
A

FIG. 10

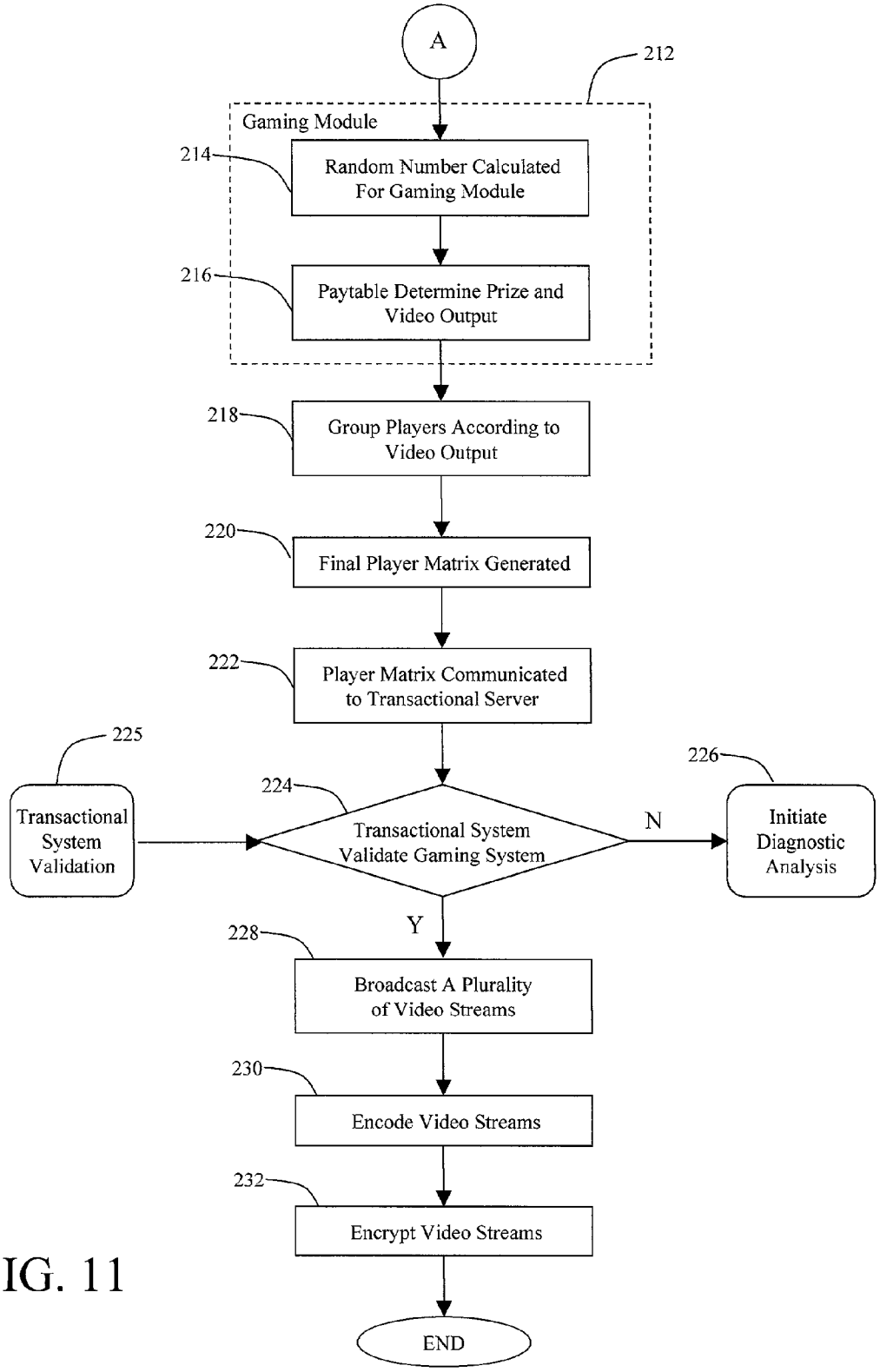

A
212
Gaming Module
214
Random Number Calculated For Gaming Module
216
Paytable Determine Prize and Video Output
218
Group Players According to Video Output
220
Final Player Matrix Generated
222
Player Matrix Communicated to Transactional Server
225
Transactional System Validation
224
Transactional System 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

BIOMETRIC BROADBAND GAMING SYSTEM AND METHOD

CROSS REFERENCES TO RELATED APPLICATIONS

[0001] This patent application is a continuation-in-part of provisional patent application 60/266,856 filed on Feb. 6, 2001.

BACKGROUND OF THE INVENTION

[0002] 1. Field of Invention

[0003] The present invention is a biometric broadband interactive gaming system and method. More particularly, the biometric broadband interactive gaming system and method operates in a networked environment which interfaces with a plurality of network access devices including personal computers, wireless devices, and interactive set-top boxes.

[0004] 2. Description of Related Art

[0005] The related art includes gaming devices, on-line gaming, networked interactive gaming, and biometrics.

[0006] Gaming Devices

[0007] 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.

[0008] Games of skill comprises 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.

[0009] On-Line Gaming

[0010] 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.

[0011] 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, the control of gambling addiction, and ensure on-line gaming is secure and reliable.

[0012] 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 on-line gaming is secure and reliable, prior art system 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 method do not ensure that the individual accessing the on-line game is a valid user.

[0013] In view of the prior art systems, a minor or other unauthorized individual may 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 simply identifying the web site's naming convention for the player. The player password can be easily determined by simply 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 and 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.

[0014] 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, is simple to implement, prevents gambling addiction, and provides a higher degree of security and reliability from unauthorized users.

[0015] Networked Interactive Gaming

[0016] 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.

[0017] 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.

[0018] 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.

[0019] Biometrics

[0020] 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.

[0021] Biometric applications for games of skill and games of chance are limited. For example biometric gaming applications are taught in U.S. Pat. 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. Patent 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 finger print imaging device, and retinal scans for verifying a player's identity.

[0022] 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 are not known.

SUMMARY OF INVENTION

[0023] 1. Advantages of the Invention

[0024] One of the advantages of the present invention is that it provides a secure and reliable on-line gaming system and method.

[0025] A further advantage of the present invention is that it provides a secure system and method for identifying a user in an open network environment.

[0026] A further advantage of the present invention is that it provides a system and method to prevent underage gambling.

[0027] A further advantage of the present invention is that it provides a more secure and reliable and secure gaming system and method.

[0028] 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.

[0029] Another advantage of the present invention is that it permits a plurality of users in a geographically broad area to play the same game.

[0030] A further advantage of the present invention is that it provides a pseudo-real time gaming system and method.

[0031] Another advantage of the present invention is that it simulates a game of chance such as a slot machine in an on-line environment.

[0032] An additional advantage of the present invention is that it provides a networked jackpot.

[0033] 2. Brief Description of the Invention

[0034] The present invention is a networked gaming system that comprises a verification system, a broadband gaming system and a transactional system. 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.

[0035] The present invention comprises a verification system for playing the networked gaming system. 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.

[0036] Additionally, the present invention includes a broadband gaming system which is in communication with the verification system. 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 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 encoders 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 permits an image to be viewed by the network access device.

[0037] Further still the present invention provides a transactional system and method that ensures secure communications occur in the verification system and the broadband

gaming system. 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.

[0038] 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

[0039] Preferred embodiments of the present invention are shown in the accompanying drawings wherein:

[0040] **FIG. 1***a* through **FIG. 1***d* provide diagrams of a plurality of network access devices.

[0041] **FIG. 2** is a high level diagram of a gaming system networked to a plurality of network access devices.

[0042] **FIG. 3** is a block diagram of an illustrative biometric input module.

[0043] **FIG. 4** is a block diagram of a gaming system configured to receive a biometric input from a network access device.

[0044] **FIG. 5** is a table of the data fields in a verification system.

[0045] **FIG. 6** is a table of the data fields in a broadband gaming system and in a transactional system.

[0046] **FIG. 7** is a block diagram of a broadband gaming system.

[0047] **FIG. 8** is a flowchart of the registration method for the gaming system.

[0048] **FIG. 9** is a flowchart of the verification method for the gaming system.

[0049] **FIG. 10** is a flowchart of the gaming method for the gaming system.

[0050] **FIG. 11** is a flowchart of the method for purchasing credits for the gaming system.

[0051] **FIG. 12** is a flowchart of the method for storing credits on the gaming system.

[0052] **FIG. 13** is a flowchart of the information processed by the broadband gaming system.

[0053] **FIG. 14** is a continuation of the **FIG. 13** flowchart.

[0054] **FIG. 15** is a flowchart of the information processed by the transactional system in communication with the broadband gaming system.

DESCRIPTION OF THE PREFERRED EMBODIMENT

[0055] 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 with out departing from the scope of the present invention.

[0056] Network Access Devices

[0057] 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.

[0058] 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.

[0059] 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.

[0060] 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*.

[**0061**] 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 a player with a history of gambling addiction from playing games of chance. 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.

[**0062**] Gaming System

[**0063**] 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.

[**0064**] Verification System

[**0065**] 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 a 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**.

[**0066**] In an alternative embodiment the user identification information is housed in a smart card (not shown) that is 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**.

[**0067**] 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**.

[**0068**] 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.

[**0069**] 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 number. 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.

[0070] 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.

[0071] 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.

[0072] 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.

[0073] Broadband Gaming System

[0074] 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**.

[0075] 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**.

[0076] 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**.

[0077] 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.

[0078] 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**.

[0079] 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**.

[**0080**] 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**.

[**0081**] 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.

[**0082**] 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.

[**0083**] 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.

[**0084**] 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.

[**0085**] Transactional System

[**0086**] 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.

[**0087**] Method For Registering a Player

[**0088**] 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**.

[**0089**] 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**.

[**0090**] 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 the proceeds to block **156**.

[**0091**] 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**.

[**0092**] 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**.

[**0093**] At block **160**, the biometric input is compressed and encrypted. It is preferable for certain biometric inputs to compressed such as fingerprint scans, retinal scans and other such scanning techniques. Other biometric inputs such as voice patterns, 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.

[**0094**] 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**.

[**0095**] 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.

[**0096**] 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.

[0097] Method for Player Verification

[0098] 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**.

[0099] 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**.

[0100] 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.

[0101] 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**.

[0102] 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**.

[0103] 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.

[0104] 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**.

[0105] Method for Operation of Broadband Gaming System

[0106] 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**.

[0107] 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**.

[0108] 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 games is closed because the period during which the game is open has expired, then the method proceeds to block **206**.

[0109] 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.

[0110] 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.

[0111] 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 prove 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**.

[0112] 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**.

[0113] 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 trans-

actional system as described in block **222**. The method then proceeds to decision diamond **224**.

[**0114**] 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 proceed to process block **226**, which initiates diagnostic procedures. If the random numbers match, then the method proceeds to block **228**.

[**0115**] 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**.

[**0116**] 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**.

[**0117**] 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.

[**0118**] 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.

[**0119**] An Illustrative Game

[**0120**] 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.

[**0121**] 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.

[**0122**] A more concrete example includes having a player select a plurality of numbers, such as the numbers below:

23	35	8	15	42

[**0123**] 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

[**0124**] The paytable module is then programmed to interpret the random numbers generating by the gaming module according to the following illustrative rules:

[**0125**] 1. If a match between one number is achieved, then a prize of 1× 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.

[**0126**] 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.

[**0127**] 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.

[**0128**] 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.

[**0129**] 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.

Conclusion

[**0130**] It can now be seen that the present invention solves many of the problems associated with the prior art. The present invention provides a verification system that uses

biometrics to identify the player. The present invention provides a broadband gaming system that communicates with a plurality of different network access devices. Furthermore, the present invention provides a system and method for generating a combined jackpot in an open network environment across a broad geographical area.

[0131] Although the description above contains many specifications, these should not be construed as limiting the scope of the invention but as merely providing illustrations of some of the presently preferred embodiments of this invention. The specification, for instance, makes reference to bonus prizes. However, the present invention is not intended to be limited to bonus prizes. Rather it is intended that the present invention can be used independently as a stand-alone game. Thus, 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, comprising;

a verification system in communication with a network, said verification system configured to receive a user biometric and compare said user biometric to a plurality of registered player biometrics;

a broadband gaming module that is enabled when said user biometric matches one of said plurality of registered players, said gaming module configured to provide a game that is played by said registered player; and

a transactional system in communication with said verification system and said broadband gaming module, said transactional system configured to monitor transactions conducted by said verification system and said broadband gaming system.

2. The gaming system of claim 1 wherein said verification system is in communication with a network access device operatively coupled to a network, said network access device having a biometric input module configured to receive said user biometric.

3. The gaming system of claim 1 wherein said broadband gaming system is configured to communicate with a first network access devices having a first protocol and a second network device having a second protocol.

4. The gaming system of claim 3 wherein said first protocol is an IP communications protocol.

5. The gaming system of claim 3 wherein said first protocol is an MPEG communications protocol.

6. The gaming system of claim 3 wherein said first protocol is an IP communications protocol and said second protocol is an MPEG communications protocol.

7. A gaming system, comprising;

a verification system configured to communication with a network, said verification system configured to receive a user biometric and compare said user biometric to a plurality of registered player biometrics; and

a gaming module that is enabled when said user biometric matches one of said plurality of registered players, said gaming module including a random number generator that is used to determine whether a prize is awarded to a player.

8. The gaming system of claim 7 wherein said verification system is configured to communicate with a network access device having a biometric input module that receives said user biometric.

9. The gaming system of claim 7 wherein said gaming module is resident in a broadband gaming system, said broadband gaming system configured to communicate with a plurality of network access devices.

10. The gaming system of claim 9 wherein at least one of said plurality of network access devices comprises a biometric input module.

11. The gaming system of claim 7 further comprising a paytable module in communication with said random number generator, said paytable module configured to determine whether said player is awarded said prize.

12. The gaming system of claim 11 further comprising a memory module in communications with said paytable module, said memory module configured to store a plurality of images that are displayed on said plurality of network access devices.

13. A gaming method, comprising:

providing a network that permits communications between a network access device and a gaming system;

inputting a user biometric into said network access device;

comparing said user biometric to a plurality of registered player biometrics;

permitting a player access to a game when said user biometric matches one of said plurality of registered player biometrics;

playing said game; and

viewing results from said game on said network access device.

14. The method of claim 13 further comprising causing said user biometric to be communicated from said network access device to a verification system, said verification system comparing said user biometric to said plurality of registered player biometrics.

15. The method of claim 13 further comprising comparing said user biometric to one of said plurality of registered player biometrics at said network access device.

16. The method of claim 14 further comprising requesting a personal identification code from a user that is providing said user biometric and using said personal identification code to identify said registered player biometric.

17. The method of claim 13 further comprising permitting a plurality of registered players to access said game when a plurality of users submit a plurality of user biometrics that identify said plurality of users as said plurality of registered players.

18. The method of claim 13 wherein playing said game comprises generating at least one random number.

19. The method of claim 18 further comprising determining whether a prize is awarded to said player based on said at least one random number.

20. The method of claim 19 further comprising generating a plurality of images that communicate said prize awarded to said player.

* * * * *