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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 November 2004 (04.11.2004)

PCT

(10) International Publication Number
WO 2004/095318 A1

(51) International Patent Classification^7: G06F 17/30

(21) International Application Number: PCT/US2004/011863

(22) International Filing Date: 16 April 2004 (16.04.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/417,689 16 April 2003 (16.04.2003) US

(71) Applicant and
(72) Inventor: ACKERMAN, David [US/US]; 9590 Chesapeake Drive, Suite 116, San Diego, CA 92123 (US).

(74) Agent: KING, Michael; 268 North, 980 East, Lindon, UT 84042 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

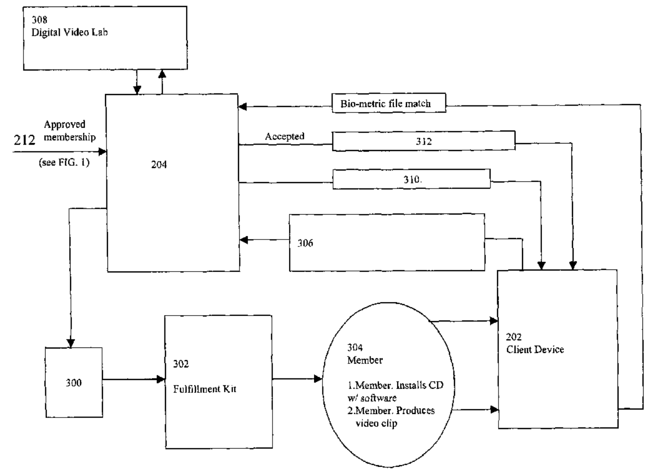
— *as to the identity of the inventor (Rule 4.17(i)) for all designations*
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for all designations*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*
— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: AN INTERNET SYSTEM FOR AUTHENTICATING MEMBERSHIP PROFILE INFORMATION



(57) Abstract: A system for verifying, authenticating, and processing membership information to generate a selectively approved searchable membership database, viewable through a computer information network, such as the internet. Membership verification includes a first processing unit (200) for transmitting data to a second processing unit (204) for verifying the information with a third party (212). A digital video lab (308) processes raw audio and video data provided by a member (304) to create a biometric file for authentication and to identify unique biometric identifiers on the raw audio and video data to create a searchable member profile. Upon member logon, each member passes biometric authentication via retinal scan, voice recognition, or the like. An interface module (120) may be used to record and deliver selected video on demand, live video, and display the video/audio files indexed with the biometric identifiers. A bandwidth scheduling module (130) improves video quality and a calendaring module creates and stores audit logs to improve member accountability and content control.

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

AN INTERNET SYSTEM FOR AUTHENTICATING MEMBERSHIP PROFILE INFORMATION

[0001] This application claims the benefit of U.S. Patent Application No. 10/417,689, filed April 16, 2003 at the United States Patent and Trademark Office, and is incorporated by reference as if fully set forth herein.

FIELD OF THE INVENTION

[0002] The present invention relates a system for verifying, authenticating, and processing membership information to generate a selectively approved searchable membership database viewable through a computer information network. More specifically, this invention relates to a system for verifying and authenticating the members to create a selectively approved populated membership database for presenting specific profiles to other members and for allowing members to virtually meet over the internet.

BACKGROUND OF THE INVENTION

[0003] Online dating services have been in operation for several years. People interested in meeting others have often found conventional online dating to be both rewarding and entertaining. Online dating services have become more and more popular and necessary in this day by the demographic and cultural changes, which make it difficult for likeminded people to meet.

[0004] Some conventional systems take advantage of telephone technology to aid in this process. In these systems, which typically involve the placement of personal ads or profiles on publication, a person wishing to meet another person must make a telephone call and listen to a prerecorded message left by another member of the service.

A disadvantage of this service is that the member can only listen to messages and there are no visual aids to assist in the process. Furthermore, in most prior telephone systems, when the member has found a person they would like to meet, they may leave a message with that person. That person may then reply to the message. In reality, these telephone-dating services are little more than voice mail systems with some additional features.

[0005] Other systems have sprouted on the World Wide Web ("the web"). In order to join an existing dating service on the Web, an applicant simply visits the website where she is prompted to enter personal information such as age, height, weight, hair color, eye color, and build, as well as geographic information, hobbies and other preferences. The applicant then becomes a member of the dating service, sometimes with a fee, and may receive and send contact information to and from other members of the service.

[0006] Unfortunately, because the web is largely unregulated, as well as the information provided to the on-line dating services, there is no assurance that all the information entered by the member is accurate or reliable. Current internet services omit large amounts of social and legal information, leaving the member compromised with guess work, no personality information, no validity of currency of photo images, no legal identity, and alias information may affect candidate verification. As a result, the member may not really be who or what she claims to be. In addition, it is possible to enroll people with the service, without their knowledge or permission, as a joke for example.

[0007] Another disadvantage with current online dating services is that anybody can access the website using another member's password, regardless of whether or not the member obtained permission to use the first member's password. The other subscribers to the service may be completely unaware that they are not communicating with the person the profile was created to represent.

[0008] Yet another disadvantage of current online dating services is that the use of video dating, or viewing others in real-time, has resulted in uncontrolled porn social environments. There is very little accountability over offensive content flashed across the screen of an unsuspecting member.

[0009] Finally, the current system of viewing video of potential dates is very time consuming and inefficient, possibly taking weeks before a meeting can occur. In such cases, a person is required to go to a designated location and search through videos in order to find a particular person. A simple way of advancing through video to find particular characteristics of a potential date is limited by the technology used; current video dating services use videocassettes as a way of showing a member to another member. This process is time consuming because once a member discovers another whom she is interested in meeting, the dating service sends a postcard or notification to the individual notifying him that another member would like to meet him. He then must go to the same location and view the other member's video profile. If he decides that he would like to meet her, the office sends a postcard to her notifying her. This process could take weeks.

[0010] Another disadvantage of current online dating services is that they have not made good use of current technology and the power of the web. Specifically, current services have not effectively made member video profiles available to the other members of the service. For those services that provide access to videos, there is not an efficient system for searching the videos to present to the members.

[0011] Finally, another disadvantage of online dating services is that the content shared between members during instant messaging or video dating is unregulated. Often times, unsuspecting video daters are suddenly presented with nudity, abusive language, and perverse actions by other members and are left without recourse.

[0012] Thus, people realize that there is a need to assure the integrity of the information presented and the integrity of service. There is a need to assure that the information represented by the member is true and accurate. There is a further need to provide better safety and security to the members of the service. Finally, there is a need to use advanced web video and audio technology to facilitate on-line communication and dating, and to control the content presented between online video daters.

SUMMARY OF THE INVENTION

[0013] The various elements of the present invention have been developed in response to the present state of the art, and in particular, in response to the problems and needs in the art that have not yet been fully solved by current systems for allowing individuals to meet over the web. Accordingly, the present invention provides a system that uses current web technology for allowing individuals to safely meet over the web.

[0014] More specifically, the present invention provides a system for verifying specific profile, legal, and social data responses for generating a selectively approved membership database, for biometrically authenticating member user, for creating a consenting digital signature and biometric file to control content shared during a virtual meeting, and for improving video communications during a virtual meeting. Membership verification includes a first processing unit (200) for transmitting data to a second processing unit (204) to verify the data through a verification module (100) with a third party (212). A digital video lab (308) processes raw audio and video data provided by a member (304) to create a biometric file for authenticating the member through an authentication module (110) and to identify unique biometric identifiers on the audio/video data to create a searchable member profile. Upon member logon, the member (304) passes biometric security authentication via retinal scan, voice recognition, or the like. An interface module (120) may be used to record and deliver selected video on demand, live video, and display the video/audio files indexed with the biometric identifiers. A bandwidth scheduling module (130) provides improved video quality and creates and stores audit logs to improve member accountability and content control.

[0015] It is therefore one feature of the present invention to ensure that a profile created by a member (304) is true and accurate through a verification process. Another feature of the present invention assures that the member represented by the profile is the actual member using the service through an authentication process.

[0016] Another feature of the present invention provides a database search capability with audio/video files indexed by unique biometric identifiers to enable member access to the audio/video files.

[0017] It is another feature of the present invention to create a system for controlling live video content through mutual consent approvals and consenting biometric files. Another feature of the present invention improves video quality through managing bandwidth

[0018] Reference throughout this specification to features, advantages, or similar language does not imply that all of the features and advantages that may be realized with the present invention should be, or are, in any single embodiment of the invention. Rather, language referring to the features and advantages is understood to mean that a specific feature, advantage, or characteristic described in connection with an embodiment is included in at least one embodiment of the present invention. Thus, discussion of the features and advantages, and similar language, throughout this specification may, but do not necessarily, refer to the same embodiment.

[0019] Furthermore, the described features, advantages, and characteristics of the invention may be combined in any suitable manner in one or more embodiments. One skilled in the relevant art will recognize that the invention can be practiced without one or more of the specific features or advantages of a particular embodiment. In other instances, additional features and advantages may be recognized in certain embodiments that may not be present in all embodiments of the invention.

[0020] These features and advantages of the present invention will become more fully apparent from the following description and appended claims, or may be learned by the practice of the invention as set forth hereinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] In order for the advantages of the invention to be readily understood, a more particular description of the invention briefly described above will be rendered by reference to specific embodiments thereof, which are illustrated in the appended drawings. Understanding that these drawings depict only typical embodiments of the invention and are not therefore to be considered to be limiting of its scope, the invention will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

[0022] FIG. 1 illustrates a simplified block diagram for verifying membership identity, authenticating members, creating member profiles, and establishing a virtual meeting according to one embodiment of the present invention;

[0023] FIG. 2 illustrates a simplified block diagram for verifying member identity according to one embodiment of the present invention;

[0024] FIG. 3 illustrates a simplified block diagram for authenticating member identity according to one embodiment of the present invention;

[0025] FIG. 4 illustrates a simplified diagram for creating a biometric authentication file according to one embodiment of the present invention;

[0026] FIG. 5 illustrates a simplified diagram of a digital video lab according to one embodiment of the present invention;

[0027] FIG. 6 illustrates a simplified block diagram of an interactive multimedia player for searching database information according to one embodiment of the present invention;

[0028] FIG. 7 illustrates a system for establishing a virtual meeting between members according to one embodiment of the present invention; and

[0029] FIG. 8 illustrates a bandwidth schedule and calendaring system according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0030] Reference throughout this specification to "one embodiment," "an embodiment," or similar language means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, appearances of the phrases "in one embodiment," "in an embodiment," and similar language throughout this specification may, but do not necessarily, all refer to the same embodiment.

[0031] Furthermore, the described features, structures, or characteristics of the invention may be combined in any suitable manner in one or more embodiments. One skilled in the relevant art will recognize, however, that the invention can be practiced without one or more of the specific details, or with other methods, components, materials, and so forth. In other instances, well-known structures, materials, or operations are not shown or described in detail to avoid obscuring aspects of the invention.

[0032] **FIG. 1** illustrates a simplified block diagram of a system for verifying membership identity, authenticating members, creating and searching member profiles, and establishing a virtual meeting according to one embodiment of the present invention. In this embodiment, the system comprises a membership identity verification module (100) to verify an applicant's credibility and to determine the applicant's character, an authentication module (110) for authenticating a member, an interface module (120) for searching a database and presenting search results, and a virtual meeting module (130) for establishing a meeting between at least two members.

[0033] In one embodiment, the verification module (100) requests personal information from an applicant for establishing a database of members that meet predetermined qualifications. In operation, the applicant inputs (101) specific applicant information, such as the applicant's drivers license number, social security number, credit card information, etc, into a processing unit, such as a computer. A server, or processing unit, collects the applicant information and compares or matches the applicant information with information obtained from a third party (102). If the verification module (100) deems the applicant information accurate or if the verification module (100) deems the character of the applicant acceptable, applicant access is granted (103) and the applicant becomes a member of the selectively approved database ("database").

[0034] After being verified, the authentication module (110) authenticates the member before granting access to the database. The authentication module (110) helps ensure that the person using the system is the person represented by the member profile stored on the database. The authentication module (110) utilizes biometric data to authenticate the member. In one embodiment, the biometric data is obtained directly from raw data obtained from the member, i.e., audio and video files created (111) by the member and transmitted to the server. Portions of the raw data are processed and a biometric file is created (112). At the same time, the raw data is processed and tagged (113) with biometric identifiers to identify particular characteristics of the new member. The member's profile is updated with tagged video and audio content and posted (114) to the database.

[0035] After the member has been verified, the biometric file created, and video and audio tagged, the member may use the interface module to search the database for other members matching preferential characteristics. Using the interface module, the member may search the video and audio database by inputting preferred characteristics (121) of other members. The server searches the database (122) for identifying audio and video files that match the preferred specific characteristics. A list of members with video and audio files matching the preferential characteristics is presented to the member, who may then view the video and audio files (123).

[0036] Once the member finds at least a second member matching the preferred specific characteristics the member may request a virtual meeting (131) with the second member through the virtual meeting module (130). A virtual meeting is a live audio and/or videoconference between at least two members of the database. In operation, a first member sends a request for a virtual meeting (131) with a date and time to the second member and the second member may accept or reject the virtual meeting request (132). If the second member accepts the date and time, the selected date and time, the members are connected via an internet connection and the virtual meeting begins (133).

[0037] FIG. 2 illustrates a system for verifying member identity according to one embodiment of the present invention. In this embodiment, the applicant 200 establishes a connection between a client device (202) and the server (204). In one embodiment, the connection is a Secure Socket Layer ("SSL") for improved security. The client device (202) may be a personal computer, a set-top box, an internet-enabled television set, or an internet-enabled wireless communications device, such as a handheld device or a cell phone. One skilled in the art will recognize that there may be many other devices that may be used for this system, including new technology as the current technology evolves.

[0038] The applicant (200) inputs personal information, such as the applicant's name, address, social security number, driver's license number, etc., through a sign on screen (206) on a website, which is transmitted to an identification process controller (208) of the server (204). In one embodiment, the server (204) composes (210) an XML query transmitted via HTTPS to a third party (212) through a secure dedicated electronic frame relay circuit, or other conventional secured wide area network approved communications link. The information may be transmitted to a credit bureau, a government agency, or other organization. In response to the transmission, the third party (212) transmits the third party information corresponding to the applicant information back to the identification process controller (208) of the server (204). For example, the third party (212) communicates the third party's recorded information relating to the applicant's drivers license number, social security number, credit report, credit score, arrest history, marriage information, etc to the identification process controller (208) of the server (204). In one embodiment, the third party (212) transmits an HTTPS response containing the third party information via SSL to the identification process controller (208) of the server (204) where the identification process controller (208) of the server (204) compares the third party information with information provided by the applicant (200).

[0039] The identification process controller (208) analyzes the third party information results to determine if the data provided by the applicant (200) was sufficiently accurate to be considered for membership. In one embodiment, the information is independently compiled and scored and the scores are added together to determine whether the applicant (200) receives a passing or failing score based on a predetermined numeric scale. For example, an applicant (200) with a credit score over 700 may receive ten points, while an applicant (200) with a credit score under 700 points may only receive five points. Similarly, an applicant (200) with a college degree may receive twenty points while an applicant (200) without a college degree may only receive five points.

[0040] In one embodiment, the identification process controller (208) of the server (204) utilizes an algorithm (mathematical formula criteria measurements) for approval or failure qualification. For example, the algorithm is configured to score information based on whether the applicant (200) included his full legal name, correct social security number, correct address, etc. Additionally, the algorithm may be configured to score information based on whether the applicant name, social security number, address, marital status, driver license, and credit card numbers from the third party (212) match the information that was transmitted to the server (204). In one embodiment, the matching information may then be scored, as discussed above.

[0041] In another embodiment, for approval or rejection, other factors may be considered, such as, for example, the applicant's full legal name must match exactly that of the legal owner of the social security number; the first initial and last name must match exactly to the owner of the driver's license (state obtained from address); the address must match exactly that of the owner of the credit card account; the last name and address must match exactly to the owner of the credit card account; the applicant (200) must stipulate that they are unmarried; the credit card purchase must be authorized.

[0042] In another embodiment, the applicant (200) transmits only a portion of the social security number. For example, only the first five digits of the social security number is submitted, or the last four digits. No matter how many digits are submitted, the digits may still be matched and compared. For approval, the input information must correlate to the driver's license number, the credit card, the phone number, and the address records. This option might be a solution for an applicant (200) who prefers not to give social security numbers.

[0043] In another embodiment, the system is configured to compile the applicant's character report to determine the applicant's character. Information such as aliases, judgments, lawsuits, marriage licenses, divorce decrees, physical address history, telephone number history, occupants of same address by male/female comparison, names of relatives, roommates, neighbors, bankruptcy filings, tax Liens, civil judgments, real property ownership, divorce records, identify theft report information, criminal background, county listing of record, arrest file, disposition date of sentence, national media service information, newspapers, magazines, and newswire files and other public social and demographic information available through public records may be requested and obtained from a variety of sources. As discussed above, such information may be valued, scored, and/or matched to a scaled measurement of acceptable criteria and added up to a sum result. As an example, a score of 1000 may be acceptable for approval, while a scale of less than 1000 may be unacceptable. Additionally, an applicant's bankruptcy history may not preclude the applicant (200) from membership; however, a criminal record may, depending on the degree. An applicant (200) with a combination of bankruptcy, tax liens, and civil judgments may be precluded if the sum value of the information is greater than a predetermined maximum.

[0044] If all input information matches, and the values of the information meet the predetermined requirements, approval is granted 214. If, however, at least one item does not match or that the value of the scaled information is deficient, approval may be denied and the applicant (200) may be notified as an automated response in the application process. For the applicant (200) who has been approved, the applicant's credit card information is transmitted to a credit approval agency (216), such as a credit card company. If the credit approval agency denies payment, the applicant (200) may be notified either immediately through a "Sorry" screen (218) or through the applicant's email account. If payment and identification are approved, the applicant (200) becomes a member (304) (See FIG. 3) and the server (204) posts (218) the member's profile to the database (220), and sends notification to mail (222) a membership fulfillment kit (302) to the member (304).

[0045] **FIG. 3** illustrates a simplified block diagram for authenticating member identity according to one embodiment of the present invention. Upon membership verification, the server (204) prepares an order processing report (301) to mail the membership fulfillment kit (302) to the member (304). The membership fulfillment kit (302) may contain a digital web cam, a compact disc ("CD") containing interface software, a serial number, a member password, authentication software (biometric software), video conferencing software, a microphone, and a custom backdrop for video imagery and production. In another embodiment, the software and password of the fulfillment kit (302) may be downloaded from the server (204). The member (304) installs the software onto the client device (202). The member (304) may use the password for an initial connection to the server (204).

[0046] After the fulfillment kit (302) has been received, the member (304) creates a video or photography file and an audio file ("raw data") that uniquely identifies the member's physical image and audio. For example, the member (304) may use the web camera, digital video device, digital camera, or other recording means to record visual and audio representations of the member (304), such as physical appearance, personal belongings, hobbies, etc. Additionally, the member (304) may recite a scripted phrase which may be used to create a biometric file. The biometric file, for member authentication purposes, is a sample of audio/video of the member (304), which has been processed to turn digitized time dependent signals into wavelength/amplitudes, on a certain number of words and/or frames of video, and storing them in the database. The biometric file is configured to serve as an additional security feature.

[0047] The raw data, including the scripted phrase, is loaded onto the client device (202) and subsequently transmitted (306) to the server (204). The raw data may be transmitted automatically to the server (204) when the interface is launched, or on member (304) command. The server (204) captures the raw data, which is processed and tagged for biometric identifiers ("biotags") at a digital video/audio lab. A digital video lab (308), or profile creation module, processes, identifies, and tags unique digital video and audio data from the raw data produced by the member (304) and processes the scripted phrase to create a biometric file. Biotags are unique tracks previously identified and rendered in processing that are correlated and matched with unique identifiers such that SQL or XML queries may quickly and efficiently fetch the requested information.

[0048] In one embodiment, the digital video lab (308) may create a new biometric file from the raw data transmitted (306) from the client device (202). Accordingly, the biometric file may be the recited phrase, or it may be other audio or video data, including video frames, such as digital photographs.

[0049] In one embodiment, the serial number of the installation software may be transmitted back to the server (204) with the raw data as an additional security feature. If the transmitted serial number matches (310) the serial number corresponding to the member profile stored in the system, the server (204) transmits the biometric file (312) created at the digital video lab (308) to the client device (202). In one embodiment, the biometric file (312) may be transmitted embedded in the biometric software. The biometric file may be encrypted. The software installed on the member's client device (202) decrypts and stores the biometric file on the client device (202).

[0050] In one embodiment, before the member (304) may use the database of members, the member (304) must be authenticated. Live audio/video authentication may be realized using cross correlation to compare the live data with the stored biometric file on the client device (202). The live data and the biometric file may be matched by measuring file sizes, sound frequency, decibel level patterns, time scale speech durations, etc. All elements may be mathematically measured, scored, and scaled generating an acceptance or a denial.

[0051] In another embodiment, authentication may be realized through matching partial file elements with randomly generated multiple key word arrangements. For instance, if a randomly generated multiple key word arrangement processed in the digital video lab (308) is "blue dogs," the server (204) may transmit the phrase "blue dogs" to the client device (202). Upon biometric initiation, the member (304) may be instructed to say "blue dogs" into the microphone. The biometric software on the client device (202) analyzes the member's audio data, or word "blue dogs," according to the methods described above, to accept or deny the member (304) access to the database.

[0052] In another embodiment, half the phrase, or "blue" is transmitted as a biometric file to the biometric software on the client device (202). Upon biometric initiation, after the member (304) speaks the phrase "blue", the phrase data is transmitted over the internet to the server (204) and links to a unique related partial file, in this case, "dogs." The server (204) matches frequency patterns, decibel level patterns, speech time duration, and file sizing calculations and parses, values, and scores the data for granting acceptance or denial.

[0053] Similarly, a digital photography image or video frame, using a custom tagging template or mask, which digitally layers unique objects and shape characteristics isolated within the image, and referenced by color identification of pixel elements using the standard RGB colors spectrum creates a unique custom color chart file for each referenced member (304). As an example, the member (304) may transmit a photo image of herself; a custom mask is digitally layered over the original produced facial image content, the mask highlights and isolates the shape of the eyes, hair, nose, etc., and captures color characteristics. The biometric file may be created by parsing the color information, scaling the color characteristics, and creating a custom color chart for the identified object. A combination of such authentication methods may be used.

[0054] In one embodiment, the server (204) is configured to update the biometric file using revolving random biometric files by periodically transmitting new biometric information to the member's client device (202). For example, the biometric software may be configured to capture random images or audio while the member (304) uses the interface. Specifically, the biometric software may capture a digital photo of the member (304), or an audio segment, every ten minutes and transmit the photo and audio to the server (204) to be stored. The digital video lab (308) may choose one of the photos or audio files to create a new biometric file. The new biometric file may be transmitted at any time to the client device (202) to keep the authentication reliable. The biometric file may also be stored on the server (204) side such that the member's biometric data is transmitted to the server (204) to be compared with the biometric file stored on the server (204).

[0055] FIG. 4 illustrates a simplified diagram for creating a biometric authentication file according to one embodiment of the present invention. In this embodiment, the member (304) installs the member fulfillment kit (302) onto the client device (202). The member (304) initiates the interface software and passes password authentication (400) to push content to launch the interface software (402). The member (304) transmits raw data from the client device (202), which is captured (404) on the server (204). The raw data is processed at the digital video lab (406) to tag the information and to create a biometric file from the raw data. A preliminary member profile is generated (408) and the resulting object stored in the member profile database (410). The member (304) may view his member profile (408) and approve or disapprove and customize the member profile (408).

[0056] To log on, the member (304) opens the interface and enters the password and initiates biometric authentication. Biometric authentication begins when the member (304) recites the scripted audio phrase in the member's recording device, such as the microphone, on the web camera, or both. In this embodiment, the biometric software on the server (204) captures the member audio/video feed, and compares the live audio and/or video, using proven voice and image-processing authentication algorithms. The server (204) may be configured to periodically update the biometric file by capturing and processing new biometric information captured from the member's recording device.

[0057] **FIG. 5** illustrates a simplified diagram of a digital video lab (308) according to one embodiment of the present invention. The digital video lab (308) is used to enhance and improve the customer's image and audio quality after it has been captured and stored in the database, to tag unique member identifiers, and to create the biometric file for authentication, as discussed above.

[0058] After the member (304) has transmitted raw audio/video data (500) to the server (204), the digital video lab (308) creates a preliminary profile (502). The digital video lab (308) performs nonlinear editing, blue screening, creates personal biometric data information rendering unique character references developed from photography images, video and audio track biotags in time code sequences, video and audio encoding, color and audio correction, watermarking, special effects, and encoding, as part of the video production process, and creates the "Sweetheart Finish" with embedded biotags. In one embodiment, the customer may choose which photography images and video and audio clips she would like on her member profile. The member (304) may customize and approve/disapprove of the preliminary profile (504).

[0059] In one embodiment, when the editing, corrections, and biotagging have been completed, the digital video lab (308) may transmit the processed video and audio to a third party video server (506) in a database configured with a search capability indexed by video objects or shapes, photography images, audio track content, and biotags. The member profile library (508) may be stored on the server (204).

[0060] FIG. 6 illustrates a simplified block diagram of the interface (600) for searching database information according to one embodiment of the present invention. As discussed above, the client device (202) may be configured with the interface software to allow the member (304) to search the database (602). In another embodiment the web site comprises the interface (600) configured to process the audio/video aspect, and other controls. The interface (600) may be configured with volume control, a digital audio equalizer, video fast forward, rewind, and play, and incorporates multiple blank fields for entering text data preferences for a membership search. As explained in **FIG. 5**, the digital video lab (308) identifies "biotags" in each member's video and audio profile. For instance, while reviewing the video and audio files, the processors identify and mark all potential member identifiers such as hair color, eye color, physical characteristics, personal belongings, hobbies, activities, etc.

[0061] Members input preferences into preference search fields incorporated into the interface (600). The preferences are transmitted to the database (602) and requested from the server (204). The video and audio data results (604) are transmitted back for the interface (600) to view.

[0062] Accordingly, as an example, a member (304) interested in meeting a second member (not shown) who owns a dog and enjoys hiking and boating can enter those preferences in the player preference search locator and search through the database (602) for video, photography, text and audio matching those preferences. The interface (600) will provide all related photography images, video, text and audio media specified to time code information on the subject requested within the existing entire video clip of each member.

[0063] In another embodiment, the method of using nonlinear video and audio tracks characterizing biotags selected between two points on a timeline can be used to identify particular properties or characteristics of any kind of personal property, for example a home, car, or a boat. Accordingly, a member (304) can transmit raw data files of personal property that he would like to sell. The second member can enter specific preferences of what he would like to buy and specific video clips can be presented for the second member to view and determine if he wants to buy it. This method would be particularly useful in second-hand sales.

[0064] FIG. 7 illustrates a system for establishing a virtual meeting between members according to one embodiment of the present invention. In this embodiment, the system controls live video content between at least the first member (304) and a second member (700) through mutual consent of the members (304) and (700) and creates accountability for those members (304) and (700). The virtual meeting is a two-way, video communication between at least two members.

[0065] In most circumstances, the virtual meeting option arises after a member (304) has reviewed video and/or audio and text profile information about the second member (700) and has a desire to meet the second member (700) virtually over the internet. After the member (304) has identified the second member (700) to meet with he sends a request (704) to a scheduler module of the server (204) indicating whom he would like to meet and at least one date and time for the virtual meeting. At the same time, the member (304) consents and acknowledges to participate in a virtual meeting and to obey pre-established rules of the virtual meeting. The server (204) sends the request for the virtual meeting (706) to the second member (700). The second member (700) has the option of reviewing the first member's profile. If the second member (700) is interested in meeting the first member (304), she can accept (708) the virtual meeting. At the same time, the second member (700) consents and acknowledges to participate in the virtual meeting and to obey the pre-established rules of the virtual meeting. In one embodiment, the response may be sent to the first member (304) with a password (710). The first member (304) may confirm (712) the virtual meeting and time by responding to the second member's response. Upon acceptance, the second member (700) receives a confirmation and a password (714). In another embodiment, once the second member (700) consents to a virtual meeting with the first member (304) a confirmation and password is automatically sent to both members (304) and (700).

[0066] When the agreed upon date and time has arrived, the members (304) and (700) log on and the server (204) notifies each member (304) and (700) that both members (304) and (700) are connected. The members (304) and (700) enter the previously received passwords, read the disclosure agreements, submit digital signature consents, pass biometric authentication, and begin their virtual meeting.

[0067] When a virtual meeting has been created a digital calendar (716) is created, which serves as an audit report of the pre-arranged mutual date. The audit report preserves proof that the members accepted the terms of the agreement. Specifically, the audit report preserves proof of the consenting digital signature, and consenting biometric authentication file preserves proof that the members were in fact the ones who consented to the terms of use.

[0068] In one embodiment, the consenting biometric authentication file is created at the moment the member accepts the terms of the virtual meeting immediately before the start of the virtual meeting. Specifically, when the member points the mouse cursor to the "I Accept" box, the digital video camera, or web cam, takes a picture of the member and the software transmits the photography image, or the video frame, to be authenticated in the same way the member is authenticated for logon. In another embodiment, the member is authenticated with audio authentication, as described above. Upon authentication, the digital signature and consenting biometric file from the web cam is stored as the audit log as proof that the member (304) accepted the terms of the virtual meeting.

[0069] In another embodiment, the virtual meeting begins with a member (304) purchasing virtual meeting minutes. The minutes may be purchased in five, ten, fifteen, half hour, hour, or more, increments. The member (304) discovers the second member (700) and selects a time and date for a virtual meeting. At that point the member (304) is presented with a consent agreement and confirms the agreement with a digital signature or electronic signature, while at the same time, becomes biometrically authenticated through the same process described above for the logon authentication. The audit log is created to file the signatures and the consenting biometric file. Finally a message is sent for a virtual meeting request to the second member (700) and the second member (700) repeats the process. When mutual consent has been recorded in the audit log, the connection is established, the bandwidth is allocated and the members (304) and (700) begin the virtual meeting.

[0070] In another embodiment, both members (304) and (700) may be logged on at the same time and the virtual meeting may be accomplished immediately. For instance, if the two members (304) and (700) are communicating by audio only or by instant messaging, they may request an instant password and if bandwidth is available, the members (304) and (700) may begin the virtual meeting immediately, after consenting to the terms and passing the biometric authentication audit controls, rather than setting up a virtual meeting at some time in the future.

[0071] **FIG. 8** illustrates a bandwidth scheduling system according to one embodiment of the present invention. Virtual meetings take up bandwidth. In order for both the video and the audio to appear clear and to make the virtual meeting enjoyable, a minimum amount of bandwidth is required. When bandwidth is burdened with excessive concurrent use the picture quality, as well as the audio quality, is compromised.

[0072] According to this embodiment, members interested in a virtual meeting may purchase prepaid minutes, for instance, $19.95 for 30 minutes, $29.95 for 60 minutes or $49.95 for 120 minutes, and schedule bandwidth for their virtual meeting, or the members may pay for the minutes as they are used. In this embodiment, a scheduling module is a calendar with a matrix comprising essentially four matrix calendars per time zone; Eastern, Midwest, Mountain, and Pacific. The horizontal columns are bandwidth sectors of 384K. As an example, assuming a service provider purchases bandwidth equivalent to 14 megabits, at 384K bits, there are twenty-six columns, or the ability to allow thirteen concurrent virtual meetings. The rows of the matrix are in minutes, allowing virtual meeting or conferencing in combinations of ten, fifteen, and thirty-minute blocks.

[0073] In operation, the member (304) (See **FIG. 7**) selects a date and time for the virtual meeting and one or more alternate dates and times, and selects the minutes requested for the virtual meeting. The request for the virtual meeting is sent to the scheduling module of the server (204), which checks the queue for time slot availability for two members, or two 384kb slots. If the slot is open the request is sent to the second member (700) (See **FIG. 7**) and the second member (700) responds with either an approval or a denial. If the slot is not available, the scheduling module checks the availability of alternate dates and times. The request is sent to the calendar module if the date and time is approved, which reserves the date and time and a confirmation and password is sent to both members (304) and (700). The server (204) may also send a reminder to the members (304) and (700) before the scheduled time. Once the time block has been reserved, the time and time slot are permanently allocated and prepaid minutes are subtracted from the members' (304) and (700) balance of prepaid minute credits. There may not be refunds, or cancellations.

[0074] It is understood that the above-described arrangements are only illustrative of the application of the principles of the present invention. The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

[0075] Thus, while the present invention has been fully described above with particularity and detail in connection with what is presently deemed to be the most practical and preferred embodiment(s) of the invention, it will be apparent to those of ordinary skill in the art that numerous modifications, including, but not limited to, variations in size, materials, shape, form, function and manner of operation, assembly and use may be made, without departing from the principles and concepts of the invention as set forth in the claims.

What is claimed is:

1. A system for uniting members of a selective database through a global computer information network, comprising:

a first processing unit configured to transmit data relating to a member to a second processing unit;

a verification module configured to verify the data relating to the member;

an authentication module configured to biometrically authenticate the member when the member attempts to use the system;

a profile creation module configured to create a member profile authored from audio, video, and/or photographic data with biometric identifiers transmitted from the member through a processing unit, wherein the biometric identifiers identify characteristics relating to the member;

a searchable database configured to store the member profile;

an interface module configured to allow other members to search the database for the member profile;

a scheduling module configured to schedule a virtual meeting between at least two members to meet over the network at a time acceptable to the members and to virtually separate an amount of bandwidth into virtual sections of bandwidth; and

a calendaring module configured to create and store an audit log to store consenting biometric files and signatures.

2. The system of claim 1, wherein the scheduling module provides a password to the members scheduled to meet over the network such that when the members enter the password they virtually meet over the network through a live broadcast.

3. The system according to claim 12, wherein the authentication module biometrically authenticates the members immediately before the members virtually meet over the network.

4. The system of claim 3, wherein the calendaring module maintains an audit log configured to store a digital signature and a consenting biometric file as proof that the members consented to predetermined terms of meeting over the network, and that the members actually were the members meeting over the network.

5. The system of claim 1, wherein the scheduling module allows a virtual meeting between two members over the network if there are at least two sections of virtual bandwidth, each having a predetermined amount of bandwidth, available at the time of the virtual meeting.

6. The system of claim 5, wherein the scheduling module virtually sections the bandwidth into 384 kilobyte sections.

7. The system of claim 6, wherein the calendaring module schedules a virtual meeting between two members at 15, 30, and 60 minute intervals.

8. A system for allowing a virtual meeting between at least two people, comprising: a scheduling module configured to virtually separate an amount of bandwidth into virtual sections of bandwidth and configured to schedule a virtual meeting between at least two people if there is at least one virtual section of bandwidth available.

9. The system of claim 8, wherein the scheduling module virtually sections the bandwidth into 384 kilobyte sections.

10. The system of claim 8, wherein the calendaring module schedules a virtual meeting between at least two members at 15, 30, and 60 minute intervals.

11. A system for uniting members of a selective database through a global computer information network, comprising:

a first processing unit configured to transmit data relating to a member to a second processing unit;

a verification module configured to verify the data relating to the member; and

an authentication module configured to authenticate the member using a biometric file.

12. The system of claim 11, wherein the first processing unit is a personal computer, a set-top box, an internet-enabled television set, or an internet-enabled wireless device.

13. The system of claim 11, wherein the verification module receives data relating to the member from a third party and matches the data relating to the member, and transmitted from the first processing unit, with data relating to the member transmitted from the third party to verify that the data relating to the member is accurate.

14. The system of claim 13, wherein the verification module assigns a value to the data transmitted to the verification module from the first processing unit and the third party and the system grants the member access to the database if the sum total of the values of the data is equal to, or greater than a predetermined minimum, and denies access if the sum total of the values is less than the predetermined minimum.

15. The system of claim 13, wherein the verification module assigns a value to the data transmitted to the verification module from the first processing unit and the third party and the system grants the member access to the database if the sum total of the values of the data less than a predetermined maximum, and denies access if the sum total of the values is equal to, or greater than the predetermined maximum.

16. The system of claim 11, wherein the biometric file is a video file or a photographic file.

17. The system of claim 11, wherein the biometric file is an audio file.

18. The system of claim 16, wherein the authentication module compares unique color identification or unique object and shape characteristic data obtained from a capture device with the biometric file.

19. The system of claim 17, wherein the authentication module determines a file size, sound frequency, decibel level patterns, or time scale speech durations of live audio data of the member when biometric authentication is initiated, and compares the member's live audio data with one of a file size, sound frequency, decibel level patterns, or time scale speech durations of the biometric file, and the member is granted access if the authentication module determines that at least one, or any combination of the file sizes, sound frequencies, decibel level patterns, or time scale speech durations of the member's live audio data and biometric file substantially match.

20. The system of claim 11, wherein the authentication module is integrated into the first processing unit and the biometric file is stored on the first processing unit.

21. The system of claim 11, wherein the authentication module is integrated into the second processing unit and the biometric file is stored on the second processing unit.

22. The system of claim 11, wherein the biometric file is periodically changed.

23. The system of claim 22, wherein the biometric file is periodically changed with audio, video, or photographic data captured from a capturing device, and wherein the audio, video, or photographic data is captured while the member is connected to the database.

24. A system for creating a database searchable by biometric information, comprising:

a profile creation module configured to create a member profile authored from audio, video, and/or photographic data with biometric identifiers transmitted from the member through a processing unit, wherein the biometric identifiers identify characteristics relating to the member;

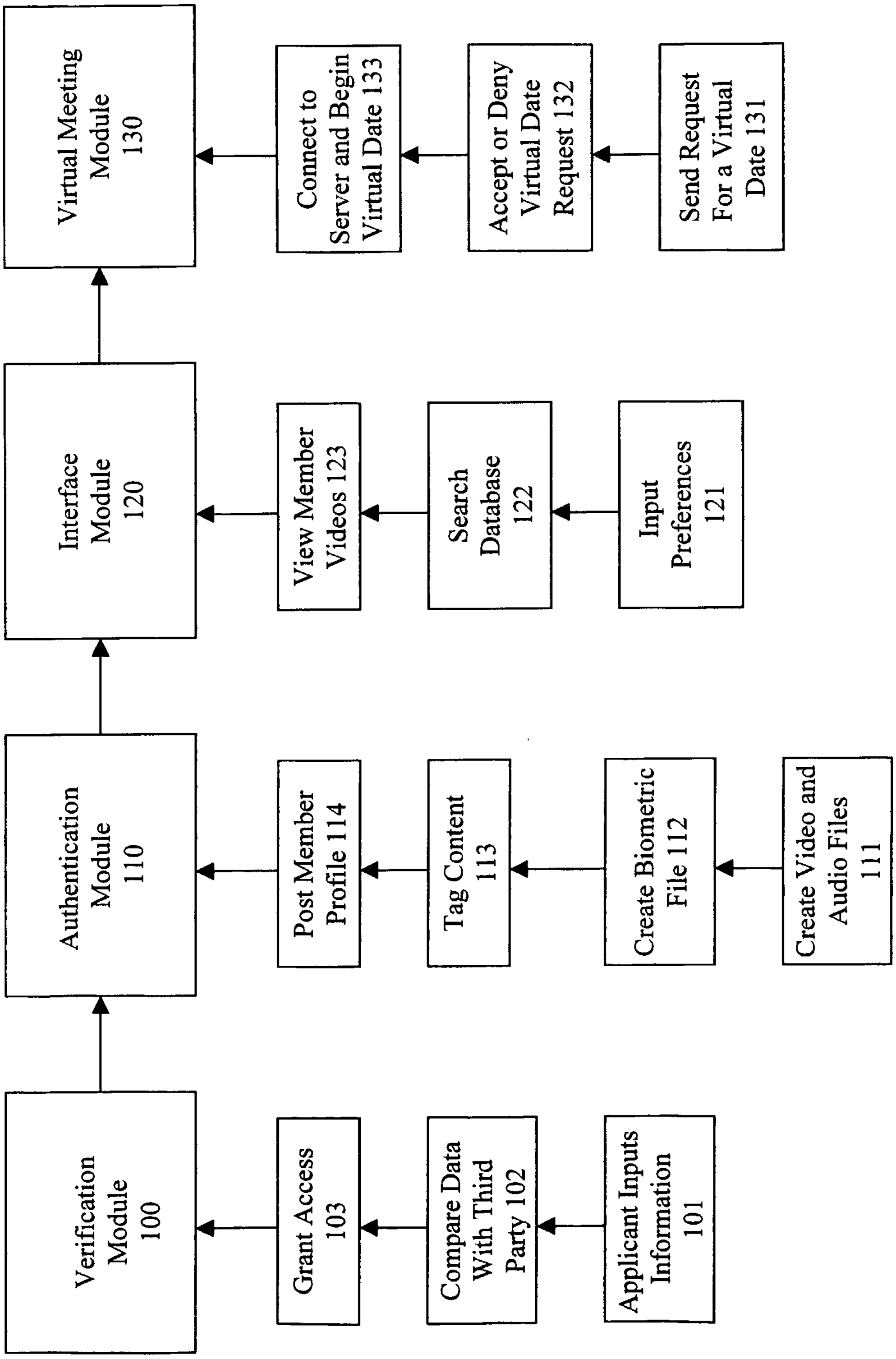
a searchable database configured to store the member profile; and

an interface module configured to allow other members to search the database for the member profile.

25. The system of claim 24, wherein the biometric identifiers are configured to identify the member's physical characteristics.

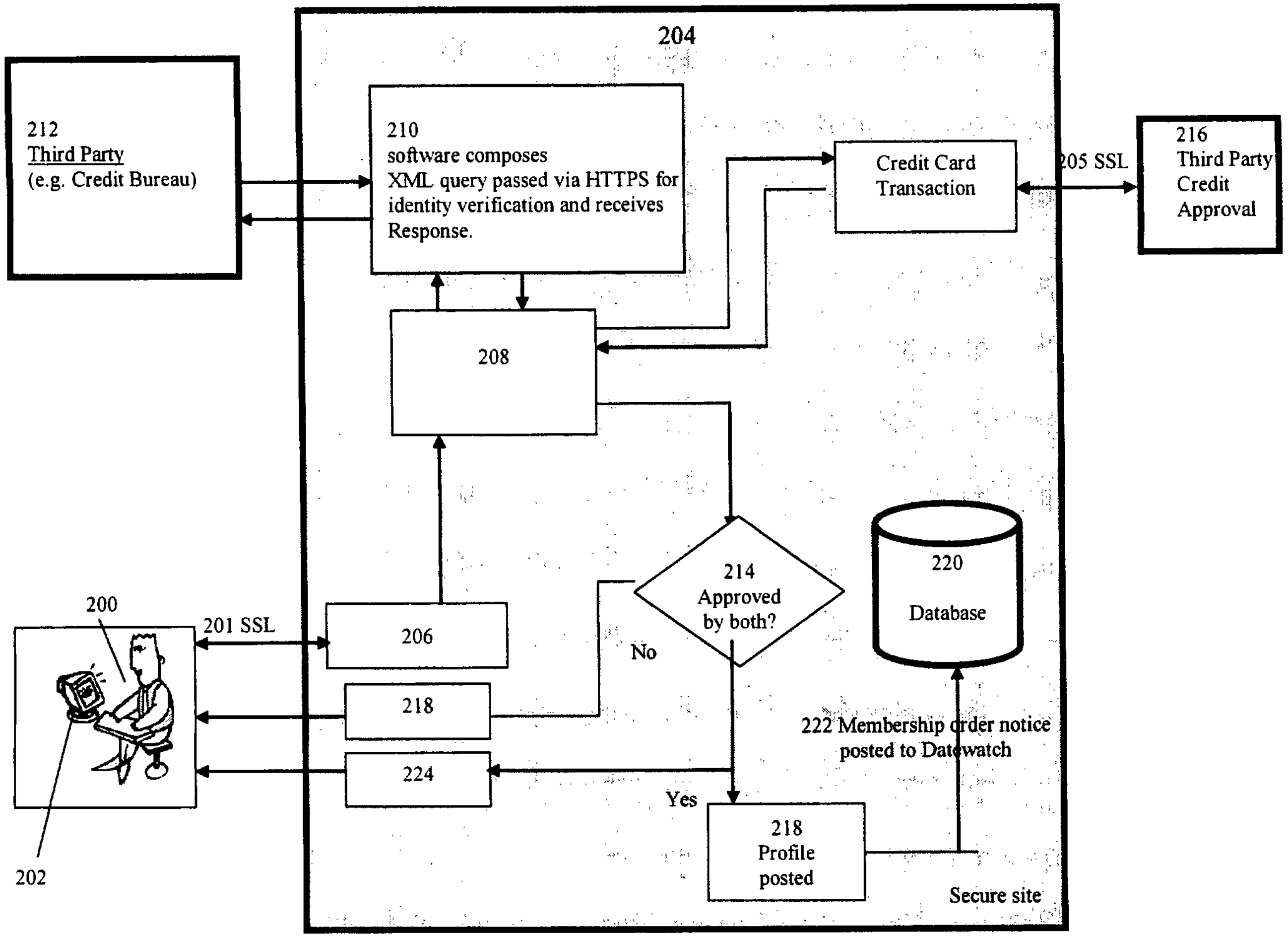
26. The system of claim 24, wherein the biometric identifiers are configured to identify hobbies and personal property owned by the member.

FIG. 1


Verification Module 100
Grant Access 103
Compare Data With Third Party 102
Applicant Inputs Information 101
Authentication Module 110
Post Member Profile 114
Tag Content 113
Create Biometric File 112
Create Video and Audio Files 111
Interface Module 120
View Member Videos 123
Search Database 122
Input Preferences 121
Virtual Meeting Module 130
Connect to Server and Begin Virtual Date 133
Accept or Deny Virtual Date Request 132
Send Request For a Virtual Date 131

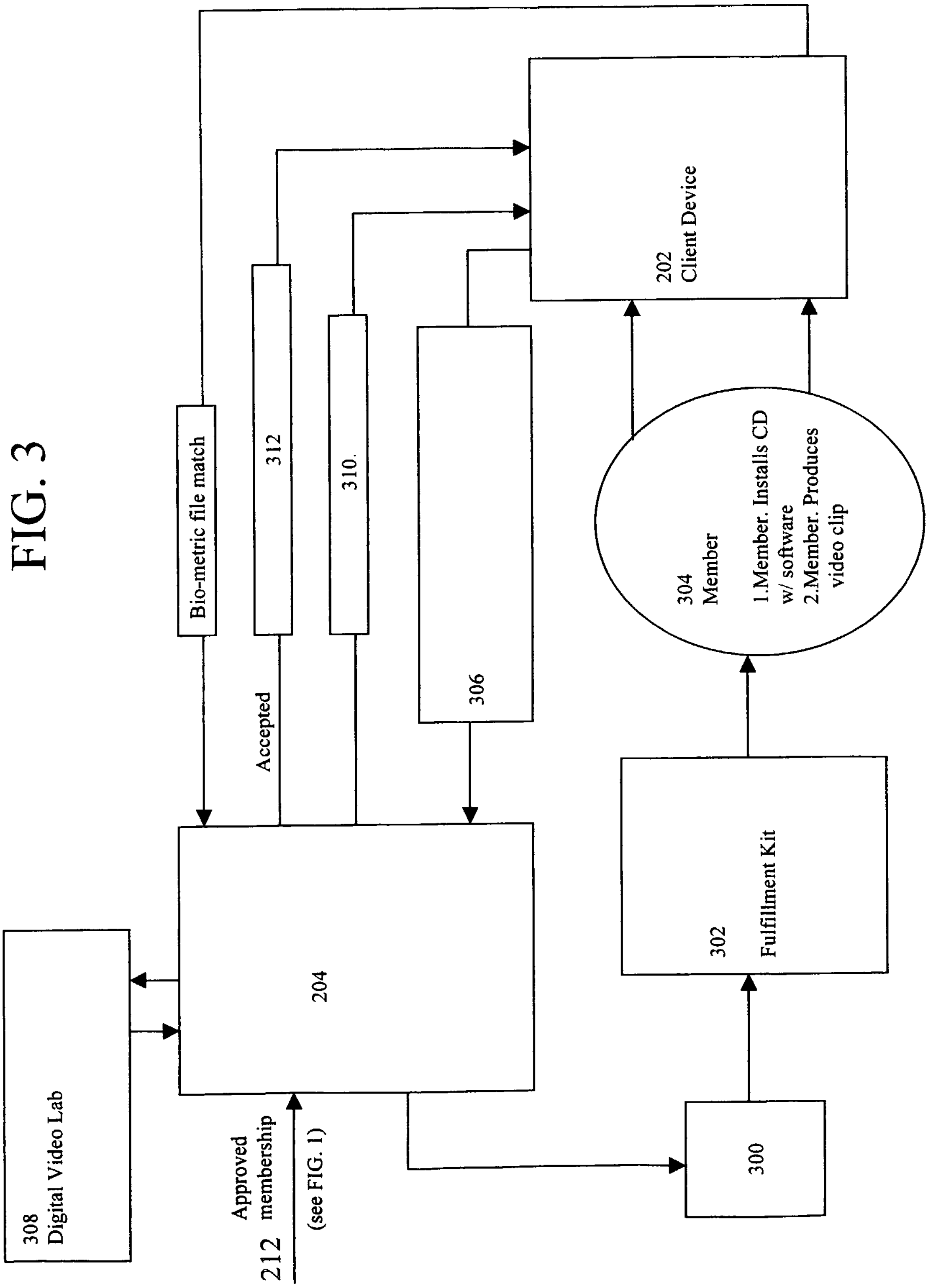
David Ackerman- 858-751-2485

FIG. 2



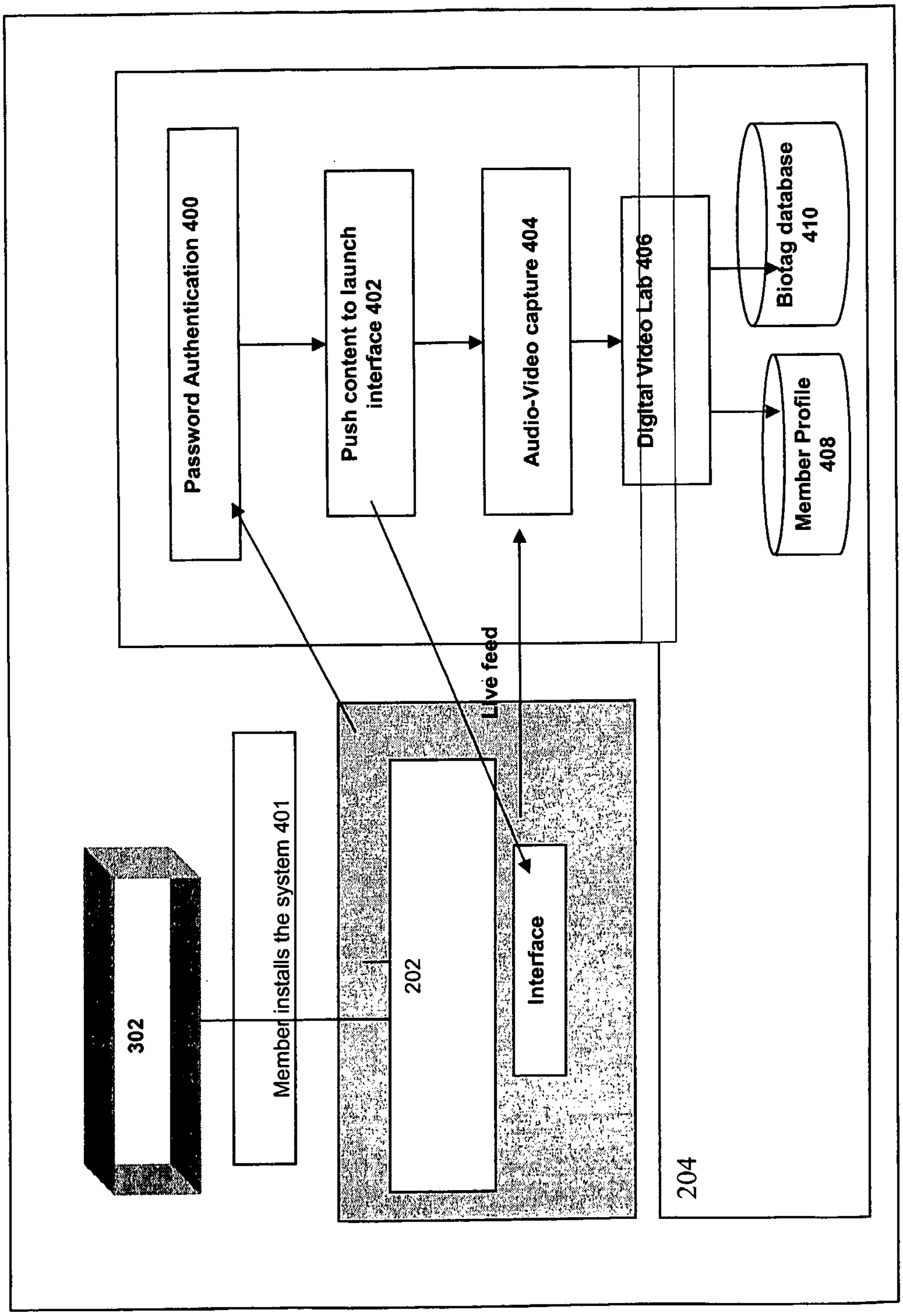
David Ackerman- 858-751-2485

FIG. 3



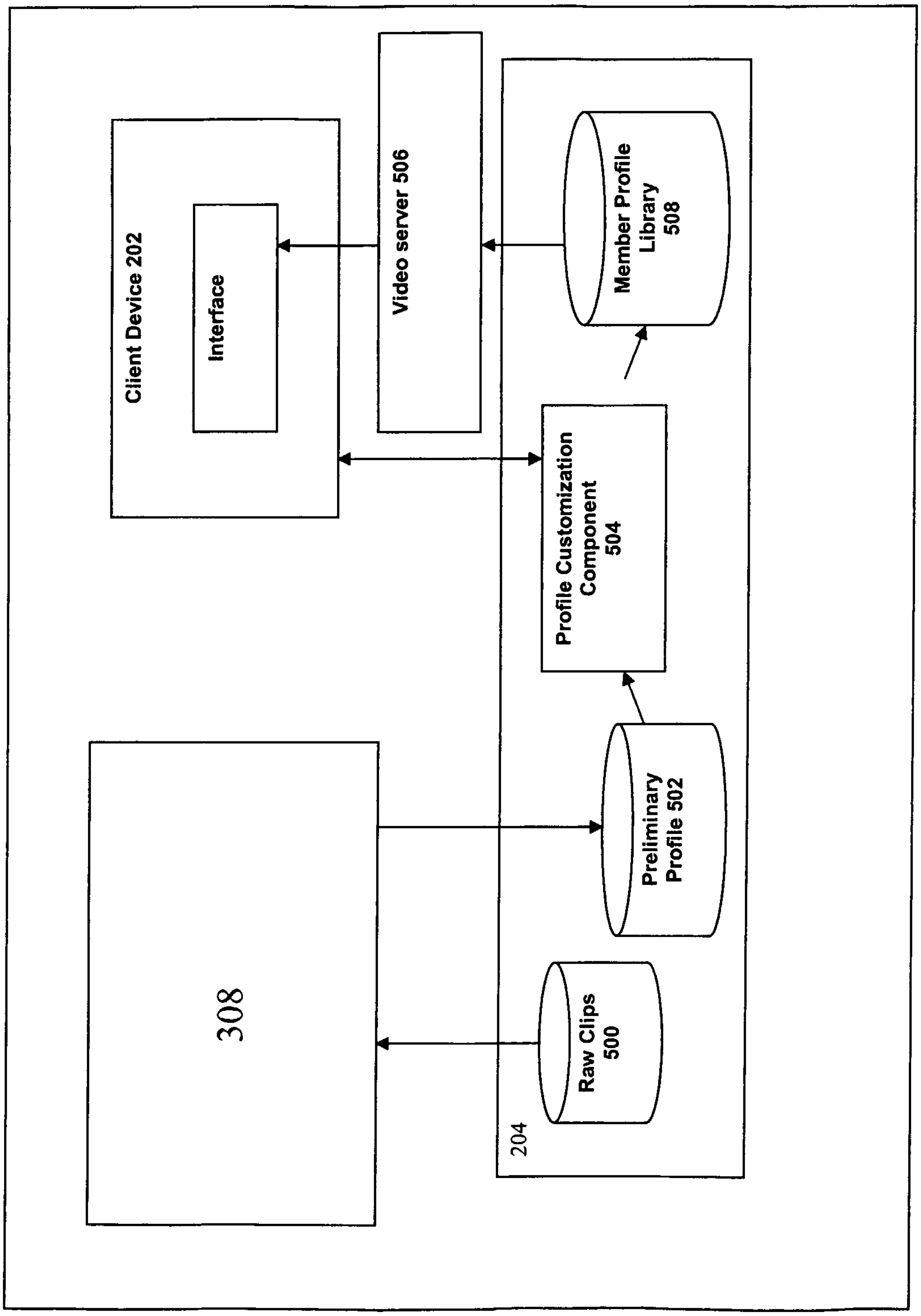
David Ackerman- 858-751-2485

FIG 4



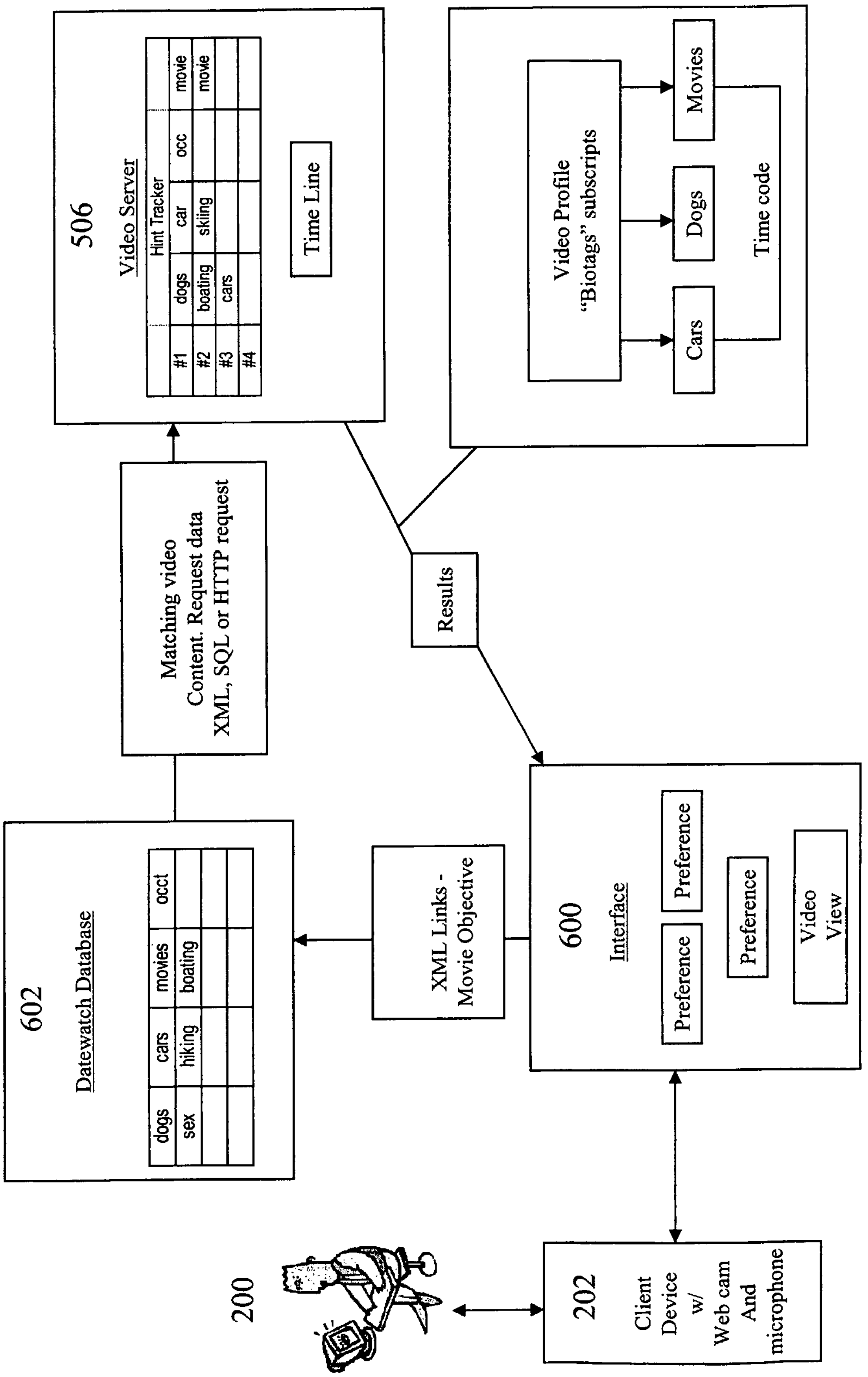
David Ackerman- 858-751-2485

FIG. 5



David Ackerman- 858-751-2485

FIG. 6

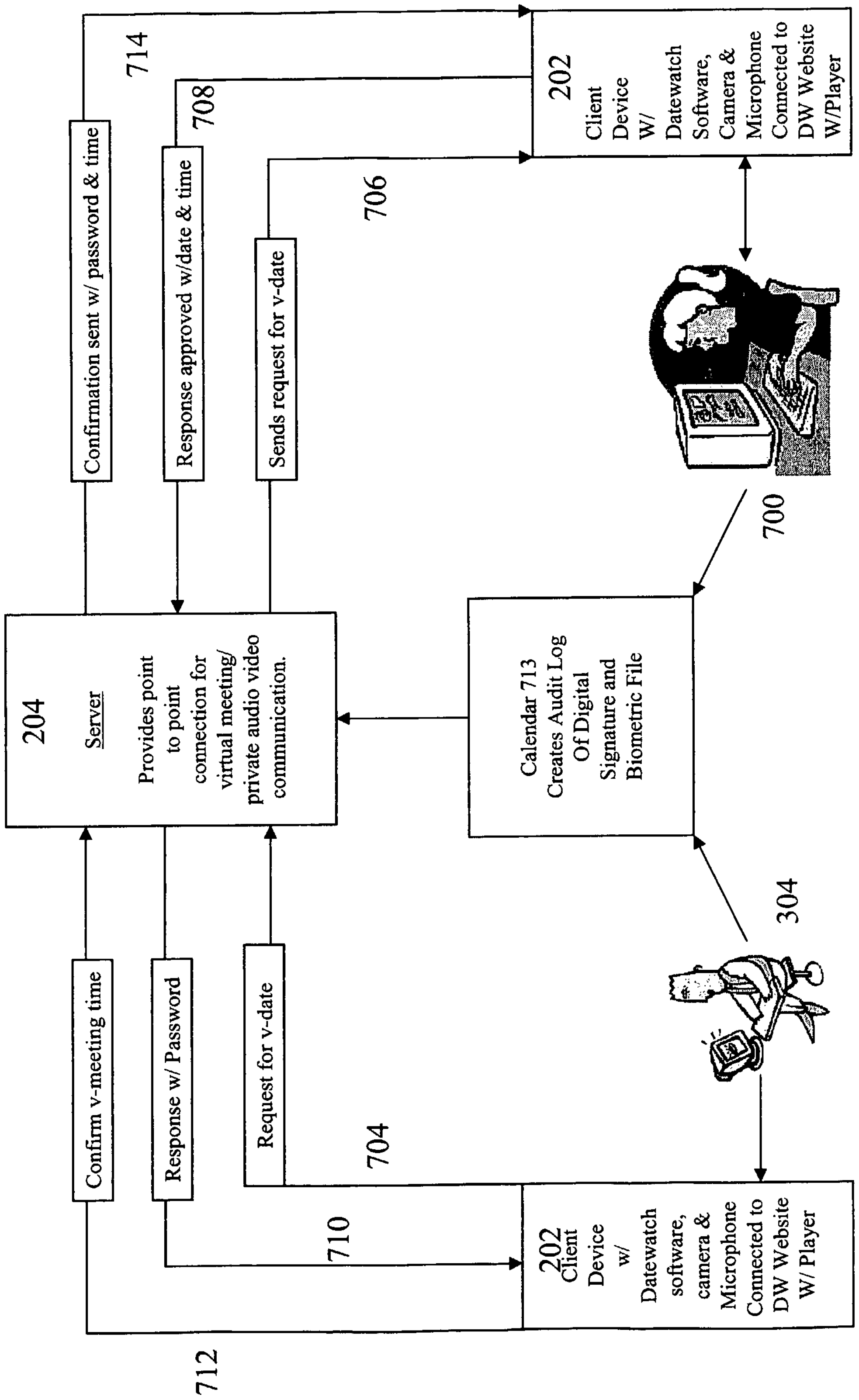


#1	dogs	car	occ	movie
#2	boating	skiing		movie
#3	cars			
#4				

dogs	cars	movies	occt
sex	hiking	boating	

David Ackerman- 858-751-2485

FIG. 7


204
Server
Provides point to point connection for virtual meeting/ private audio video communication.
Confirmation sent w/ password & time
714
Response approved w/date & time
708
Sends request for v-date
706
202 Client Device W/ Datewatch Software, Camera & Microphone Connected to DW Website W/Player
700
Calendar 713 Creates Audit Log Of Digital Signature and Biometric File
304
Confirm v-meeting time
Response w/ Password
Request for v-date
704
710
712
202 Client Device w/ Datewatch software, camera & Microphone Connected to DW Website W/ Player

David Ackerman- 858-751-2485

FIG. 8

Bandwidth	Slice 1 (Two sectors) 384kb	Slice 2 384kb	Slice 3 384kb	Slice 4 384kb
Noon to 1	XY	X	X	X
1 to 2pm	X			
2 to 3pm	XY	XY	X	
...				
...				
11 to 12 Noon	X	X		

David Ackerman- 858-751-2485

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US04/11863

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 17/30
US CL : 707/2-4,9,10,102,104.1; 709/203,219,228; 713/186

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 707/2-4,9,10,102,104.1; 709/203,219,228; 713/186

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y, P	US 2003/0093405 A1 (MAYER) 15 May 2003 (15.05.2003), pagraphs 9-92.	1-26
Y, E	US 2004/0158723 A1 (ROOT) 12 August 2004 (12.08.2004), paragraphs 2-102.	1-26
Y	US 6,256,737 B1 (BIANCO et al) 03 JuLY 2001 (03.07.2001), column 2, line 53 - column 58, line 38.	1-26
Y	US 6,195,699 B1 (DENNIS) 27 February 2001 (27.02.2001), column 2, line 55 - column 10, line 59.	1-26
Y	US 6,029,195 A (HERZ) 22 February 2000 (22.02.2000), column 4, line 35 - column 96, line 5.	1-26

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

* Special categories of cited documents:

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

"E" earlier application or patent published on or after the international filing date

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search
17 August 2004 (17.08.2004)

Date of mailing of the international search report
20 SEP 2004

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703)305-3230

Authorized officer
for Michelle R. [illegible]
John E Breene
Telephone No. (703) 305-3900

PCT/US04/11863

INTERNATIONAL SEARCH REPORT

Continuation of B. FIELDS SEARCHED Item 3:

EAST

creat$3, generat$3, profile$1, audio, video$1, photo$, biometric$6, dating, service$1, system$1, schedul$3, meet$3, bandwidth, section$1, segment$1, fragment$1, virtual$3, authenticat$3, verif$8, compar$3.