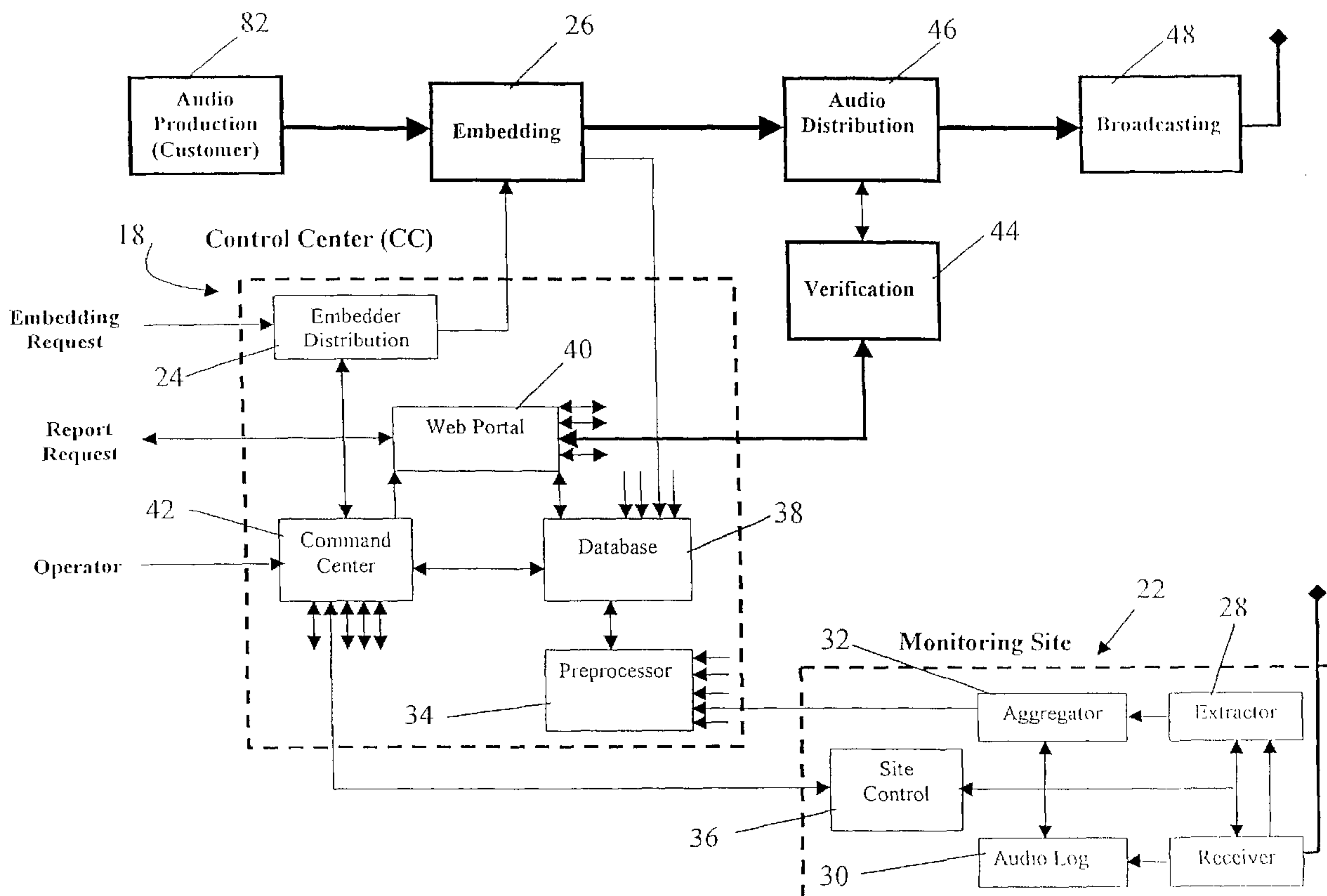




(86) Date de dépôt PCT/PCT Filing Date: 2003/10/07
 (87) Date publication PCT/PCT Publication Date: 2004/04/29
 (85) Entrée phase nationale/National Entry: 2005/03/22
 (86) N° demande PCT/PCT Application No.: US 2003/031816
 (87) N° publication PCT/PCT Publication No.: 2004/036352
 (30) Priorité/Priority: 2002/10/15 (60/418,597) US

(51) Cl.Int.⁷/Int.Cl.⁷ G06F 17/60
 (71) Demandeur/Applicant:
VERANCE CORPORATION, US
 (72) Inventeurs/Inventors:
PETROVIC, RADE, US;
TEHRANCHI, BABAK, US;
JEMILI, KANAAN, US;
WINOGRAD, JOSEPH M., US;
ANGELICO, DEAN, US
 (74) Agent: RIDOUT & MAYBEE LLP

(54) Titre : SYSTEME DE SUIVI DE MEDIA, DE GESTION ET D'INFORMATION
 (54) Title: MEDIA MONITORING, MANAGEMENT AND INFORMATION SYSTEM



(57) Abrégé/Abstract:

Systems and methods are provided for monitoring transmissions of media content (such as audio and audiovisual content) in order to obtain independent and objective data regarding the use of specific media content recordings or works within the transmissions. Processing and reporting of such data is provided in various ways to serve a variety of business needs. Methods for employing content identification technology to efficiently and automatically obtain reliable, accurate, and precise monitoring data are also disclosed. Various information products and services based on such monitoring systems are proposed.

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

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
29 April 2004 (29.04.2004)

PCT

(10) International Publication Number
WO 2004/036352 A3

(51) International Patent Classification⁷: **G06F 17/60**

Dean [US/US]; 2874 Avenida Cereza, Carlsbad, CA 92009 (US).

(21) International Application Number:
PCT/US2003/031816

(74) Agent: **LIPSITZ, Barry, R.**; Law offices of Barry R. Lipsitz, 755 Main Street, Building N°. 8, Monroe, CT 06468 (US).

(22) International Filing Date: 7 October 2003 (07.10.2003)

(25) Filing Language: English

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, 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, 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.

(26) Publication Language: English

(30) Priority Data:
60/418,597 15 October 2002 (15.10.2002) US

(71) Applicant (*for all designated States except US*): **VERANCE CORPORATION** [US/US]; 10145 Pacific Heights Boulevard, Suite 200, San Diego, CA 92121 (US).

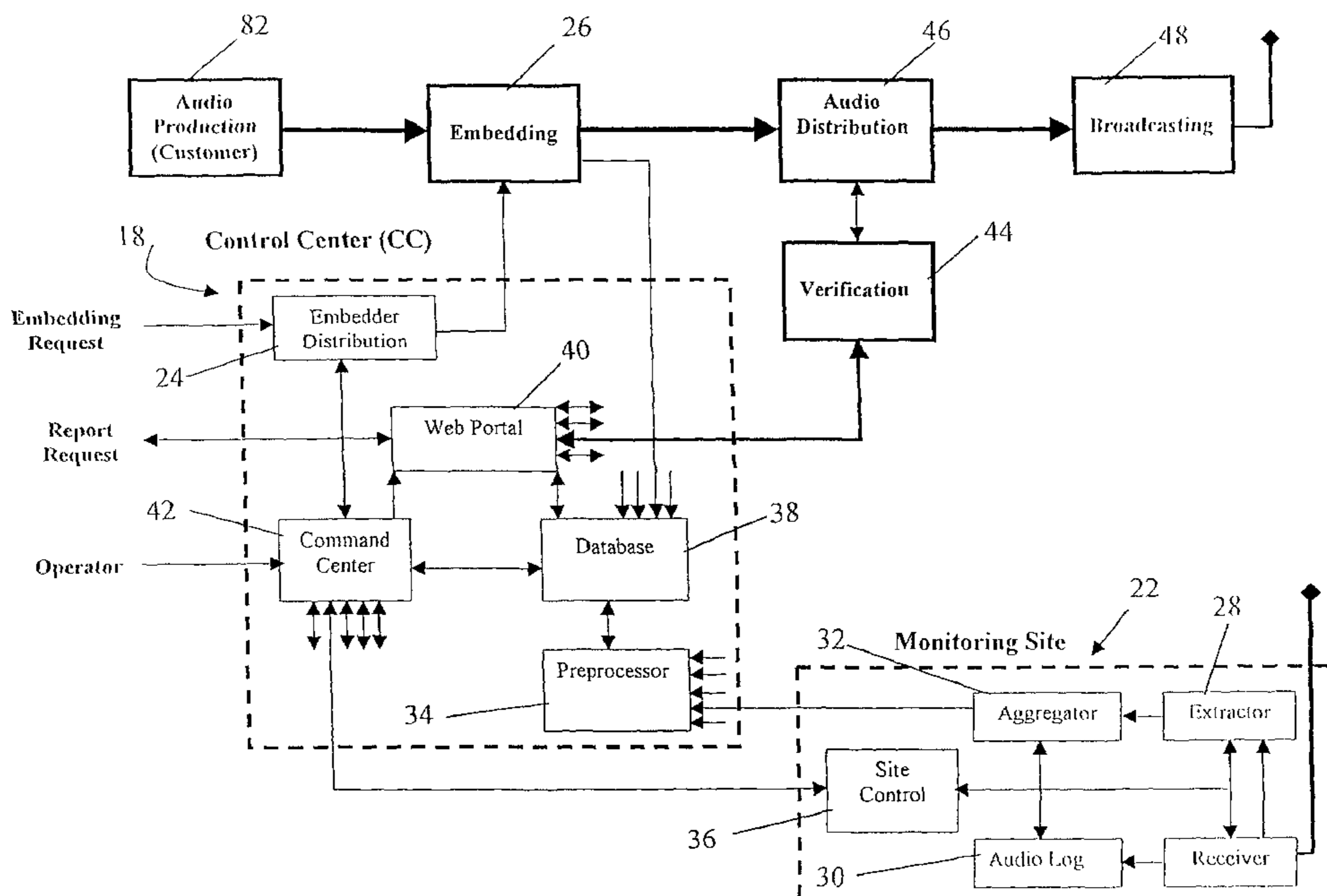
(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ,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

(72) Inventors; and
(75) Inventors/Applicants (*for US only*): **PETROVIC, Rade** [US/US]; 11416 Cypress Woods Drive, San Diego, CA 92131 (US). **TEHRANCHI, Babak** [IR/US]; 12570 Spindletop Road, San Diego, CA 92129 (US). **JEMILI, Kanaan** [TN/US]; 4485 Vision #10, San Diego, CA 92121 (US). **WINOGRAD, Joseph, M.** [US/US]; 3353 Harborview Drive, San Diego, CA 92106 (US). **ANGELICO,**

Published:
— with international search report

[Continued on next page]

(54) Title: MEDIA MONITORING, MANAGEMENT AND INFORMATION SYSTEM



(57) Abstract: Systems and methods are provided for monitoring transmissions of media content (such as audio and audiovisual content) in order to obtain independent and objective data regarding the use of specific media content recordings or works within the transmissions. Processing and reporting of such data is provided in various ways to serve a variety of business needs. Methods for employing content identification technology to efficiently and automatically obtain reliable, accurate, and precise monitoring data are also disclosed. Various information products and services based on such monitoring systems are proposed.

WO 2004/036352 A3

WO 2004/036352 A3



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

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.

(88) Date of publication of the international search report:
15 July 2004

MEDIA MONITORING, MANAGEMENT AND INFORMATION SYSTEM

BACKGROUND OF THE INVENTION

This application claims priority from provisional application no. 60/418,597 filed on October 15, 2002, the entire contents of which is hereby incorporated by reference.

The present invention relates generally to systems for monitoring transmissions of media content (such as audio and audiovisual content) in order to obtain independent and objective data regarding the use of specific media content recordings or works within said transmissions. The invention also relates to the processing and reporting of such data in various ways to serve a variety of business needs. More particularly, the invention relates to methods for employing content identification technology to efficiently and automatically obtain reliable, accurate, and precise monitoring data. The invention further relates to methods for producing information products and services based on such monitoring systems.

It is often desired to perform monitoring to obtain information regarding the use of (or the failure to use) particular media content (such as live or prerecorded music, radio and television programming, and advertising) within various types of transmissions (such as radio and television broadcasts, Internet downloads and streams, and public address systems). The commercial reasons for desiring such information are many and varied, including: providing proof-of-performance for paid advertisements, determining compliance with syndication licenses, identifying uses of copyrighted sound recordings within other programming, administration of the performing rights associated with copyrighted musical compositions, determining the audience size of broadcasts, identifying retransmissions of network or syndicated content, identifying corrupted or partial transmission of advertisements or programming, identifying unauthorized transmissions of copyrighted works, and identifying uses of promotional content and public service announcements.

- [0004] In such monitoring, it may be desirable to obtain a variety of pieces of information regarding the use of the media content, including identification of the exact time, date, location of reception, duration, quality, origin, and method of transmission of the content. In addition, it is advantageous to perform such monitoring automatically without significant intervention from human operators.
- [0005] There are a number of prior art broadcast monitoring systems, which may generally be classified in two groups: passive and active systems. In passive systems, where no additional signals are added to the broadcast programs, measurements of individualizing innate characteristics of the broadcast signals are used to identify a particular segment. These characteristics are sometimes referred to as “fingerprints” in analogy with human fingerprints that are used to identify individuals. Some examples of fingerprints include spectral variations of the broadcast signals, statistical moments, predefined patterns, such as key words, or predefined signal shapes, etc. Descriptions of passive monitoring and identification systems may be found in U.S. Patents 3,919,479; 4,230,990; 4,677,466; 4,697,209; 4,843,562; 5,210,831; 5,436,653; 5,481,294; 5,504,518 and 5,581,658. Such fingerprinting techniques have the disadvantage of requiring complicated search algorithms for comparing the fingerprints that are extracted from broadcast segments to a large database of previously stored fingerprints. In addition, they require a sizeable database of stored fingerprints which only grows in size and complexity as the monitoring service is expanded to include newly produced content.
- [0006] Active systems modify broadcast signals by introducing (e.g., via “embedding”) additional data-carrying signals into the broadcast in a way that does not interfere with normal viewing and/or listening of the broadcast content. However, such additional signals can be detected and decoded (i.e. “extracted”) by an appropriately designed device. Active systems may be classified into two categories, usually known as ‘out-of-band’ and ‘in-band’ systems.
- [0007] In out-of-band systems, the additional information does not reside within the frequency, time or spatial content of the broadcast signal. For example, some video monitoring

signals use the vertical blanking intervals of a video signal to insert identification codes. Other systems use a carrier signal outside the frequency spectrum of audio signals for carrying the identification information. Examples of such systems are described in U.S. Patents 4,686,707; 4,967,273 and 5,425,100. The primary disadvantage of such systems is their vulnerability to format conversion and filtering of the broadcast signals during distribution of the content. For example, data inserted in the vertical blanking intervals (VBI) of an NTSC format video signal may be lost if the video signal is converted from NTSC to MPEG format. Likewise, additional data signals inserted in the audio spectrum outside the range of human hearing may be removed by bandpass filtering of the encoded audio signals.

[0008] In contrast, the additional information in an 'in-band' system is inserted within the visible portion of video and/or audible portion of audio content, which is more likely to be preserved during any further duplication, distribution, processing, or broadcast of the content. This type of embedding of auxiliary signals into humanly-perceivable media content is often called "watermarking." Some examples of such watermarking systems include embedding auxiliary information into television broadcasts by changing the luminescence of adjacent horizontal lines of video in opposite directions. In a typical viewing situation, the human visual system would 'average' adjacent horizontal lines and not notice the deviations from the original. Other systems modulate the auxiliary identification information with an independently generated carrier signal using well-known modulation techniques such as AM, FM, PM or spread-spectrum, and then introduce the modulated signal as low level noise into the broadcast segment. Examples of such systems can be found in U.S. Patents 3,842,196; 3,885,217; 4,686,707; 4,945,412; 4,969,041; 5,200,822; 5,379,345; 5,404,377; 5,404,160; 5,408,258; 5,425,100; 5,450,490; 5,579,124; 5,581,800 and 6,404,898. These systems can generally be made resilient to a wider variety of transmission channel impairments than their out-of-band counterparts. Extraction of reliable identification information under more severe channel impairments, however, usually necessitates increasing the strength of the embedded watermark. This, in turn, compromises visual and/or audio quality of the broadcast segment. In addition, these systems usually fail to withstand combinations of such unintentional impairments or intentional attacks. A short list of typical transmission channel impairments which may be

present in an audio-visual transmission channel include: lossy compression (e.g. MPEG), linear time compression/expansion, pitch-invariant time compression/expansion, Gaussian and non-Gaussian noise, equalization, voice over, change in resolution, change in bit depth, filtering, digital-to-analog and analog-to-digital conversions, interpolation, cropping, rotation, geometrical distortions, dynamic range compression, etc.

[0009] While a number of broadcast monitoring systems that have been deployed commercially employ image or video-based watermark technology, there are certain advantages in using audio watermarks for monitoring. For example, it may be less computationally-expensive to process audio information because of its relatively slow data rate (compared to typical video data rates). Of course, the processing requirements strongly depend on the particular technology in use. It is also possible to monitor both audio and audiovisual content through the use of audio watermarking, whereas image or video-based watermarking fails to address the monitoring of exclusively audio content.

SUMMARY OF THE INVENTION

[0010] It is a principal object of this invention to provide reliable and comprehensive monitoring methods that overcome various deficiencies of the prior art systems. It is another object of the present invention to provide improved monitoring data through the use of redundant receivers and combined analysis of multiple copies of the same transmitted content. It is also an object of this invention to improve the accuracy or effectiveness of monitoring by measuring the quality of the received transmission or the transmission channel by measuring received transmission channel characteristics such as Signal-to-Noise-Ratio (SNR) or dropped packet rate. It is another object of this invention to differentiate between multiple points of origin of a composite transmission, such as the local, regional and national broadcast segments of a given networked television broadcast or an interstitially inserted advertisement in an Internet stream. It is a further object of the present invention to monitor the use of content in the presence of multiple transmission channel impairments. It should be noted that the term "transmission" as used herein will be understood to encompass, but not be limited to, broadcast programming, including satellite, network and cable television and radio programs, Internet broadcast programs, or any other type of program that is transmitted for reception by an audience. All or parts of such programming segments may reside on tangible storage media such as optical, magnetic, and electronic storage media for the purposes of storage, playback or distribution.

[0011] In accordance with the invention, a method is provided for monitoring broadcast multimedia content. Multimedia source content is received, and identification information related to the source content is generated. An audio component of the multimedia source content is imperceptibly and repeatedly embedded with the identification information. A detectability metric is produced by assessing the success of the embedding. The detectability metric is transferred to a central repository together with the identification information. The embedded multimedia content is transmitted through one or more broadcast networks, and received at a receiver. The received multimedia content is processed to extract identification information related to the multimedia content. It is noted that as used herein, the term "imperceptibly" includes "substantially imperceptibly",

as it is conceivable that a person with a trained ear or an unusually acute aural sense may be able to perceive some distinction between the audio component prior to and after the identification information is embedded therein.

- [0012] In an illustrated embodiment, extraction of embedded information is conducted in the presence of multiple transmission channel impairments. The embedding can be repeated in either or both of the temporal domain and frequency domains. Where the repetition is done in the frequency domain, it can occur at different frequencies.
- [0013] Extraction of multiple copies of embedded information can be used to improve the reliability of multimedia monitoring. For example, extraction of multiple copies of embedded information can be used in accordance with the invention to estimate the duration of multimedia content embedded with identification information.
- [0014] In one disclosed embodiment, the multiple copies are extracted from the multimedia content received over a single transmission channel. Alternatively, the multiple copies can be extracted from the multimedia content received from a plurality of transmission channels. The multiple copies can, for example, be extracted using a redundant network of receivers. The redundant receivers can be deployed in separate geographical locations.
- [0015] At least one transmission channel for the embedded multimedia content can be a terrestrial broadcast channel. Alternatively, at least one transmission channel can be an Internet broadcast channel.
- [0016] The spacing of the extracted copies of embedded information can be used to estimate the boundaries of back-to-back encoded multimedia clips. Moreover, the effectiveness of monitoring can be enhanced by measuring received transmission channel characteristics such as Signal-to-Noise-Ratio (SNR) or dropped packet rate. This technique can provide a measure of the quality of at least one of a received transmission or a transmission channel.
- [0017] The detectability metric can be used at the monitoring sites to improve the reliability of

detection reports. Further, the detectability metric and measured transmission channel characteristics (such as Signal-to-Noise-Ratio (SNR) or dropped packet rate) can be used at the monitoring sites to improve the reliability of multimedia monitoring. It is also disclosed that the identification information may be re-embedded with a modified embedding strength based on the detectability metric.

[0018] The type and extent of impairments present in the transmission channel can be identified based on the quality of extracted information from the embedded multimedia content.

[0019] The present disclosure also teaches that multiple points of origin of a composite transmission, such as the local, regional and national broadcast segments of a given networked television broadcast or an interstitially inserted advertisement in an Internet stream, are differentiated.

[0020] Prior to the transmission of multimedia content, the multimedia content can be examined for the presence of a valid watermark. For example, the validity of an embedded watermark can be ascertained by verifying the embedded identification information against corresponding information residing in a database.

[0021] A system is also disclosed for monitoring broadcast multi-media content. Receiving means are provided for receiving multimedia source content. Identification information generating means are used to generate identification information related to the source content. Embedding means imperceptibly and repeatedly embed the audio component of the multimedia source content with the identification information. Watermark assessment means produce a detectability metric by assessing the success of the embedding. Transfer means transfer the detectability metric together with the identification information to a central repository. Transmission means transmit the embedded multimedia content through one or more broadcast networks. Reception means receive the broadcast multimedia content. Processing means process the received multimedia content to extract identification information related to the multimedia content.

[0022] These and additional features and advantages of the present invention, such as its novel system architecture, set of services offered, system control and maintenance features, which result in exceptional performance characteristics, will become more readily clear from the following detailed description of the media monitoring, management and information system, together with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates a general monitoring network connectivity framework;

FIG. 2 is detailed block diagram of a preferred embodiment of the monitoring system;

FIG. 3 is a step by step description of an encoding process in accordance with the invention;

FIG. 4 is a step by step description of an extraction process in accordance with the invention;

FIG. 5 illustrates a first alternate embodiment of the system of FIG. 2;

FIG. 6 illustrates a second alternate embodiment of the system of FIG. 2;

FIG. 7 illustrates a third alternate embodiment of the system of FIG. 2;

FIG. 8 is a step-by-step description of a fail-safe verification process; and

FIG. 9 is block diagram illustrating a real-time embedding process.

DETAILED DESCRIPTION OF THE INVENTION

[0023] FIG. 1 is a high-level diagram of a monitoring system for detecting encoded information carried in a data signal. The source content 10 may comprise, for example, TV and radio commercials, programs, movie and program promos, music which is produced for broadcast, etc. All or parts of such source content 10 may reside on storage devices such as magnetic tapes, hard drives, optical storage or electronic memory devices. Alternatively, the source content 10 may be the soundtrack of a motion picture that is stored on the same medium or separate from the motion picture, e.g., as a digital or analog signal using any of a variety of well-known optical or magnetic techniques. In such cases, means must be provided to extract the associated audio in a computer-readable form for subsequent watermark embedding. It is further possible to directly access the audio signal from the production source without the need for intermediate storage. Such scenarios include direct (acoustical) coupling from the sound source, such as in live musical concerts or theatrical events, or during the studio production via digital and/or streaming networks and apparatus. Delivery means for such source content 10 also includes, but is not limited to, telephone lines, high-speed and/or wireless networks or a simple physical storage medium, as depicted in FIG. 1.

[0024] The source signal is digitized, if necessary, and sent to an encoding station 12 for embedding. In FIG. 1, this encoding station 12 is depicted to contain a Personal Computer (PC) as its processing unit. However, the PC may be readily replaced by any other processor capable of carrying out complex mathematical operations. Examples of such processors include, but are not limited to, the following: digital signal processors (DSP's), electronic circuits containing ASIC and FPGA devices, laptop and handheld electronic devices such as Personal Digital Assistants (PDA's) and mobile phones. Clearly, for the purposes of embedding watermarks into source content 10, a software solution may be more economically feasible, but it may be necessary to utilize a hardware implementation in, for example, time-critical audio-visual applications where synchronization between audio and video is required. It is further possible to place an embedding engine directly inside of a sound capturing device such as a movie camera,

audio recording device and/or studio sound equipment, thus eliminating the need for a PC embedding device. In such cases, hardware or firmware modifications to the conventional sound capture/processing apparatus will be necessary.

[0025] The particular embedding techniques used in the monitoring system can be described under the general terminologies “Feature Modulation” and “Replica Modulation.” These techniques, which are one of the differentiating factors of the present invention, transform part of the source signal, i.e. the replica or the feature, into a carrier of multi-bit auxiliary information that is subsequently added to the broadcast signal using psycho-acoustical masking considerations. The source signal embedded this way does not contain audible artifacts that can be discerned by ordinary or even highly trained human listeners; yet, the embedded information can be successfully extracted with accuracy rates of close to 100%, even in the presence of extreme intentional and unintentional transmission channel impairments and attacks. Using these algorithms, watermarks are inserted simultaneously and redundantly in separate frequency bands in order to withstand different types of distortion, such as noise addition, time scaling, reverberation etc. Because these watermarks reside in separate frequency bands, their audible artifacts are not cumulative; i.e. if the watermark in each band is transparent to the listener, then combining these bands together will not produce audible artifacts. This feat is accomplished through numerous subjective tests and is consistent with the well-known feature of the human auditory system in which different spectral bands are detected with different receptors (hair cells inside cochlea). The exceptional robustness of the watermark is further complimented by several levels of error correction techniques. The details of the embedding algorithms are disclosed in commonly owned U.S. Patents 5,940,135; 6,175,627; and 6,427,012. Another feature of the embedding technique in the system of the present invention is its security against intentional attacks that attempt to remove or obliterate the embedded watermark; the detailed disclosure of this feature is given in commonly owned US Patent 6,145,081.

[0026] During the embedding process, a multi-bit ID field is encoded in the source content 10 and, as shown in FIG. 1, the ‘metadata’ associated with the encoded content is transferred to the Control Center 18 upon each successful embedding. This metadata may comprise a

full description of the owner and content, date and time stamps, etc. that are used to facilitate the identification and tracking of broadcast signals once the embedded content is received by the monitoring stations 16. It is also possible for the embedded watermark to carry all the pertinent information required for tracking and identification of the broadcast segment. However this would require a large watermark payload capacity which necessitates either longer embedded segments or a lower expected detection reliability. For example, a 3-minute music track may be a suitable candidate for this type of embedding but a 20-second commercial may not qualify due to its short duration. The connection between the encoding stations 12 and the Control Center 18 may be any high-speed or low-speed network connection such as telephone lines or cable networks. This transfer of information may also take place either immediately after encoding or after a delay. To illustrate this point by way of example only, and not by way of limitation, one may consider saving the metadata for one or more encodings onto a storage medium, such as a magnetic or optical disk, and subsequently sending the metadata to the Control Center 18 via email or postal delivery at a later time.

[0027] The embedded content is then sent to the broadcast network 14 for distribution to the general public and/or paying customers. In FIG. 1, a satellite broadcast example is depicted. It will be appreciated by those skilled in the art that other means of signal distribution can readily replace and/or compliment the terrestrial broadcast model. Such distribution channels include, but are not limited to, cable television distribution networks, telephone-lines, DSL and broadband networks that power the Internet and local storage devices and server farms.

[0028] At the reception sites, monitoring stations 16 continually monitor the airwaves in search of encoded content. These monitoring stations 16 may be spread throughout different geographical locations within the United States or throughout the world, monitoring a variety of AM and FM radio stations as well as Cable and Network television broadcasts. Other broadcast systems such as short-wave radio, satellite radio, local cable and Internet systems may also be monitored by including the appropriate receivers/decoders at the monitoring sites. These sites are chosen to allow simultaneous monitoring of a large number of radio and TV broadcast signals with good quality of reception. This is

accomplished by using computer simulations of RF propagation in conjunction with databases of 'digital terrain' and FCC approved antenna locations, heights and broadcast powers, for finding optimum locations for the monitoring antennas. Such elaborate analysis is not required for other broadcast systems such as digital satellite broadcasts, web 'streaming' broadcasts, and local cable TV networks, where access convenience and cost are among major factors.

[0029] The Control Center 18 is an integral part of the overall monitoring system, interacting with both the embedding and detection branches. Generating detection and data reports 20, issuing embedding and distribution authorizations and discerning false detection alarms are among tasks performed at the Control Center 18. The connectivity of the Control Center 18 to the outside world is established through a variety of low- and high-speed network connections as well as operator interaction. Data and commands may also be carried via tangible storage media such as optical and magnetic disks. These and other functionalities of the Control Center 18 will be described shortly herein.

[0030] FIG. 2 is a block diagram of a preferred embodiment of the present invention. Two dashed-line rectangles contain two major components of the system: Control Center (CC) 18 and Monitoring Site 22, which is sometimes also referred to as EAR (Event Airplay Receiver). There are many EARs that are connected to the Control Center 18 using a circuit-oriented TCP/IP Wide Area Network (e.g., virtual circuits over a frame relay cloud). This connectivity may also be realized with a variety of other topologies and techniques such as using Virtual Private Networks (VPNs) or point-to-point connections. Data communication between EARs and the Control Center 18 is done through secure protocols to ensure integrity of all reports and prevent unauthorized access. Preferably, the individual EARs are situated on the premises of independent contractors and out of the control of broadcasters, to further reduce any possibility of signal tampering. The system of FIG. 2 is capable of monitoring broadcast signals at the national, regional and/or local distribution levels. This way, the monitoring system can tap onto broadcast signals in the same way as ordinary listeners/viewers, and can detect whatever goes to the ordinary public, including broadcast interruptions, cropping of the clips, voice-overs, etc.

[0031] FIG. 2 includes a number of related blocks that enable encoding of the audio source material in accordance with the steps outlined in FIG. 3. In step 1, Customer Request Processing 50, customer requests are processed which typically include customer identification documents, type of embedder required, reasons for embedding, etc. This communication may take place through sales personnel, but an automatic system for processing customer requests is preferable. In step 2, Embedder ID Generation 52, an identification code is generated which uniquely identifies the customer and the matching embedder. This Embedder ID code, which becomes part of the embedded watermark, can be used during detection to automatically identify the customer as well as the matching embedder. In step 3, Embedder Authorization 54, embedder authorization is issued to the customer. Referring to FIG. 2, steps 1 through 3 are all done in the box labeled Embedder Distribution 24. Other variations of the embedder authorization process are also possible. For example, if the embedders are in the form of software modules, they may not be authorized to operate immediately upon installation. In this case, certain key parameters of the platform (e.g. serial numbers of key hardware components) must be read and communicated to the embedder distribution module 24 before embedding authorization is issued for that particular platform. This way, proliferation of embedders and generation of duplicate codes for multiple audio pieces are prevented.

[0032] In step 4, Self-assigned Code Generation 56, a "self-assigned" code is automatically generated by the embedder, without user intervention or notification, identifying the particular audio content. In step 5, Watermark Embedding 58, the actual embedding of the watermark takes place and upon successful completion, in step 6, Embedder Log Generation and Transfer to Database 60, the Embedder ID, the self-assigned code and other embedder data are combined to form what is known as an "embedder log", which is transferred to the database 38 which resides within the Control Center 18. It is important to note that the embedder log contains embedder generated data, such as description of the audio content in terms of duration, sampling rate, number of channels, energy profile, etc., and user entered data describing the audio or audio visual watermarked content, i.e., title, owner, industry codes etc. Referring to FIG. 2, steps 4 through 6 are performed in the box labeled Embedding 26. In step 7, Verification 62, which may occur at a much later time, the embedded content is checked for the presence of a valid watermark before

being distributed for broadcast in step 8, Distribution and Broadcast 64. In FIG. 2, the Verification 44, Audio Distribution 46 and Broadcasting 48 modules are used to carry out the procedures outlined in steps 7 and 8 above.

[0033] FIG. 4 illustrates the steps required for the detection of embedded content in accordance with the preferred embodiment of FIG. 2. In step 1, Signal Reception 66, broadcast signals are received by the EARs; each monitoring site 22 is used to monitor multiple broadcasts, typically between 8 and 80 stations. Appropriate receivers are used to extract audio streams from different types of broadcast signals. For example, AM and FM receivers are utilized to receive AM and FM radio broadcasts, respectively. However, for receiving an audio signal from a TV broadcast, or an analog local cable, it suffices to simply use an FM receiver tuned to the audio carrier of TV broadcasts. In step 2, Watermark Extraction 68, the audio outputs of the receivers are examined by the extractor 28 module of FIG. 2 in order to determine whether or not they contain an embedded watermark. Since it is possible for the same content to contain different types (i.e., layers) of watermarks, the extractor 28 should be equipped to search for and report the data contained within the detected watermarks as well as the type of detected watermark. It is noted that different types of watermarks may be embedded in different content such as music, commercials, and programs. It is also possible to embed different types of watermarks in the same content, but for different purposes such as identifying the content, source, distribution path, or for copy control, etc.

[0034] In step 3, Audio Logging and Transfer 70, of FIG. 4, audio output from the receiver is compressed, using any one of the well-known audio compression techniques in the art, and saved in chunks of predefined duration with a date/time stamp. This step is performed in the Audio Log 30 module at the monitoring site 22. The stored audio logs may be retrieved by the Control Center 18 on a regular basis or in response to commands issued by the Control Center 18. The main purpose of the audio logs is to resolve disputes over discrepancies between broadcast monitoring reports and broadcaster logs. In principle, the audio logs may also be used to resolve disputes when the system erroneously detects a watermark in an un-encoded audio clip, i.e., a false detection. However, these cases are much less likely, because well-designed watermarks in the present system have very low

probability of false detections. Besides dispute resolution, audio logs are useful for troubleshooting in the case of outages occurring in the broadcast system or the monitoring sites 22. Similarly, audio logs can be used to further analyze anomalous detection results, for example, detections that are short, fragmented, time-compressed, etc. While the stored audio logs are compressed in order to save storage space and transmission bandwidth, it is entirely possible to produce audio logs that are of the original broadcast quality by using less aggressive or even lossless audio compression techniques. Compression factors, and thus the audio log quality, may be changed at different monitoring sites 22 via simple commands from the Control Center 18.

[0035] As noted earlier, the same code is embedded simultaneously in multiple frequency bands and repeated many times throughout the audio clip. As a result, there are numerous watermark detections from the same audio clip. In step 4, aggregation 72 of FIG. 4, these detections are organized and combined together by the Aggregator 32 module of FIG. 2. This module is responsible for identifying all watermarks that belong to the same clip, i.e., all watermarks with identical values, and combining them together. In doing so, the preprocessor 34 may also analyze the spacing between neighboring watermarks; if the watermarks belong to the same clip they have a predefined spacing, also known as the heartbeat of the watermark. This analysis is helpful when the same clip is broadcast in a back-to-back fashion; in such cases there is a high likelihood of discontinuity in the heartbeat, which can be used for separating the neighboring clips. An aggregated string of watermarks contains the detected (common) code, start time of the first detected watermark in the string, and end time of the last detected watermark in the string. In the case of delay sensitive applications, the aggregator 32 may immediately report the first detection of a watermark in a new audio clip. It should be noted that digital equipment at the monitoring sites 22 can measure time precisely using their internal crystal based clocks. However, these clocks have precision tolerances, and drift in time. In order to compensate for the clock drift, they are periodically synchronized to a common (atomic) clock over communication lines from the Control Center 18, through a Site Control module 36.

[0036] In step 5, Transfer to Control Center 74 of FIG. 4, the aggregator module 32 sends the

detection results as well as the ID of the receiver and the broadcast station frequency to the Control Center 18. This information is instrumental in identifying the source of broadcast that carries the extracted codes. The transfer of information to the Control Center 18 occurs in real-time in most cases, and a copy of the detection logs is stored locally for future reference. While Fig. 2 indicates separate links for the aggregator-to-preprocessor and the Site Control-to-Command Center modules, it is entirely possible to utilize a single link for both communication paths.

[0037] In step 6, Preprocessing 76 of FIG. 4, aggregated watermark detections, called 'arrivals', are preprocessed by the preprocessor module 34 of FIG. 2. The main task here is to convert the arrivals from multiple aggregators into 'events' by using the information contained in the database 38. The preprocessor module 34 may be called to task at several other occasions, as well. For example, in cases where multiple receivers are tuned to the same broadcast station, all arrivals are converted into a single event by the preprocessor module 34. In some cases, the aggregator 32 may not have been able to merge disjoint watermarks, either because of large gaps between the detections or due to processing delays; the preprocessor module 34 can use the information contained in the database 38 to merge those arrivals. In other cases, the same clip may be consecutively broadcast two or more times in such a way that it is erroneously identified as one long clip. In such cases, the preprocessor module 34, receiving an arrival with longer than expected duration, may perform 'reverse aggregation' and split a single arrival into two or more events. The preprocessor module 34 also contains several algorithms specific to each type of content. Therefore, the arrivals can be processed differently depending on the *a priori* information stored in the database 38 about the content and detection information.

[0038] In step 7, Embedder Log Association 78 of FIG. 4, all events generated by the preprocessor module 34 are transferred to the database 38 where they are associated with the matching embedder logs. Successful matches are saved in a report folder for future report generation. While a large majority of the matches are successful, there are a few instances where proper matching and identification of the events may not occur. For example, in some cases Embedder IDs may not match any of the issued Embedder IDs in the database 38. These events are stored in a 'false detections' folder for the purpose of

statistical analysis. In other cases, the Embedder ID may be recognized, but the self-assigned code may not match anything in the embedder logs. These events are saved in an 'orphans' folder and are re-tested at a later time (e.g., when new embedder log files are uploaded). Finally, if all attempts in recognizing an orphan detection fail, technical support personnel may contact registered users to resolve inconsistencies.

[0039] In step 8, Report Generation 80, of FIG. 4, customer reports are generated using the appropriate folders in the database. Reports may be generated upon customer request, or at predefined periodic intervals. Fig. 2 indicates that reports are delivered through the Control Center's web portal 40, but it is certainly possible to deliver them by other means, such as e-mail, hard copy, etc. The Command Center 42 governs who has the rights to obtain reports as well as the format and the type of data in the reports. The report generation step 80 also includes formatting and customizing the final report according to the customer specifications. This allows seamless integration of the detection reports into the customer's workflow. Formatting and integration of the final report may be done internally at the Control Center 18 or performed through third party 'middleware' development (not shown in FIG. 2).

Alternative Architectures

[0040] According to a preferred embodiment of the present invention, components in FIG. 2 not contained within the dashed boxes are outside the physical control of the Control Center 18. For example, watermark embedding 26 is done outside of the Control Center 18, typically at customer premises. This is done in order to avoid transfer of audio content from the customer to Control Center 18 and back. Aside from confidentiality concerns over transport of pre-broadcast material to remote locations, the architecture of FIG. 2 avoids any possible delays in the production process due to network and workflow congestion at the Control Center 18. This architecture further simplifies the collection and storage of metadata associated with particular contents. Additionally, some cost savings are realized by avoiding the need for a high-speed connection between the customers and the Control Center 18.

[0041] There are also several disadvantages with the embedding architecture of FIG. 2. Particularly, more sophisticated embedder designs are required to maintain proper operation on different computer platforms such as PC, Macintosh, Unix and Linux at customer sites. It also becomes necessary to keep track of the status and the number of distributed embedders. Significant software and/or hardware development efforts must also be undertaken to ensure user-friendliness of the embedding tools in order to avoid embedding mistakes such as a mix-up between original and embedded files, improper embedder installation, wrong selection of embedder options, and embedding the same content multiple times. This also places more demand on customer service efforts for delivering periodic software/hardware upgrades and assisting customers. Complications may also arise if the network connection between the customer and the Control Center 18 is severed and the embedded content is aired without proper transfer of metadata to the Control Center 18. In such cases, the monitoring sites 22 may produce orphan detections that are not readily identifiable. Distributing of the embedding software to the customers may also open the possibility for unauthorized usages of embedding technology and reverse engineering.

[0042] In the alternate embodiment of FIG. 5, the above and other disadvantages of the system are overcome by moving the embedding operation entirely into the Control Center 18. In the embodiment of FIG. 5 only one customer 82 is shown, but it is understood that the same architecture allows interaction with multiple customers. According to this architecture, verification and embedding operations are all done in one step, in the Embedding/Verification module 84 of FIG. 5, at the Control Center 18. The customers, however, may decide to optionally verify their content before distribution in order to avoid distribution of un-encoded material. In FIG. 5, this optional verification 86 is shown as a box with dot-dashed borders. Although it is entirely possible to utilize a portable storage medium for the transport of data between the customers 82 and the Control Center 18, the alternate embodiment of FIG. 5 indicates a high-speed connection 88 for data transfer purposes. It also requires additional storage 88 and/or buffering of incoming audio as well as the encoded content at the Control Center 18. Security concerns may also necessitate encryption of the stored audio data and presence of secure internal and external connections. Other concerns regarding the embodiment of FIG. 5

include the amount of work required to generate, enter and collect the related metadata for each and every content by the personnel at the Control Center 18. Improvements in workflow efficiency may be possible by requiring all customers to adhere to a standard information-sharing format and/or directly accessing existing databases at customer sites in order to automatically download portions of the metadata.

[0043] FIG. 6 illustrates another alternate embodiment of the present invention, overcoming some of the workflow, security and cost issues associated with the embodiments of FIG. 2 and FIG. 5. According to the architecture of FIG. 6, customers 82 directly send their audio and/or audio-visual content to the distribution center 92 where embedding 26 and verification 44 of content takes place. This architecture avoids the cost and security concerns of a high-speed data connection between individual customers 82 and the Control Center 18. In addition, most of the metadata-related work will be shifted to the distribution center 92 where similar tasks are usually performed for distribution and billing purposes regardless of whether or not watermark insertion is taking place.

[0044] FIG. 7 shows yet another embodiment of the present invention. It was previously disclosed in Figures 2, 5 and 6 that each monitoring site contains an aggregator module 32. In FIG. 7, this module has been moved into the Control Center 18 to form a combined preprocessor and aggregator module 94. This way, detections from the extractor 28 are directly sent to the preprocessor and aggregator unit 94 at the Control Center 18 where sophisticated aggregation computations are performed using all available resources at the Control Center 18. In addition, fewer control commands are required to regulate the operation of each monitoring site 22. From an economics point of view, it is also advantageous to simplify the design of monitoring sites 22 by eliminating as many components as possible in order to help proliferation and maintenance of the sites, granted that the cost of transferring more detection data may not become prohibitive.

[0045] While different embodiments for the embedding, delivery and monitoring of audio content have been disclosed, it should be appreciated that various combinations of the above architectures may be used to effect suitable embedding and monitoring of different types of audio-visual content. For example, while one architecture may be used to deliver

production (non-feature) music, another architecture may be used for feature music and yet another architecture may be used for TV or radio advertisements and promotions. Furthermore, while some monitoring sites may contain several sophisticated processing and storage components, others, being located in less accessible locations, for example, may contain only a few components that convey the data for further processing to the Control Center. The complexity of a monitoring site facility may also be influenced by the number and the type of channels being monitored.

Additional Features

[0046] As previously disclosed, the Site Control module 36 is used to pass commands and extract status reports from the monitoring sites 22. They are also instrumental in providing accurate timing information for aggregators and extractors and handling requests for on-demand uploading of the audio logs. However, there are many more important functions and features achieved through the communication link between the Site Control 36 and the Control Center 18. One of features is the capability to upgrade various software components that reside within the monitoring site 22. This may include a full replacement of previous software modules or just selection and/or modification of configurable parameters. For example, the monitoring site 22 may be remotely configured to detect additional types of watermarks, e.g., additional watermark layers, or to modify the parameters that are used in detection of a particular watermark layer. It is also possible to remotely switch to spare receivers in case of receiver failures, increase or decrease the number of stations being monitored, adjust certain parameters such as carrier frequency, modulation type, volume, RF attenuation, etc. Similarly, 'first packet reporting', described earlier, may be enabled or disabled in the aggregator.

[0047] The Site Control module 36 is also responsible for monitoring the overall status of the monitoring site 22 and communicating the alarm signals to the Control Center 18. These alarm signals are generated by different mechanisms, indicating the status of software, environmental and communication subsystems. For example, temperature and humidity within the monitoring sites 22 are constantly monitored and alarms are generated if they go beyond certain thresholds. Status of internal communications within the monitoring

site is also periodically checked for outages and anomalies. Uninterruptible Power Supply (UPS) units may also generate alarms in order to initiate a graceful shutdown of the site. Several other alarms are also generated to assess the quality of the received audio signals. For example, at each monitoring site 22, the RF power of the incoming broadcast signal is continually measured to ensure that it is within acceptable bounds. Similarly audio levels are monitored to make certain they are within a predefined range of values. These measurements provide valuable information regarding the quality of the audio signal which may be used to predict watermark detection reliability.

Signal-to-Noise-Ratio

[0048] A standard measure of signal quality is Signal-to-Noise-Ratio (SNR). Monitoring sites 22 are capable of measuring the SNR for all incoming audio signals at the signal reception sites. One method of monitoring SNR is to compare the long-term average of audio signal power with the short-term minimum audio power. Long-term average represents a measure of signal plus noise power. Short-term power calculations, measured over several tens of milliseconds, typically represent intervals where there is no signal present, thus comprising of only noise power. So, SNR can be simply calculated from the following equation:

$$\text{SNR} = (\text{Long term power} - \text{minimum short term power}) / (\text{minimum short term power})$$

[0049] The above technique for calculating SNR was given by way of example and not by way of limitation. Other SNR calculation techniques may be utilized where appropriate. For example, a different method may be applied if a pilot signal used for demodulation is included in the broadcast. This is the case for FM radio and TV broadcasts, where pilot signals are inserted at 19 KHz and 15.75 KHz, respectively. In such broadcasting techniques, the natural audio components around the pilot frequency are removed prior to broadcast. Accordingly, any signal that is detected in the received audio in the vicinity of the pilot signal can be safely attributed to channel noise. In this case, the method of estimating the SNR is based on comparing the signal power in the vicinity of the pilots with the overall power level of received audio.

[0050] Using the calculated SNR values, it is possible to continually monitor and log the quality of different audio stations. Alarms generated based on SNR anomalies, in addition to other alarms generated due to, for example, variations in mean signal RF and volume levels, may be used to prompt the Control Center personnel to take appropriate actions. These alarms could be the result of monitoring site equipment failures, broadcast interruptions or poor quality of broadcast signals. In the monitoring system of the present invention, all monitored broadcast channels are periodically assessed in a process known as "channel grooming." The results can be used to predict and improve the watermark detection success rates. In addition, the channel quality information for each geographical location may be shared with the customers and broadcasters. Broadcasters may use this information, for example, to boost their transmission power at certain locations and/or during certain time periods.

Watermark Verification

[0051] Embedded audio watermarks in the present invention are substantially inaudible; it is virtually impossible to discern whether or not an audio clip contains a watermark by just listening to it. It is thus essential to systematically verify the presence of a watermark before embedding and before distributing the content for broadcast. As described previously in relation to various embodiments of the present monitoring system, verification may be performed at different points in the encoding chain. For example, it is important to determine whether or not an audio segment already contains a watermark before attempting to re-embed the content. This task can be accomplished with an "integrated extractor" as part of the embedding engine. This way, embedding may be aborted or interrupted if a watermark is detected. In a basic configuration, it suffices to signal the presence or absence of a watermark by an appropriate display or a flag while identifying the clip by just listening to the content. In more sophisticated applications, however, such as automatic inventory of audio clips, it is necessary to convey the metadata related to the watermark back to the Control Center 18. The database inquiries can also clarify the status of a watermark. Some of the detected watermarks may be attributed to test trials conducted at the customer sites or simple mislabeling of the

content. In such cases, the Control Center 18 has either no information about the detected watermark or it correctly identifies the customer as the rightful owner of the audio segment.

[0052] Other detections may be due to presence of additional watermarks within the content. As previously disclosed, several watermark layers may be inserted into the same audio content for different purposes. By reporting all detections to the Control Center 18, one can track all embedded content, even those embedded previously by a different content owner. This way, for example, the rightful owner of a music piece would be able to collect royalties if his/her music were used in a TV commercial. Detection of different watermark layers is possible at other points within the disclosed monitoring system, as well. For example, as will be described shortly, it may be done at the Verification stage that follows embedding, or it may be done at the monitoring sites after receiving the broadcast signal. This is possible since embedding of one watermark layer over another does not usually obliterate either layer. However, one or more of the layers may be weakened. Furthermore, in the presence of transmission channel noise accompanying broadcast signals, it may be more difficult to reliably detect the presence of older watermarks at the monitoring sites. In such cases, the information residing at the database can be used to verify the existence of all watermarks.

[0053] It is also important to verify the presence of a valid watermark before the audio segment is distributed for broadcast. This is done by the block labeled 'Verification' 44 in FIG. 2. The functionality of the verifier is very similar to the integrated extractor, described above, as it searches through the audio segment to detect and report the presence of all embedded watermarks. In a stand-alone configuration, the presence or absence of a watermark may be signaled using an appropriate display or a flag. In a verification scheme with connectivity, the detected watermarks are reported back to the Control Center 18 and checked for validity.

[0054] The presence of additional watermarks may also be reported and logged. The connectivity between the database and the verifier may also be used to implement a fail-safe verification technique. This procedure is described in FIG. 8. The process starts in step 1,

Content Acquisition 100, by acquiring the audio content prior to distribution for broadcast. In case of an audio-visual content, the audio portion must be separated from the visual content and the signals. If the audio is in analog form, it must be converted into digital form. In step 2, Watermark Detection 102, the content is checked for the presence of watermark. In step 3 (104), a decision is made based upon whether or not a watermark was detected in step 2. If embedded watermarks are not detected, a 'Denial Notification' 106 is issued. This notification could be in the form of a beep or a visual alert, or could include physical interference with the shipping procedure. Some examples of this physical interaction will be given shortly. If embedded watermarks are detected, in step 4, Check Control Center 108, watermark information is communicated back to the Control Center 18 and checked for validity. In step 5 (110), a decision is made to issue a 'Denial Notification' 106 for invalid watermarks or an "Approval Notification' 112 for valid watermarks. A detected watermark may be declared invalid, for example, if no matching metadata is found at the database, i.e., an orphan watermark, or if the watermark has expired or does not contain the proper embedder ID, etc.

[0055] Obviously, successful operation of the above system requires timely uploads of the embedder logs upon successful embedding of the content. An approval notice could be in the form a beep or visual cue as well as more sophisticated physical interaction with the workflow. For example, the verification system could be set up so that once an approval notice is issued, the audio filename is changed to conform to the shipping workflow specification. Alternatively or additionally, an approval label may be printed and placed to the disk or the tape that is used for the transportation of content. The complexity and reliability of the verification process strongly depends on workflow procedures and resources available at the verification sites. While in some instances, such as the system described in FIG. 6, the above fail-safe verification system may be an invaluable resource, in other architectures, such as the system of FIG. 2, it may not be economically feasible.

Optimized Detection and Reporting

[0056] One of the features of the disclosed monitoring system is that it allows transfer of a

variety of information to the Control Center 18 upon successful completion of embedding. This includes embedder- and watermark-related ID information as well as other parameters, generally referred to as “detectability metric.” Since the robustness of an embedded watermark is related to the characteristics of the particular audio segment, a set of embedded watermarks may exhibit different degrees of resiliency to channel distortions if embedded within different audio segments. Detectability metric, conveyed to the Control Center 18 after embedding of each segment, indicates how well the embedding process succeeded in encoding the content and predicts how reliably the embedded watermarks can be detected after undergoing various amounts of distortion and noise during broadcast and reception. This information may be provided to the users of the system, which in turn, may decide to increase the embedding strength to improve detection probability. Alternatively or additionally, the detectability metric may be used to diagnose why a certain embedded content may not have been detected at the monitoring sites. It will be later described how the detectability metric and SNR measurements can be combined to improve detection probability.

[0057] Among other information relayed to the Control Center 18, after embedding is the exact duration of the embedded segment. This way, upon extraction of watermarks it is possible to detect if the original clip has been shortened for broadcast. Note that some audio clips begin and/or end with silence, typically as a means for separation between clips, but sometimes due to presence of video without audio. During embedding, the initial silence interval is automatically detected and skipped; embedding starts only when audio signals are present. This feature is particularly helpful in detection of short clips, where losing the initial portion of the first embedded watermark may affect overall detectability. The duration information for such clips can be more precisely determined by combining the information obtained from watermark detection with duration information contained in the database.

[0058] User selectable parameters such as watermark strength, dither algorithm, psycho-acoustic model for adjustment of watermark strength, etc. allow user control over transparency and/or detectability of the watermark. These parameters are included in the metadata and subsequently transferred to the database 38 and stored as the embedder log. The

embedder log information can be used to optimize the reporting process. For example, if weak watermarks are being processed, only channels with good signal quality may be reported and if strong watermarks are being processed, marginal channels may be included as well.

Dynamic Decoding

[0059] Knowledge of watermark quality, prior to detection, coupled with knowledge of channel quality parameters, for example, the SNR value, the Bit Error Rate (BER), etc., can be used to implement a 'dynamic decoding' technique. There are several levels of error correction and packet detection strategies used during extraction of watermarks in the disclosed monitoring system. At one level, well-known error correction codes, for example Reed-Solomon and BCH codes, are used to detect erroneous watermark bits and subsequently correct them. Error correction capabilities may be further improved by probabilistically assigning 0 and 1 values to the extracted bits. This technique is also known as soft-decision decoding. Still, at a different decoding level, once a single watermark packet is successfully detected, forensic techniques are used to predict the presence or absence of future and past watermark packets. In addition, since watermarks in the present system are redundantly encoded, averaging techniques may be utilized to improve the detection probability.

[0060] In an error-free communications channel, where perfect embedding, transmission and reception of watermarks are carried out, such error correction and detection techniques are not needed. In all other cases, however, depending on the amount of noise in the channel, some or all of the above may become necessary. In such cases, certain parameters and thresholds must be selected to effect maximum detection while minimizing the probability of false watermark detections. Examples of these parameters include, but are not limited to, the following: maximum number of errors to be corrected by the Reed-Solomon decoder, number and threshold of probabilistic levels assigned to "soft" bits, minimum number of packets that needs to be collected for implementing averaging techniques, thresholds for forensic detection, etc. These parameters may further be dynamically optimized according to the quality of the particular

transmission/embedding channel. The dynamic decoding technique, in its simplest form, entails having different sets of decoding parameters for differing channel qualities, i.e., for different SNR values. More sophisticated systems involve decoding of at least one watermark packet, searching the database to obtain the detectability metric for that segment and setting more or less aggressive decoding parameters based on channel quality-detectability combination. By way of example only, and not by way of limitation, decoder settings versus different channel quality and detectability levels are displayed in the following TABLE:

<u>Watermark Detectability</u>	<u>Channel Quality</u>	<u>Decoder Setting</u>
Good	Good	Setting 1
Good	Bad	Setting 2
Bad	Good	Setting 3
Bad	Bad	Setting 4

[0061] While only two levels of detectability and channel quality are shown in the TABLE above (either good or bad), it is appreciated that these parameters may be classified using more than two levels, in which case, more decoder settings may be necessary.

Real-Time vs. File Mode Embedding

[0062] As previously mentioned, the embedder may be implemented using software, hardware or a combination of both components. In addition, embedders may be used at different locations within the distribution chain, as described in FIG. 2, FIG. 5 and FIG. 6. Depending on the application, location, available resources and workflow, embedding may be done in real-time or file mode. In a file-mode implementation, audio watermarks are embedded into audio files without much consideration for delay or synchronization issues. Embedding can be done one file at a time, or on a series of files in what is called "batch processing."

[0063] Real-time applications include embedding of live or streaming events, and applications where embedding is done during the transfer of content from one storage medium to

another. The latter includes tape-to-tape, server-to-tape, server-to-disk, tape-to-disk and other transfers of recorded audio or audio-visual information. The challenging task of a real-time encoder is to embed the audio watermark while maintaining synchronization between the audio and video portions of the input signal. FIG. 9 shows a block diagram of an exemplary real-time encoding system for an analog audio-visual input signal. In accordance with this figure, after multimedia components are separated in Audio-Video Separator 120, the analog audio signal is digitized in the A/D Converter 122, embedded in Audio Watermark Embedder 124, and converted back into analog form, in D/A Converter 126, while the video portion remains idle in the video delay block 128. Next, the embedded audio is combined with the corresponding video signal in Audio-Video Combiner 130 and is made available for further processing and/or transmission. The video delay block 128, shown in FIG. 9, accommodates fixed pipeline delays in the system and ensures proper audio-video synchronization. These delays may be due to internal and/or external loading and transfer of audio data; typically a video delay buffer of a few video frames is sufficient. The real-time watermarking engine depicted in FIG. 9 needs to process the incoming audio signal at a fast enough rate to maintain synchronization with the corresponding video frames. In NTSC-encoded video, frames are separated by approximately 33 milliseconds; it is desired to maintain synchronization to within a fraction, for example, one-tenth, of one frame duration. It is possible, with today's microprocessor capabilities, to implement such an engine using entirely software modules. However, if more embedding features and/or processing steps are added, real-time embedding using an all- or part-hardware implementation may be preferable.

[0064] Other variations of the system of FIG. 9 are certainly possible. For example, in an all-digital system, A/D and D/A conversions are not necessary yet it may become necessary to process compressed input signals. In such systems, the input audio and/or video signals must be decompressed, embedded with audio watermark and then converted back to their original compressed format. In other exemplary systems where audio and video portions of the input signal are completely separate from each other, audio-video separation 120 and combination 130 modules, depicted in FIG. 9, become irrelevant. Still, in other systems, metadata streams containing information such as time code, are included in the audio and video signals. In such systems, not only audio, video and

metadata streams need to be separated, but also synchronization must be maintained among multiple streams. Finally, batch processing can also be made possible in a real-time embedding system by providing an embedding list of time instances when a new clip begins and ends.

Local, Regional and National Monitoring

[0065] Given the vast geographical coverage of the disclosed monitoring system, it is possible to provide monitoring capability at local, regional and national levels. This feature is particularly useful for monitoring radio and TV commercials where local media distributors may (or may not) replace the national advertisements with local ads. Since such replacements are not done on a regularly scheduled basis, it is important for the content owners to precisely know when, where and how many times their program segment was broadcast. Using the present invention's satellite, cable and Internet monitoring capabilities, it is possible to provide such detailed reports to the customers. The detection results are collected at the Control Center 18 and processed in order to generate the pertinent information for each advertiser.

Redundant Monitoring

[0066] The monitoring capabilities of the present invention may be further enhanced by taking advantage of a redundant network of receivers. Redundant monitoring is accomplished in several ways. Multiple receivers may be able to monitor the same station because of geographical coverage overlap between monitoring sites. In addition, the same content may be monitored simultaneously through different types of channels such as over-the-air, local and national cable broadcast channels. It is also possible to intentionally tune multiple receivers, of the same channel type, to the same station in order to improve reliability of detection and/or for troubleshooting purposes. Redundant monitoring can be used to improve the accuracy of timing information generated for detected clips. Such information may be used, for example, to tie a commercial to a particular show.

Channel Quality Assessment

[0067] As noted above, the quality of received RF signals, volume levels, and other signal parameters can be monitored at the monitoring sites. In addition, SNR values corresponding to individual channels can be continually calculated for the incoming signals throughout the monitoring system. The above parameters can be evaluated regardless of the presence or absence of watermarked content. It is additionally possible to use the detected watermarks for channel quality assessment. For example, it is possible to determine whether or not the broadcast content has undergone time compression by measuring the duration of detected watermarks. Time compression artifacts may arise due to ordinary processing of content via substandard equipment or could be the result of intentional processing by an unscrupulous broadcaster in order to make room for additional advertisements. Nevertheless, it is important for the customer to be aware of such possible channel impairments. Similarly, it is possible to measure wow and flutter, typically associated with analog tape players, and the amount of noise in the broadcast channel (e.g., by measuring bit-error-rate). Analyzing the quality of detected watermarks in the frequency domain and assessing the extent and type of damage to watermarks in each frequency band can also shed light on possible frequency domain impairments such as bandpass filtering and compression. The information regarding channel quality can be provided to the interested customers as well as broadcasters. They can also provide a measure of confidence about detection rates on particular channels.

Network Identification

[0068] One of the watermark layers deployed in the present monitoring system is utilized by the Radio and Television Networks to identify and monitor the times and programs where a network affiliated local station is carrying the network's broadcast signal. This information may be important to the networks in order to measure and verify compliance. In the case where content is distributed to the network as local or regional stations, this capability allows for differentiating the different sources. Real-time embedders may be deployed in the network facilities to ensure all content is watermarked.

International Deployment

[0069] The Broadcast Monitoring Network may also be expanded internationally, allowing content encoded in one country to be detected at the country of origin or in any other country where monitoring devices are available. For the purpose of maintaining compatibility, a set of design constraints is defined for the various subsystem blocks. These constraints may be classified in two categories, where the first category contains the physical and logical layers of the system and the second has more to do with the metadata and detection data exchange. These constraints include, and are not limited to, the definition of certain core rules that govern the underlying watermarking technology and how it is applied in the broadcast monitoring system, the minimum set of data fields that insure proper dialog between systems in the different countries.

Content Tracing

[0070] The broadcast monitoring may also reveal the unauthorized airing of certain content, in cases where the content is earmarked for preview only or before official releases. A set of rules around the metadata of such content will allow for the tracing of the aired copy.

Other Applications

[0071] Monitoring and data collection capabilities of the present invention can be utilized in other ways, as well. One such application relies on the fact that most people may not pay particular attention to radio and TV commercials at the exact moment of their broadcast. Yet, at some later time, when they are in search of a particular service or product, they may become interested in special promotions and discounts. The advantage of the disclosed monitoring system is that it retains the exact knowledge of time and geographical location of certain broadcast commercials. It also has the capability of replaying those commercials by directly accessing the stored audio logs. In addition, if certain information about the content, for example, a contact phone number or an Internet link, is included in the embedder log for each content, the Control Center database 38 is further capable of providing such contact information to an interested consumer. These

features of the present monitoring system make it a suitable candidate for becoming a secondary source of direct advertisement for targeted audiences based on geographical location. As an example, someone that is interested in buying a car may use the present system to obtain a list of all auto-related advertisements, promotions or discounts that have aired in a particular region in the span of a few days. In addition, the present system can provide a replay/reprint capability of commercials for the interested consumer. In effect, this system becomes a repository of aired commercials that are readily available for re-utilization.

[0072] There are many possibilities on how to access this system. Connectivity to the system may be realized through a variety of means, some of which include an Internet connection, a cell phone, a PDA with connectivity, a TV with connectivity, a car radio with cell phone connectivity, a GPS car navigation system with connectivity, etc. Implementation of this system requires expansion of the system resources in order to cope with increased access and processing demands. It also requires a large base of embedded broadcast content in order to provide sufficient diversity in the database of stored advertisements.

[0073] Based on the port of entry and capabilities of devices available to the consumer, the commercials may be replayed in full or referenced in an abbreviated manner (e.g., www address, phone number, etc.). The user interface can also have sorting and searching capabilities and may even automatically alert the user if a commercial is played that meets a pre-selected criterion tailored to the user's liking. Other possibilities include printing out the commercial in text form (via for example, conversion of the audio log segments to text form via voice-to-text software), automatically dialing a phone number, mapping the location of the advertiser on a GPS navigation system, or even buying the product.

[0074] One advantage of the above system is that commercials need to only air in one medium (for example, on the local AM station) yet, they can be made available to a wide range of audiences that access the system's repository. Further extensions can involve inclusion of print media commercials into the system; metadata for all local print media may be routed

to the local monitoring station or directly to the Control Center.

[0075] As is evident from the foregoing description, certain other aspects of the invention are not limited to the particular details of the embodiments illustrated, and it is therefore contemplated that other modifications and applications will occur to those skilled in the art.

What is claimed is:

1. A method for monitoring broadcast multi-media content, comprising the steps of:
 - (a) receiving multimedia source content;
 - (b) generating identification information related to the source content;
 - (c) imperceptibly and repeatedly embedding the audio component of said multimedia source content with said identification information;
 - (d) transferring said identification information to a central repository; and
 - (e) transmitting the embedded multimedia content through one or more broadcast networks.
2. The method of claim 1, further comprising:
 - (f) receiving the transmitted multimedia content; and
 - (g) processing said received multimedia content to extract identification information related thereto.
3. The method of claim 1, wherein a detectability metric is produced by assessing the success of said embedding and the detectability metric together with said identification information is transferred to a central repository.
4. The method of claim 2, wherein extraction of the identification information is conducted in the presence of multiple transmission channel impairments.
5. The method of claim 1, wherein said embedding is repeated in the temporal domain.
6. The method of claim 1, wherein said embedding is repeated at different frequencies.

7. The method of claim 1, wherein said embedding is repeated in both the temporal and frequency domains.

8. The method of claim 2, wherein multiple copies of embedded information are extracted to improve the reliability of multimedia monitoring.

9. The method of claim 2, wherein multiple copies of embedded information are extracted to estimate the duration of multimedia content embedded with identification information.

10. The method of claim 8, wherein said multiple copies are extracted from the multimedia content received from a single transmission channel.

11. The method of claim 8, wherein said multiple copies are extracted from the multimedia content received from a plurality of transmission channels.

12. The method of claim 8, wherein said multiple copies are extracted using a redundant network of receivers.

13. The method of claim 12, wherein said redundant receivers are deployed in separate geographical locations.

14. The method of claim 1, wherein the embedded multimedia content is transmitted over at least one terrestrial broadcast channel.

15. The method of claim 1, wherein the embedded multimedia content is transmitted over at least one Internet broadcast channel.

16. The method of claim 1, wherein the embedded multimedia content is transmitted over at least one cable broadcast channel.

17. The method of claim 1, wherein the embedded multimedia content is

transmitted over at least one satellite broadcast channel.

18. The method of claim 2, wherein said extracted identification information is used to identify at least one of:

- (i) broadcast advertisement content,
- (ii) broadcast music content,
- (iii) broadcast television or radio program content.

19. The method of claim 1, wherein:

copies of embedded information are extracted from the transmitted multimedia content, and

spacing of the extracted copies is used to estimate boundaries of back-to-back encoded multimedia clips.

20. The method of claim 1, wherein:

the transmitted multimedia content is received; and

the effectiveness of monitoring is enhanced by measuring received transmission channel characteristics to provide a measure of the quality of at least one of a received transmission or a transmission channel.

21. The method of claim 20, wherein said received transmission channel characteristics comprise at least one of Signal-to-Noise-Ratio (SNR) and dropped packet rate.

22. The method of claim 1, wherein the detectability metric is used at monitoring sites to improve the reliability of detection reports.

23. The method of claim 1, wherein the detectability metric and measured transmission channel characteristics are used at monitoring sites to improve the reliability of multimedia monitoring.

24. The method of claim 23, wherein said received transmission channel

characteristics comprise at least one of Signal-to-Noise-Ratio (SNR) and dropped packet rate.

25. The method of claim 1, wherein the identification information is re-embeddable with modified embedding strength based on the detectability metric.

26. The method of claim 1, wherein the type and extent of impairments present in a transmission channel are identified based on the quality of information extracted from the embedded multimedia content carried on said channel.

27. The method of claim 1, wherein multiple points of origin of a composite transmission of said embedded multimedia content are differentiated.

28. The method of claim 27, wherein said multiple points of origin comprise at least one of:

- (i) a local broadcast segment of a given networked television broadcast,
- (ii) a regional broadcast segment of a given networked television broadcast,
- (iii) a national broadcast segment of a given networked television broadcast,
- (iv) an interstitially inserted advertisement in an Internet stream.

29. The method of claim 1, wherein prior to the transmission of multimedia content in step (f), the multimedia content is examined for the presence of a valid watermark.

30. The method of claim 29, wherein the validity of an embedded watermark is ascertained by verifying the embedded identification information against information residing in a database.

31. A system for monitoring broadcast multi-media content, said system comprising:

- (a) a receiver for receiving multimedia source content;
- (b) identification information generating means for generating identification information related to the source content;
- (c) an embedder for imperceptibly and repeatedly embedding an audio component of said multimedia source content with said identification information;
- (d) transfer means for transferring said identification information to a central repository;
- (e) a transmitter for broadcasting the embedded multimedia content through one or more broadcast networks;
- (f) reception means for receiving said broadcast multimedia content; and
- (g) a processor for processing the received broadcast multimedia content to extract identification information related thereto.

32. The multimedia monitoring system of claim 31, further comprising watermark assessment means for producing a detectability metric by assessing the success of said embedding and transfer means for transferring said detectability metric together with said identification information to a central repository.

33. The multimedia monitoring system of claim 31, wherein extraction of embedded information is conducted in the presence of multiple transmission channel impairments.

34. The multimedia monitoring system of claim 31, wherein said embedding is repeated in the temporal domain.

35. The multimedia monitoring system of claim 31, wherein said embedding is repeated in different frequency domains.

36. The multimedia monitoring system of claim 31, wherein said embedding is repeated in both the temporal and frequency domains.

37. The multimedia monitoring system of claim 31, wherein extraction of multiple

copies of embedded information is used to improve the reliability of multimedia monitoring.

38. The multimedia monitoring system of claim 31, wherein extraction of multiple copies of embedded information is used to estimate a duration of multimedia content embedded with identification information.

39. The multimedia monitoring system of claim 38, wherein said multiple copies are extracted from the multimedia content received from a single transmission channel.

40. The multimedia monitoring system of claim 38, wherein said multiple copies are extracted from the multimedia content received from a plurality of transmission channels.

41. The multimedia monitoring system of claim 38, wherein said multiple copies are extracted using a redundant network of receivers.

42. The multimedia monitoring system of claim 41, wherein said redundant receivers are deployed in separate geographical locations.

43. The multimedia monitoring system of claim 31, wherein at least one transmission channel for the broadcast multimedia content is a terrestrial broadcast channel.

44. The multimedia monitoring system of claim 31, wherein at least one transmission channel for the broadcast multimedia content is an Internet broadcast channel.

45. The multimedia monitoring system of claim 31, wherein at least one transmission channel for the broadcast multimedia content is a cable broadcast channel.

46. The multimedia monitoring system of claim 31, wherein at least one

transmission channel for the broadcast multimedia content is satellite broadcast channel.

47. The multimedia monitoring system of claim 31, wherein said extracted identification information is used to identify at least one of:

- (i) broadcast advertisement content,
- (ii) broadcast music content,
- (iii) broadcast television or radio program content.

48. The multimedia monitoring system of claim 31, wherein spacing of extracted copies of embedded information is used to estimate the boundaries of back-to-back encoded multimedia clips.

49. The multimedia monitoring system of claim 31, wherein the effectiveness of monitoring is enhanced by measuring received transmission channel characteristics to provide a measure of the quality of at least one of a received transmission or a transmission channel.

50. The multimedia monitoring system of claim 49 wherein said channel characteristics comprise at least one of Signal-to-Noise-Ratio (SNR) and dropped packet rate.

51. The multimedia monitoring system of claim 31, wherein the detectability metric is used at monitoring sites to improve the reliability of detection reports.

52. The multimedia monitoring system of claim 31, wherein the detectability metric and measured transmission channel characteristics are used at the monitoring sites to improve the reliability of multimedia monitoring.

53. The multimedia monitoring system of claim 31, wherein the identification information is re-embeddable with a modified embedding strength based on the detectability metric.

54. The multimedia monitoring system of claim 31, wherein the type and extent of impairments present in a transmission channel for the broadcast multimedia content are identified based on a quality of extracted information from the embedded multimedia content.

55. The multimedia monitoring system of claim 31, wherein multiple points of origin of a composite transmission of said embedded multimedia content are differentiated.

56. The multimedia monitoring system of claim 55, wherein said multiple points of origin comprise at least one of:

- (i) a local broadcast segment of a given networked television broadcast,
- (ii) a regional broadcast segment of a given networked television broadcast,
- (iii) a national broadcast segment of a given networked television broadcast,
- (iv) an interstitially inserted advertisement in an Internet stream.

57. The multimedia monitoring system of claim 31, wherein prior to the transmission of multimedia content in step (f), the multimedia content is examined for the presence of a valid watermark.

58. The system in accordance with claim 57, wherein the validity of an embedded watermark is ascertained by verifying the embedded identification information against information residing in a database.

59. A method for real-time embedding of identification information into an audio component of multimedia content, comprising:

- separating the audio component from a video component of said content;
- embedding the audio component imperceptibly and repeatedly with identification information; and
- combining the video component with the embedded audio component so that

synchronization between video frames and the corresponding audio component is preserved.

60. The method of claim 59, wherein said audio component is in analog form, is converted into digital form prior to embedding, and is converted back into analog form after said embedding.

61. The method of claim 59, wherein multiple audio components are embedded.

62. Apparatus for real-time embedding of identification information into an audio component of multimedia content, comprising:

an audio-video separator for separating audio and video components of said content;

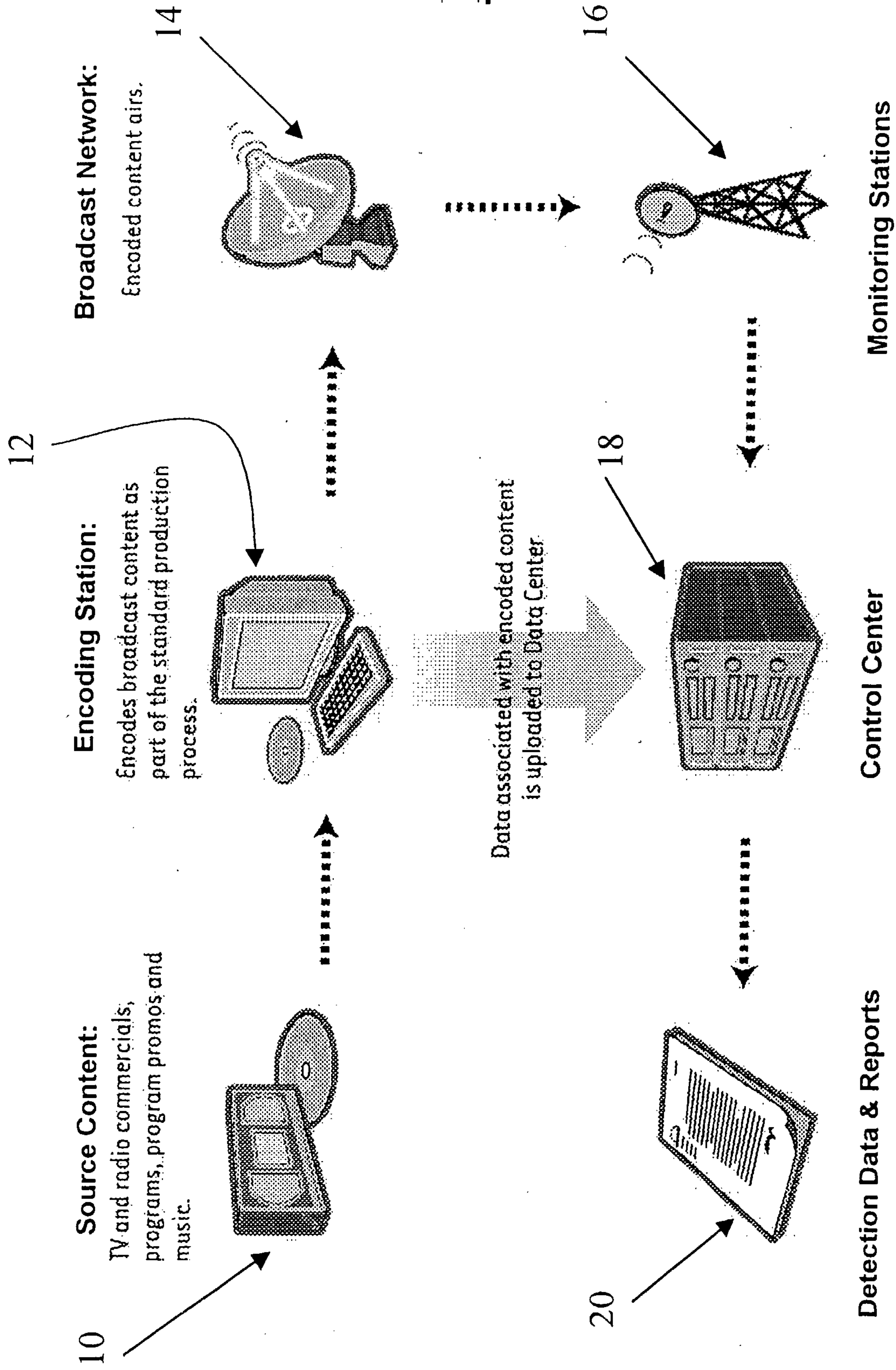
an audio watermark embedder for embedding the audio component imperceptibly and repeatedly with identification information; and

an audio-video combiner for combining the video component with the embedded audio component so that synchronization between video frames and the corresponding audio component is preserved.

63. Apparatus in accordance with claim 62, wherein an analog-to-digital converter is used to convert said audio component into digital form prior to embedding, and a digital-to-analog converter is used to convert the audio component back into analog form after said embedding.

64. Apparatus in accordance with claim 62, wherein multiple audio components are embedded.

FIG. 1



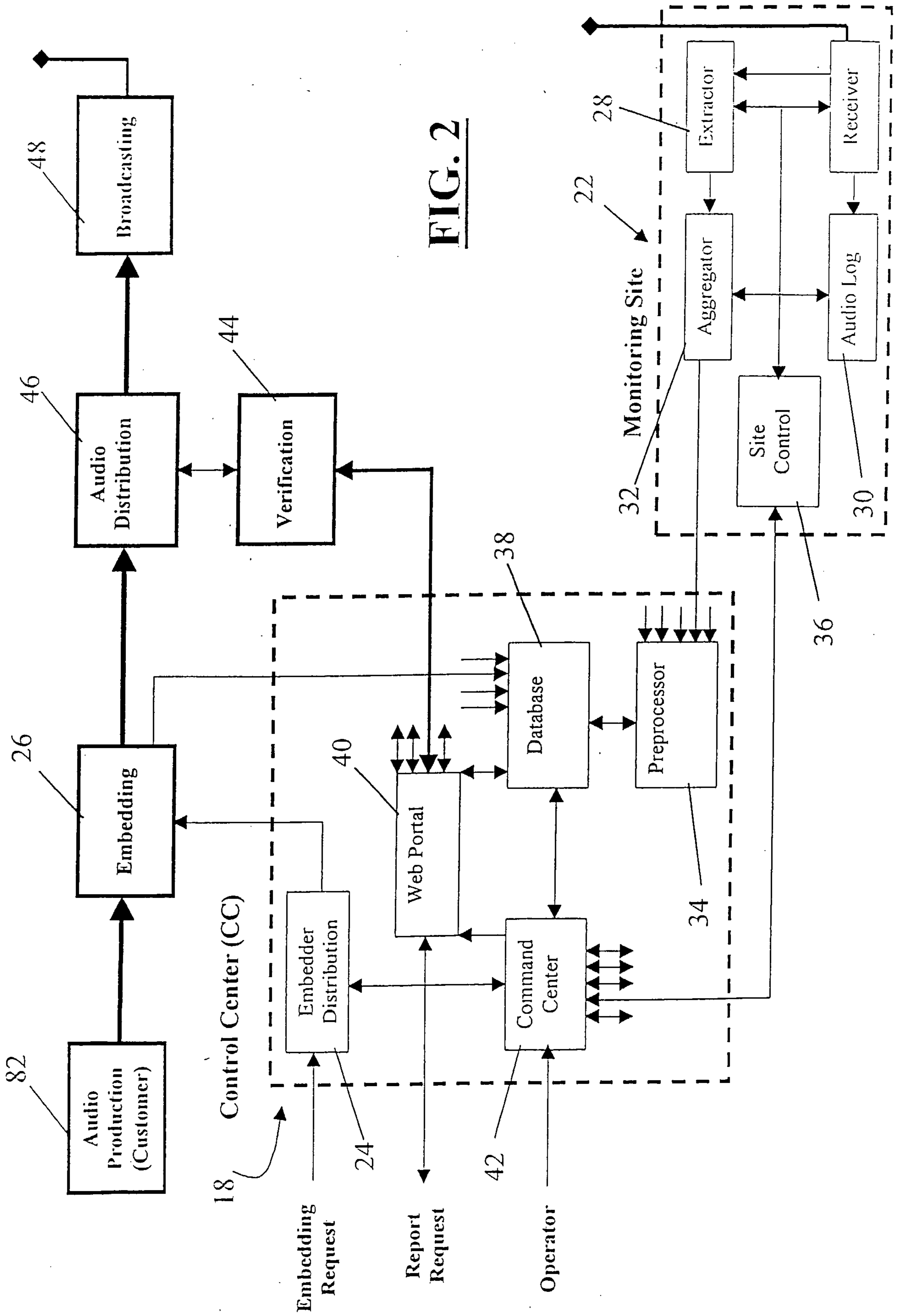


FIG. 2

3/9

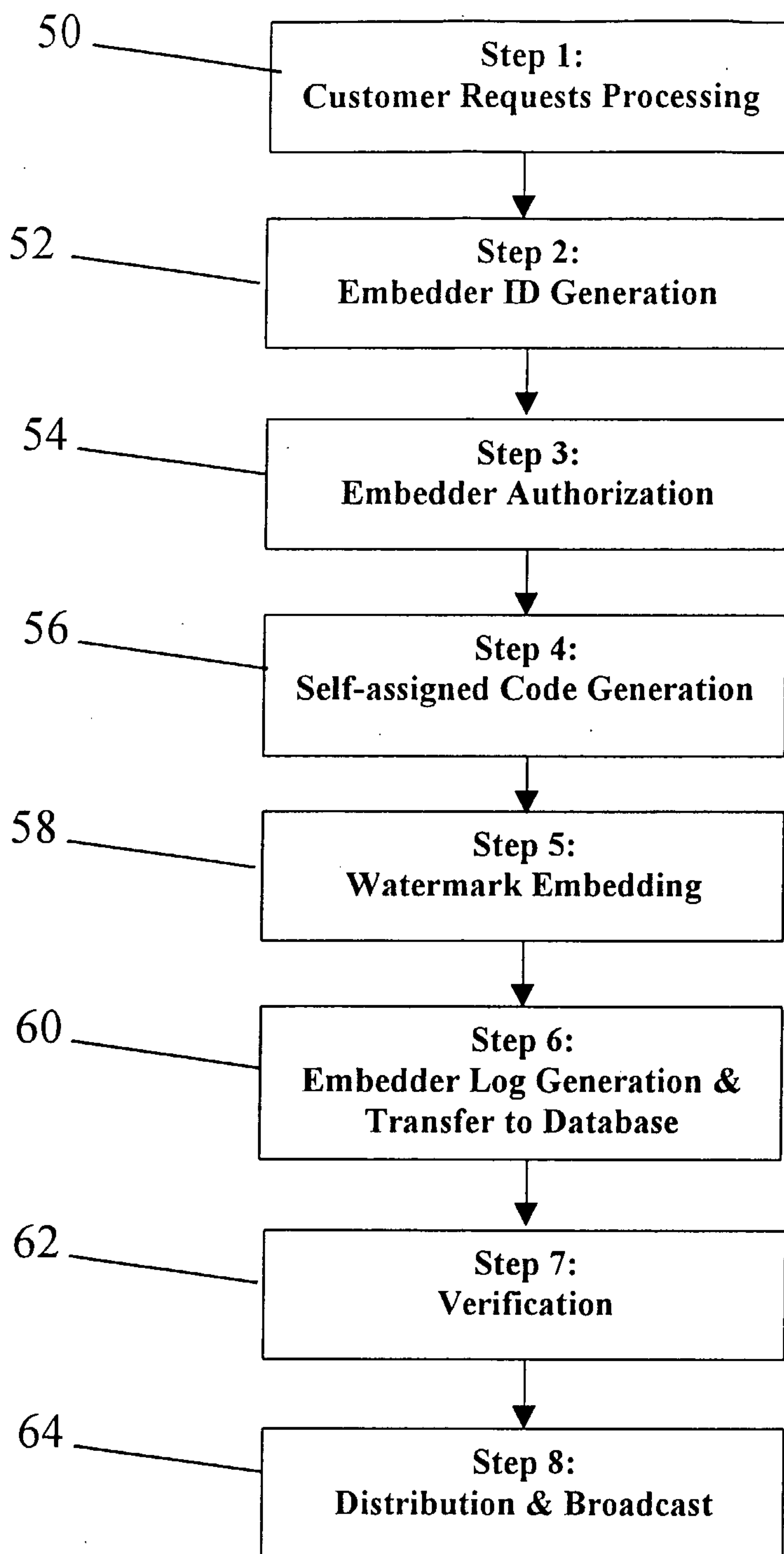


FIG. 3

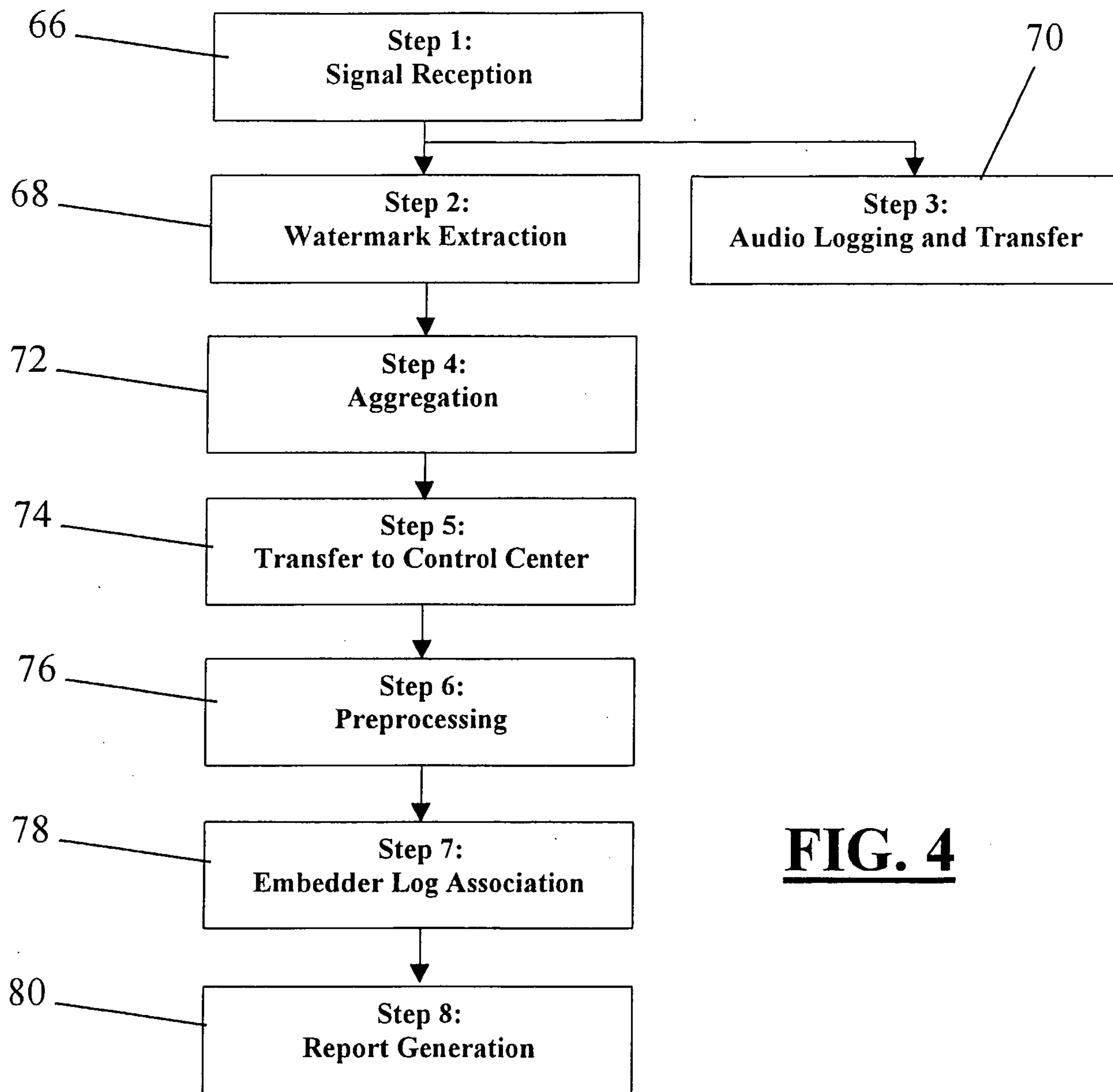


FIG. 4

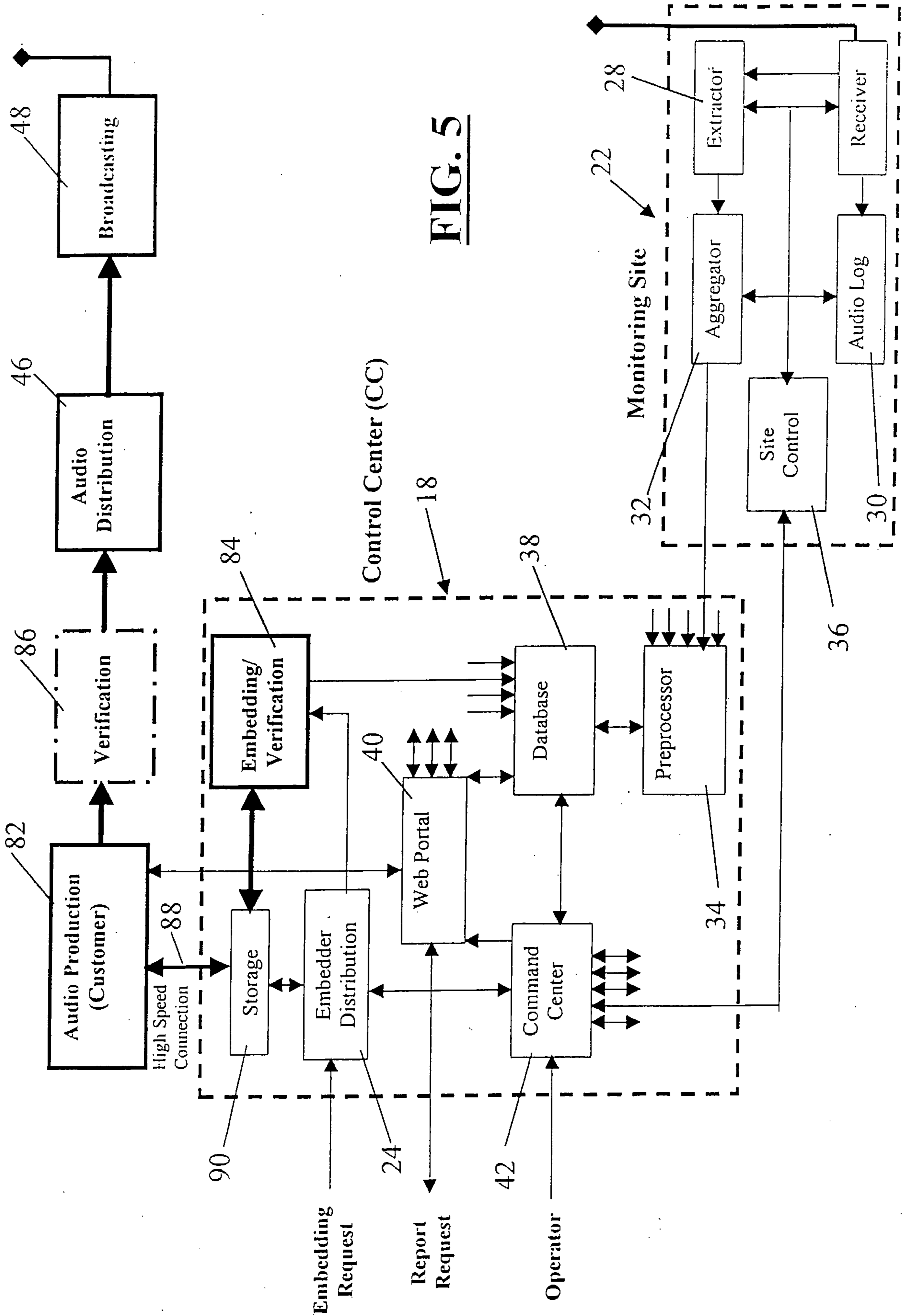


FIG. 5

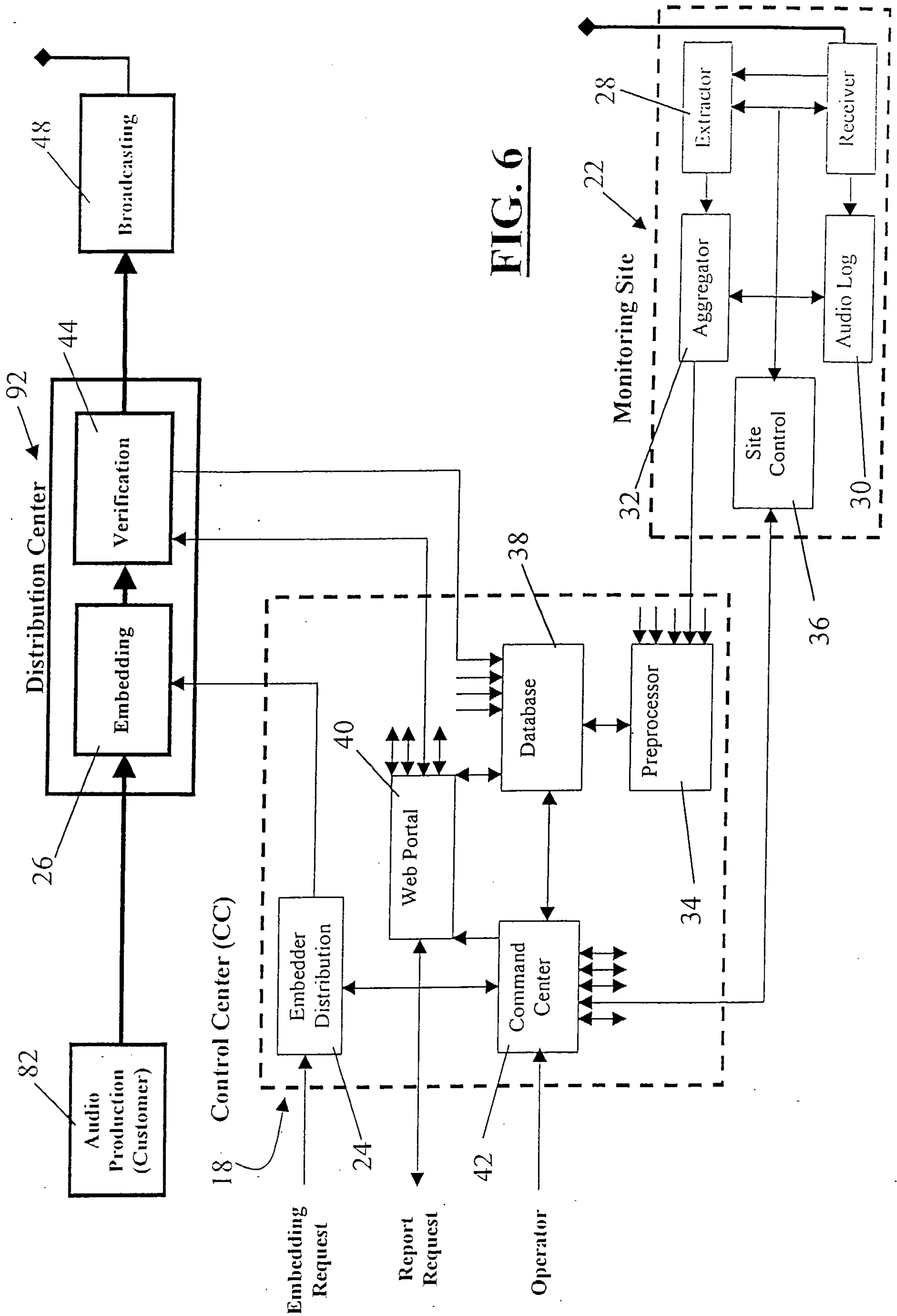


FIG. 6

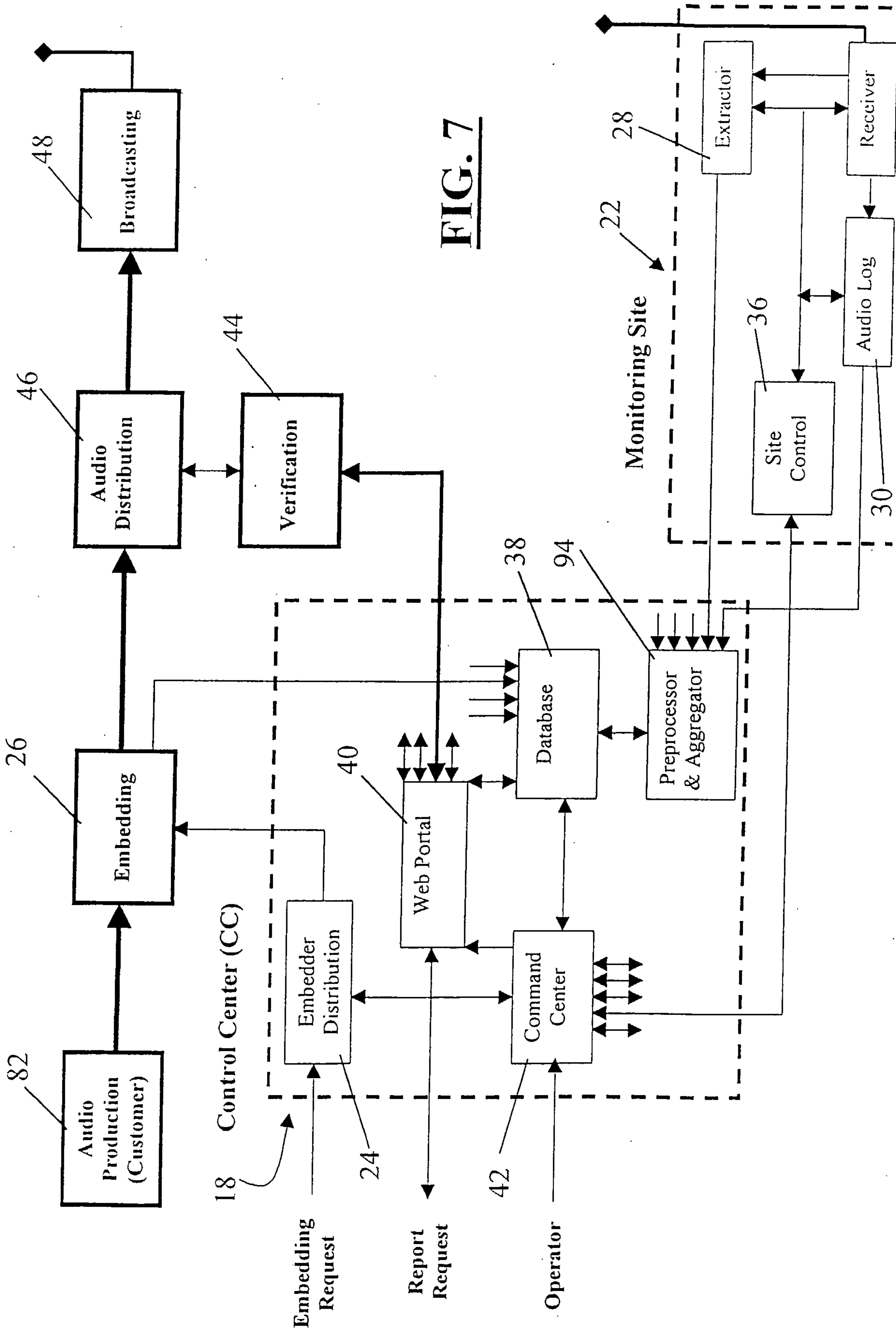
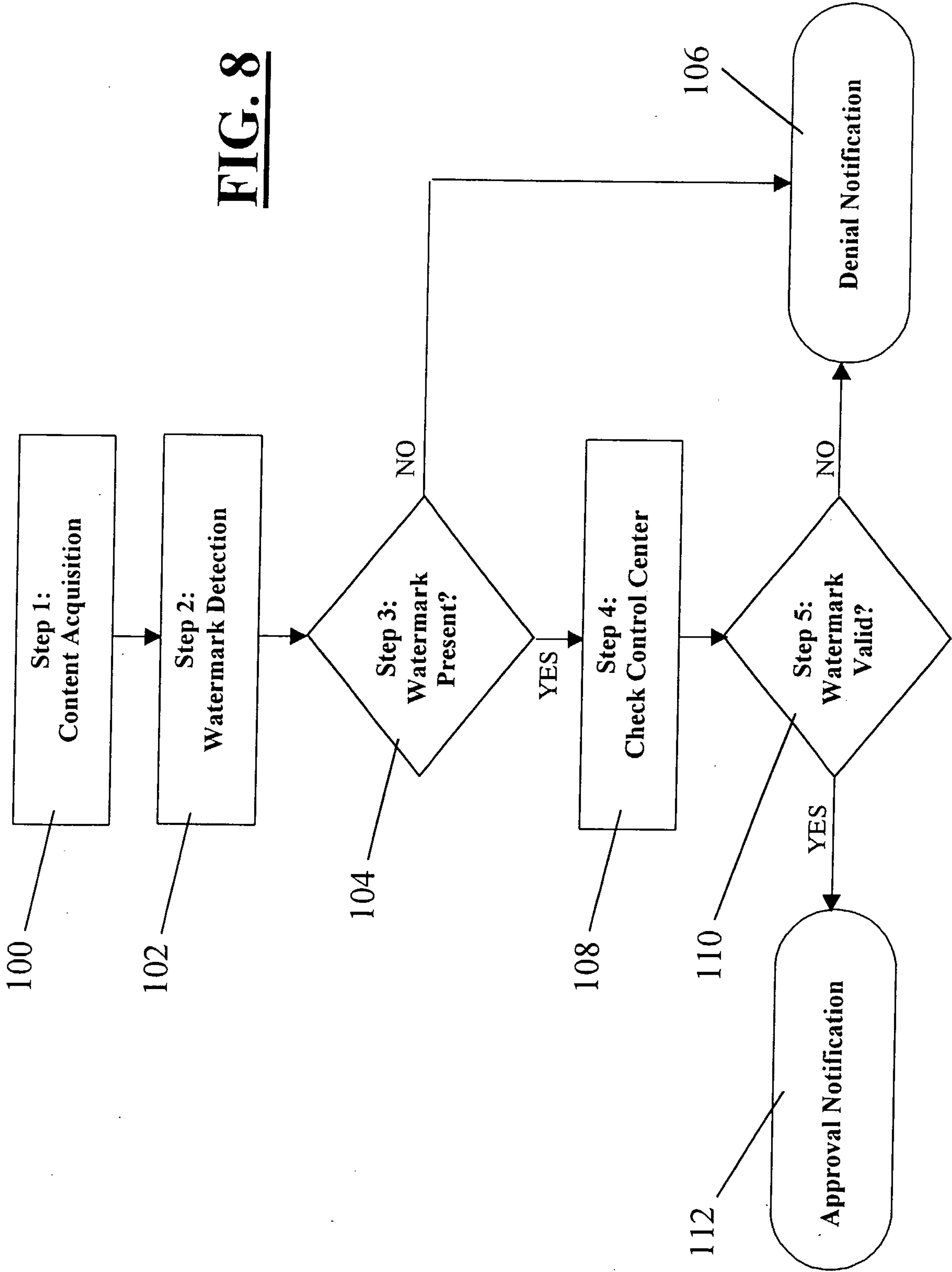


FIG. 7

FIG. 8



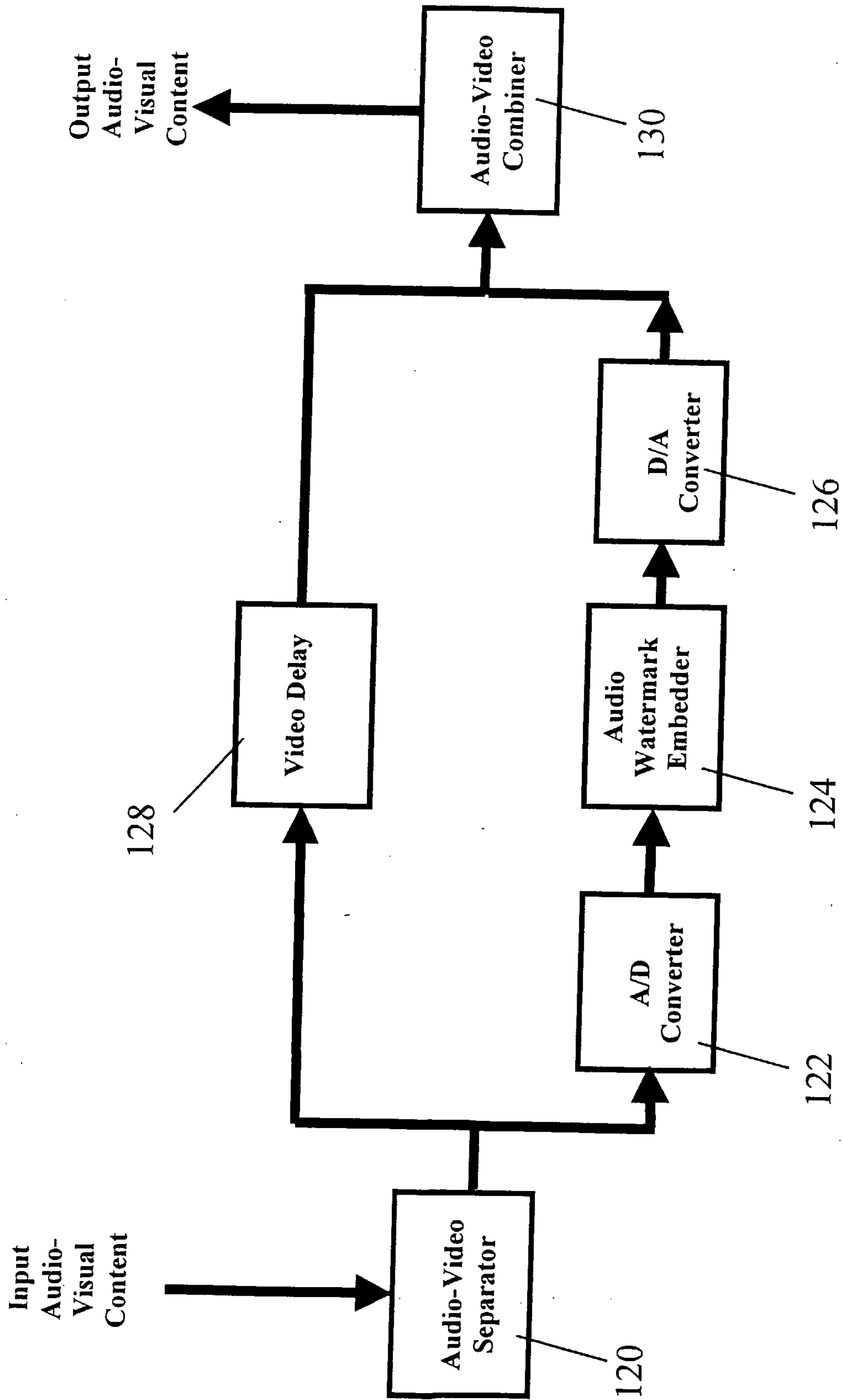


FIG. 9

