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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 July 2005 (28.07.2005)

PCT

(10) International Publication Number
WO 2005/067538 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2005/001334

(22) International Filing Date: 13 January 2005 (13.01.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/536,144	13 January 2004 (13.01.2004)	US
60/536,133	13 January 2004 (13.01.2004)	US

(71) Applicant *(for all designated States except US)*: **INTERDIGITAL TECHNOLOGY CORPORATION** [US/US]; 300 Delaware Avenue, Suite 527, Wilmington, DE 19801 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KAEWELL, John, David Jr.** [US/US]; 1727 Lafayette Drive, Jamison, PA 18929 (US). **CHITRAPU, Prabhakar, R.** [US/US]; 135 Brochant Drive, Blue Bell, PA 19422 (US). **OLESEN, Robert, Lind** [US/US]; 3 Country Club Drive, Huntington, NY 11743 (US). **SHIN, Sung-Hyuk** [US/US]; 104 Eider Way, Northvale, NJ 07647 (US). **HOFFMANN, John, Erich** [US/US]; 516 Latania Palm Drive, Indialantic, FL 32903-3816 (US). **REZNIK, Alexander** [US/US]; 1212 River Road, Titusville, NJ 08560 (US).

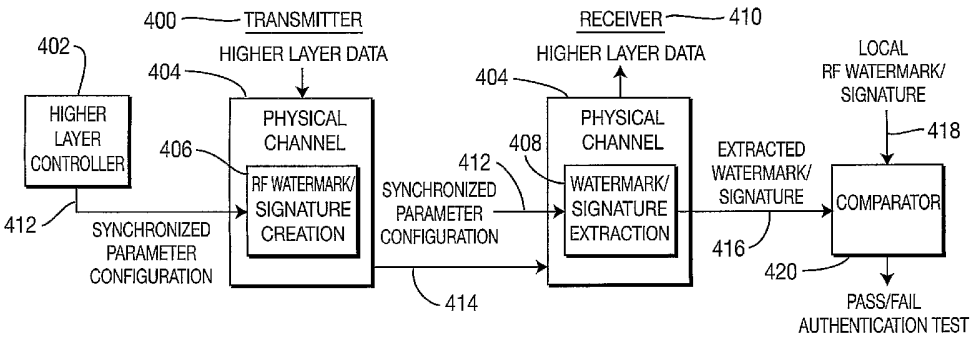
(74) Agent: **BALLARINI, Robert, J.**; Volpe and Koenig, P.C., United Plaza, Suite 1600, 30 S. 17th Street, Philadelphia, PA 19103 (US).

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

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

[Continued on next page]

(54) Title: CODE DIVISION MULTIPLE ACCESS (CDMA) METHOD AND APPARATUS FOR PROTECTING AND AUTHENTICATING WIRELESSLY TRANSMITTED DIGITAL INFORMATION



(57) Abstract: A spread spectrum method and apparatus for protecting and authenticating wirelessly transmitted digital information using numerous techniques. The apparatus may be a wireless code division multiple access (CDMA) communication system, a base station, a wireless transmit/receive unit (WTRU), a transmitter, a receiver and/or an integrated circuit (IC). The wireless CDMA communication system includes a transmitter which steganographically embeds digital information in a CDMA communication signal and wirelessly transmits the CDMA communication signal. The system further includes a receiver which receives the CDMA communication signal and extracts the steganographically embedded digital information from the received CDMA communication signal.

WO 2005/067538 A2

Published:

— *without international search report and to be republished upon receipt of that report*

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.

[0001] # CODE DIVISION MULTIPLE ACCESS (CDMA) METHOD AND APPARATUS FOR PROTECTING AND AUTHENTICATING WIRELESSLY TRANSMITTED DIGITAL INFORMATION

[0002] ## FIELD OF INVENTION

[0003] The present invention is related to a wireless communication system. More particularly, the present invention is related to using SS techniques, e.g., code division multiple access (CDMA), to protect and authenticate digital information transmitted to and received from a user's wireless transmit/receive unit (WTRU).

[0004] ## BACKGROUND

[0005] Wireless systems are susceptible in many respects. These susceptibilities are increasing as new wireless technologies are growing in prevalence. Ad-hoc networks, where individual users communicate with each other directly without using intermediary network nodes, creates new susceptibilities to the users and networks. These susceptibilities can be categorized as "trust", "rights", "identity", "privacy" and "security" related issues.

[0006] "Trust" refers to the assurance that information communicated in these systems can be shared. To illustrate, a wireless user may want to know that a communication was sent to it from a trusted source and using trusted communication nodes. The user in an ad-hoc network may have no knowledge that the communication was transferred over a hacker's wireless device with packet sniffing software. Additionally, with the use of tunneling, intermediate nodes transferring the communication may be transparent to the wireless user.

[0007] "Rights" ("rights management") refers to the control of data. To illustrate, one wireless user may have limited rights in a wireless system. However, if that user colludes (knowingly or unknowingly) with a second node having superior rights, that user may gain rights above those that the user is allowed.

[008] "Identity" refers to the control linked to the identity of the wireless user. To illustrate, a rogue wireless device may attempt to access a wireless network by pretending to be an authorized user of the network, by using that authorized user's identity. "Privacy" refers to maintaining privacy of the individual, data and context. A wireless user may not want others to know, which web sites he/she visits and, in particular, information sent to these sites, such as financial, medical, etc. "Security" refers to the security of the data and context, such as preventing an unauthorized individual access to a wireless user's information.

[009] To reduce the susceptibility of wireless networks, various techniques are used. Although these techniques provide some protection, they are still susceptible to the trusts, rights, identity, privacy and security issued. For example, although a particular wireless communication node may have the correct keys to communicate with a wireless user, that user may not know whether the node can be trusted.

[0010] Additionally, authentication of the user using these keys typically occurs at higher layers of the communication stack. Accordingly, even when these controls are in place, a rogue wireless user or hacker may have some (although limited) access to the communication stack. This access creates vulnerabilities, such as to denial of service attacks, among others.

[0011] Steganography is the art of passing information in a manner that the very existence of the message is unknown. The goal of steganography is to avoid drawing suspicion to the transmission of a hidden message. If suspicion is raised, then this goal is defeated. Steganography encompasses methods of transmitting secret messages through innocuous cover carriers in such a manner that the very existence of the embedded messages is undetectable. Creative methods have been devised in the hiding process to reduce the visible detection of the embedded messages.

[0012] Watermarking is a well-known technique for protecting and tracking digital information, which has been successfully exploited in the area of music and video data storage and communication. The traditional framework for

watermarking consists of three elements: 1) cover signal s, 2) watermark w, 3) embedding function E and 4) secret key k. The watermarked signal is then defined as $s_w = E_k\{s, w\}$. The watermark carrying signal s_w must be robust to common signal processing operations such as filtering, compression or any other operation that are the basic functionalities of the network. Robustness is defined by the ability to extract the watermark from an altered signal. The second requirement of any watermarking scheme is imperceptibility, (i.e., the difference between s and s_w must not alter the operation of the system in any perceptible manner). The watermark must also be transparent in the sense that the watermark-unaware portions of the network must be able to process s_w without additional hardware or software. The watermark must also be secure even though the watermarking algorithm itself may be public. This security is frequently achieved through a secret key that is exchanged with the receiver through some form of secure key exchange.

[0013] In the prior art, the concept of digital watermarking is used in information assurance and User Authentication. A watermark is embedded into the user data, which is then transported by the physical layer of the communication link. The recipient extracts the watermark and compares it with a local copy to authenticate the transmitter.

[0014] Watermarks and signatures are techniques for adding metadata or unique information to media for signaling and/or security purposes. To reduce these susceptibilities to wireless communications, it is desirable to have alternate approaches to watermarking and adding signatures to wireless communications.

[0015] SUMMARY

[0016] The present invention is related to a spread spectrum method and apparatus for protecting and authenticating wirelessly transmitted digital information using numerous techniques. The apparatus may be a wireless CDMA communication system, a base station, a WTRU, a transmitter, a receiver and/or an integrated circuit (IC).

[0017] The wireless CDMA communication system includes a transmitter which steganographically embeds digital information in a CDMA communication signal and wirelessly transmits the CDMA communication signal. The system further includes a receiver which receives the CDMA communication signal and extracts the steganographically embedded digital information from the received CDMA communication signal. The digital information may comprise at least one token, at least one key, at least one watermark or at least one signature.

[0018] The transmitter may embed the digital information in a frame quality indicator. The frame quality indicator may include a cyclic redundancy check (CRC).

[0019] The transmitter may embed the digital information in at least one encoder tail bit or at least one reserved/erasure indicator.

[0020] In one embodiment, at the transmitter, a slow scrambled code jitter is applied with respect to a carrier frequency and frequency-shift keying (FSK) modulation of the digital information placed on top of the jitter. The digital information may be mapped to a predefined frequency offset. At the receiver, a local descrambler in the receiver is synchronized to generate the same code jitter and a local carrier demodulator is then synchronized to generate the mapped/applied frequency offset.

[0021] In another embodiment, at the transmitter, particular chips are selected in at least one of a scrambling code and a channelization code, and the digital information is embedded in the selected chips. At the receiver, the particular chips are determined and the digital information is extracted from the particular chips.

[0022] In yet another embodiment, at the transmitter, the digital information is mapped to physical channel combinations based on at least one channelization code and a spreading factor (SF) according to a predefined rule. The channelization code may be an orthogonal variable spreading factor (OVSF) code.

[0023] In yet another embodiment, the digital information is represented as a relative gain or power offset between any pair of channelization codes.

[0024] In yet another embodiment, the digital information is mapped as a delay of a channelization code transmission.

[0025] In yet another embodiment, the transmitter may embed the digital information in a pilot channel and/or in certain pilot symbols in the pilot channel. The receiver may extract the digital information from the certain pilot symbols in the pilot channel.

[0026] In yet another embodiment, the transmitter may embed the digital information in a control channel or a data channel.

[0027] In yet another embodiment, the transmitter includes two antennas, and the transmitter embeds the digital information in two different data symbols every other symbol period. The two different data symbols are simultaneously transmitted by the respective ones of the two antennas.

[0028] In yet another embodiment, the digital information is directly transported by defining a new physical channel or field.

[0029] In yet another embodiment, the digital information is treated as dirty paper coding (DPC) encoded information, and any other CDMA signals are treated as side information.

[0030] In yet another embodiment, bits of the digital information are combined with bits of a CRC.

[0031] In yet another embodiment, the digital information is used to initialize a shift register of a CRC generator prior to CRC generation for data.

[0032] In yet another embodiment, the digital information is used to initialize a shift register of a forward error correction (FEC) encoder prior to channel coding for data.

[0033] In yet another embodiment, bits of an FEC output are punctured, bits of the digital information are inserted in locations of the punctured bits and a CRC output embedded with the digital information bits is provided. The receiver extracts the digital information from the punctured bit locations of the FEC output.

[0034] In yet another embodiment, tail bits of an FEC output are encoded with the digital information rather than being set to a binary value of zero.

[0035] In yet another embodiment, the digital information is used to mask an FEC output.

[0036] In yet another embodiment, at the transmitter, a transport channel (TrCH) is inputted, a set of transport formats for the input TrCH is determined, the digital information and a least one mapping rule is inputted, a transport format is selected from the transport format set based on the digital information and the at least one mapping rule and the selected transport format is used to transmit the TrCH.

[0037] In yet another embodiment, the transmitter sends the digital information during the transmission gaps of the CDMA communication signal when it is in a compressed mode.

[0038] In yet another embodiment, the transmitter sends the digital information during a period of an activated discontinuous transmission mode using a predetermined transport format.

[0039] The transmitter may embed the digital information in the CDMA communication signal as a watermark in a transmitting (TX) layer 2/3, a TX physical layer, and/or a TX radio frequency (RF) layer.

[0040] The receiver may extract the digital information from the CDMA communication signal using a receiving (RX) layer 2/3 processing device, an RX physical layer processing device and/or an RX RF processing device.

[0041] BRIEF DESCRIPTION OF THE DRAWINGS

[0042] A more detailed understanding of the invention may be had from the following description, given by way of example and to be understood in conjunction with the accompanying drawings wherein:

[0043] Figure 1A shows a traditional digital communication transmitting system;

[0044] Figure 1B shows a watermarking digital communication system configured in accordance with the present invention;

[0045] Figure 1C is an exemplary block diagram of a wireless communication system configured in accordance with the present invention;

[0046] Figure 2 is a flow diagram of a process including method steps for watermarking wireless communications in accordance with the present invention;

[0047] Figure 3 is a block diagram of a system that creates physical channels in order to transmit and receive watermark/signature information in accordance with the present invention;

[0048] Figure 4 is a block diagram of a system that performs RF watermark/signature creation and extraction in accordance with the present invention;

[0049] Figure 5 illustrates that watermarks may be incorporated into a CRC and tail bits of a CDMA reverse fundamental channel in accordance with the present invention in accordance with the present invention;

[0050] Figure 6 illustrates the frame structure of the CDMA reverse fundamental channel of Figure 5;

[0051] Figure 7 illustrates a CDMA reverse fundamental channel and reverse supplemental channel structure in which watermarks may be incorporated into reserved bits, CRC and tail bits of the structure in accordance with the present invention;

[0052] Figure 8 shows a spreader for spreading CDMA data channels in accordance with one embodiment of the present invention;

[0053] Figure 9 shows a modulator for modulating signals received from the spreader of Figure 8 in accordance with one embodiment of the present invention;

[0054] Figure 10 illustrates an FSK modulation-based watermarking system using scrambling code jitter in accordance with one embodiment of the present invention;

[0055] Figure 11 shows a code-tree for generation of OVSF codes;

[0056] Figure 12 illustrates utilizing channelization code and SF for watermarking in accordance with one embodiment of the present invention;

[0057] Figure 13 illustrates spread data chip sequences with difference gains;

[0058] Figure 14 is a flow diagram of a process including method steps for utilizing a gain offset between a pair of channelization codes for watermarking in accordance with one embodiment of the present invention;

[0059] Figure 15A illustrates a space-time block coding (STBC) encoder structure in accordance with one embodiment of the present invention;

[0060] Figure 15B illustrates a space-frequency block coding (SFBC) encoder structure in accordance with one embodiment of the present invention;

[0061] Figure 16A illustrates an exemplary dirty paper coding (DPC) system using a simple adder (or modular summer);

[0062] Figure 16B illustrates an exemplary dirty paper coding (DPC) system using a watermarking embedding device in accordance with one embodiment of the present invention;

[0063] Figure 17 illustrates transport channel multiplexing structure for 3GPP uplink in accordance with one embodiment of the present invention;

[0064] Figure 18 illustrates CRC based watermarking in accordance with one embodiment of the present invention;

[0065] Figure 19A shows a rate 1/2 convolutional coder;

[0066] Figure 19B shows a rate 1/3 convolutional coder;

[0067] Figure 20 illustrates FEC redundant bits replacement for watermarking in accordance with one embodiment of the present invention;

[0068] Figure 21 shows an example of a watermark embedded FEC output in accordance with one embodiment of the present invention;

[0069] Figure 22 is a flow diagram of a process including method steps for selecting the format of a TrCH based on watermark information and at least one mapping rule in accordance with one embodiment of the present invention; and

[0070] Figure 23 shows an example of using a watermark in a compressed mode in accordance with one embodiment of the present invention.

[0071] DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0072] The present invention is applicable to communication systems using spread spectrum, (e.g., CDMA, CDMA 2000, time division synchronous CDMA

(TDSCDMA)), universal mobile telecommunications system (UMTS) frequency division duplex (FDD) - time division duplex (TDD), orthogonal frequency division multiplexing (OFDM) or the like. However, the present invention is envisioned to be applicable for incorporation into any type of communication system.

[0073] The present invention may be implemented in a WTRU or in a base station. The terminology "WTRU" includes but is not limited to user equipment (UE), a mobile station, a fixed or mobile subscriber unit, a pager, or any other type of device capable of operating in a wireless environment. The terminology "TRU" may be any type of wireless communication device (e.g., a WTRU) or any type of non-wireless communication device. The terminology "base station" includes but is not limited to a Node-B, a site controller, an access point or any other type of interfacing device in a wireless environment.

[0074] The features of the present invention may be incorporated into an IC or be configured in a circuit comprising a multitude of interconnecting components.

[0075] The present invention discloses methods to implement Information Assurance (IA); Authentication (of User, WTRU, and base station), Data Confidentiality, Data Integrity and Network Availability. The present invention discloses IA implemented based on RF watermarking. Embedded physical channels (EPCHs) can be used to transport security related data from higher layers. The EPCHs may include watermarks or signatures (permanent or temporary) associated with users, WTRUs, and/or base stations. Depending upon the security level of the EPCHs, they may be sent in the clear or encrypted by higher layer schemes. The EPCHs may also be used to transport 'challenge-words' for generating session keys, which may be used for encryption or for specifying the structure of EPCHs. The advantage of the embedded channel approach is that it is better suited for long-term continual application, such as periodic authentication etc. Furthermore, the use of EPCHs (as opposed to regular physical channels, for example) allows security operations to be performed in a manner that is transparent to higher layer data or data processing. This implies that higher layer software and applications do not need

to be modified. Finally, the operational load of the higher layer processing remains unaffected.

[0076] RF watermarks/signatures are powerful concepts that can be used for authentication, data confidentiality as well as data integrity. For example, the RF watermarks/signatures could be used as keys for data encryption and for generating message authentication codes. These keys may be used by themselves or in conjunction with other security keys.

[0077] Figure 1A shows a traditional digital communication system which receives source data d_{source}, (e.g., binary data). This data may represent digitized speech or image or video signals or binary text or other digital data. This data is sometimes compressed (through a process called source coding) 76 producing a compressed binary data stream, denoted as $d_{compressed}$. The compressed data $d_{compressed}$ is processed by higher open system interconnection (OSI) layers, (e.g., hyper text transfer protocol (HTTP), transmission control protocol (TCP), Internet protocol (IP) layers, etc.) 78 producing a binary data denoted as d_{HL}. The resulting data is now processed by the OSI layers belonging to the Radio Interface, namely Layer 3 80, Layer 2 82, Layer 1 84 and Layer 0 (RF) 86. The resulting data are denoted as d_4, d_3, d_2, s_1, and s_0, respectively, where d_4, d_3 and d_2 are binary data, and s_1 and s_0 are analog signals. At the receiver side, the processing is performed similarly, but in a reverse order (Layer 0 (RF) followed by Layer 1, followed by Layer 2, followed by Layer3, followed by higher layers and then decompressed).

[0078] For the following (excluding claims), 'data' and 'signals' refer to 'binary data' and 'analog signals' respectively, unless otherwise noted.

[0079] Figure 1B shows a watermarked digital communication system including a transmitter processing chain for embedding watermarks/signatures into communicated (binary) data and/or (analog) signals. Watermarking involves binary watermark data w, cover data or signal d or s, a watermark embedding scheme/algorithm E and a watermarked data/signal d_w or s_w, such as per Equation 1.

$$s_w = E\{s,w\} \text{ or } d_w = E\{d,w\}$$

Equation (1)

[0080] The binary watermark data may be generated by digitizing an analog watermark signal. For example, the finger print or a handwritten signature is an analog signal that can be digitized to produce binary watermark data.

[0081] Since embedding allows the watermark to be communicated along with the main source data, the embedding scheme may also be viewed as defining (perhaps implicitly) an Embedded Channel into the source data itself. As such, the embedding scheme may be said to define 'watermarking channels' or 'embedded radio channels'. If these channels are defined at the Layer 1 or Layer 0 (RF), the corresponding embedded radio channels may also be referred to as 'Embedded Physical Channels'.

[0082] The watermark/signature may be embedded in content 85 (ws) prior to compression (source coding) 86; embedded in content 87 (wc) after compression (source coding) 86; embedded during higher layer processing 88 (wHL); embedded during Layer 3 89 (w3), Layer 2 90 (w2), Layer 1 91 (w1) and Layer 0 (RF) 92 (w0).

[0083] Although the following refers to watermarks, signatures may be used instead of watermarks in the same context for wireless communications. Figure 1C is an exemplary block diagram of a wireless communication system 100 and is described in conjunction with Figure 2, which is a flow diagram of a process 200 including method steps for watermarking wireless communications. A transmitting (TX) transmit/receive unit (TRU) 20 transmits user data stream(s) for wireless communication with a receiving (RX) TRU 22. The user data streams are processed using a TX layer 2/3 processing device 24 to perform layer 2/3 (data link/network) processing. Although the layer 2/3 processing is illustrated as occurring in both the TX TRU 20 and the RX TRU 22, it may alternately occur in other communication network nodes. To illustrate, in a UMTS communication system, the layer 2/3 processing may occur within a radio network controller, core network or Node-B.

[0084] The layer 2/3 processed data is physical layer processed by a TX physical layer processing device 26. The physical layer processed data is processed for radio transmission by a TX RF processing device 28.

[0085] The TX TRU 20 (or alternate network node) receives tokens/keys for producing watermarks (step 202). The tokens/keys are processed by a watermark embedding device 30, which embeds the tokens/keys as a watermark in any one or across multiple ones of the TX layer 2/3, TX physical layer and TX RF layer (step 204). The watermark embedded RF communication is transmitted by an antenna or an antenna array 32 (step 206). The watermark embedded RF communication is received over the wireless interface 36 by an antenna or antenna array 34 of the receiving (RX) TRU 22 (step 208). The received watermark embedded RF communication is RF processed by an RX RF processing device 38. The RF processed communication is physical layer processed by an RX physical layer processing device 40. The physical layer processed communication is layer 2/3 processed by an RX layer 2/3 processing device 42 to produce the user data stream(s). During any one or across multiple ones of the RF layer, physical layer or layer 2/3 processing, the embedded watermark is extracted by a watermark extraction device 44 (step 210), producing tokens/keys such as for use in authentication and other trust, rights, identity, privacy or security purposes.

[0086] The various embodiments below describe various techniques for hiding or embedding digital watermarks or signatures at the physical or RF layer of a wireless communication system. It should be understood, however, that any of the following embodiments can be implemented on any layer within the communication system.

[0087] To begin, a description is provided of two primary watermarking techniques: 1) hiding watermark information on embedded physical channels; and 2) imprinting watermark information directly into one or more existing physical channels so as to provide information assurance by creating an authenticating signature. In the first primary technique, a new channel is defined to carry a watermark and the watermark channel is then embedded in a

physical channel. To illustrate, one technique to produce such a channel is to slowly differentially amplitude modulate physical channel(s) to produce a new watermark channel co-existing with the existing physical channel(s). Watermarks are carried by these channels. This technique can be modeled as follows. The existing physical channel(s) can be viewed as a cover signal s. The watermark is w, an embedding function is E and the embedded physical channel is EPCH. The EPCH creation techniques are described below. The watermarked signal s_w may be expressed according to Equation 2 as follows:

$$s_w = E_{EPCH}\{s,w\} \quad \text{Equation (2)}$$

[0088] The first primary watermarking technique is illustrated in Figure 3. Figure 3 is a block diagram of a system, including a transmitter 300 and a receiver 308, for creating physical channels in order to transmit and receive watermark/signature information, (i.e., digital information). Transmitter 300 is shown transmitting higher layer data on physical channel 302. An embedding function creates embedded physical channel 304 in order to transmit watermark/signature information to receiver 308. The embedded physical channel 304 is transmitted under the cover of physical channel 302 to the receiver 308 via a transmission path 306. The receiver 308 extracts the watermark/signature information from the embedded physical channel 304 and compares the extracted watermark/signature information 310 with local (i.e., expected) RF watermark/signature information 322 of the receiver 308 by a comparator 320. If the comparison is positive, transmitter 300 is deemed a trusted data source and the watermark/signature information 306 is processed. Otherwise, the receiver 308 will reject all further data transmissions from the transmitter 300.

[0089] To enhance security further, the embedded physical channels may be encrypted to prevent a rogue TRU from being able to copy the watermark, if the rogue TRU is somehow aware of the embedded channel. These embedded channels may be used to carry security related data from higher OSI layers. To illustrate, encryption and other keys from higher layers are carried by the embedded channel. Other data carried on these channels may include "challenge

words", so that a TRU can authenticate itself when challenged by another TRU or the network.

[0090] The embedded physical channels preferably occur on a long-term continual basis; although non-continuous and short term embedded channels may be used. In some implementations, the watermarking channels operate on their own without data being transmitted on the underlying physical channel(s). As a result, the underlying physical channel(s) may need to be maintained, even when they have no data to transmit. The physical channel can be viewed as a cover work for the watermarking channel. Preferably, the data transmitted on the cover work physical channel is configured so that it seems typical of data transmitted on that channel. The existence of uncharacteristic data on the channel, such as a long run of zeros, may draw an eavesdropper's attention to that channel. Such data preferably mimics data actually sent on the channel, which makes it difficult for the eavesdropper to ascertain when cover data is being transmitted. Alternately, a random bit pattern may be used on the cover channel. For encrypted or scrambled channels, a random bit pattern may provide adequate security for some implementations.

[0091] In a military application, for example, the cover data transmitted may be misleading information (misinformation). If an enemy unit encounters the communication node transferring the cover information, the enemy may leave the node intact as to attempt to decode the misleading data or cover data. In one embodiment, the generation of appropriate quality cover data is preferably automated, as manual operations to produce such data may be prone to errors and difficult to implement.

[0092] The watermarking channels can be used to increase the bandwidth of the overall communication system. The bandwidth available on the watermarking channel is (in some implementations) in addition to the bandwidth of the underlying physical channel. As a result, the overall bandwidth is increased. To add further security, when multiple watermarking channels are utilized, the watermarking data hops the channels in a predetermined or

randomly determined pattern. As a result, an eavesdropper monitoring one channel may only have access to a portion of the watermark data.

[0093] The embedded physical channels can be used to allow security operations to be performed in a manner transparent to higher layers. As a result, added security can be achieved without modification to higher layer software and applications and without a change in the operational load of these layers.

[0094] In the second primary watermarking technique, the watermark is embedded (imprinted) into the physical channel. To illustrate, synchronization bits or unused bits in a physical channel can be varied to effectively carry the watermark in that physical channel. This technique can be modeled as follows. The existing physical channel(s) can be viewed as a cover signal s. The watermark is w, an embedding function is E and a secret key is k. The secret key k can be viewed as the specific physical channel embedding technique, which is described subsequently. The watermarked signal s_w may be expressed according to Equation 3 as follows:

$$s_w = E_k\{s,w\} \qquad \text{Equation (3)}$$

[0095] The watermarked signal s_w is preferably robust with respect to common signal processing operations, such as filtering, compression or other typical wireless network functionalities. It is also desirable that the watermarked signal s_w be imperceptible. The use of the watermark does not impact the operation of the wireless system in a perceptible manner. To illustrate, components of the wireless system not aware of the watermark can process the wireless communication without a hardware or software modification. Additionally, if the watermarking technique is publicly known, it is desirable that a form of secure key is used to secure the exchange.

[0096] This second primary technique is illustrated in Figure 4. Figure 4 is a block diagram of a system, including a transmitter 400 and a receiver 410, which performs RF watermark/signature creation and extraction in physical channels, and authenticates received communications to determine if they were originated by a trusted source. Figure 4 shows a higher layer controller 402 manipulating physical channel 404 with a synchronized parameter configuration 412 so as to

perform RF watermark/signature creation 406 in physical channel 404 whereby watermark/signature information (i.e., digital information) is steganographically embedded. This synchronized parameter configuration 412 is known in the receiver 410 and applied to physical channel 404 upon receiving watermark signature information from the transmitter 400 via a transmission path 414 and performing watermark/signature extraction 408 whereby the steganographically embedded watermark/signature information 416 is extracted and compared with local (i.e., expected) RF watermark/signature information 418 of the receiver 410 by a comparator 420. An acceptable comparison authenticates the transmitter 400 as being a trusted data source by performing a pass/fail authentication test.

[0097] Below is a description of various types of CDMA watermarking techniques. SS systems refer to any radio air interface systems using SS techniques, including UMTS FDD/TDD and CDMA2000. Different candidate watermarking solutions for SS systems described below may be implemented in various system layers.

[098] **CRC or Parity Bit Failure**

[099] Figure 5 illustrates that watermarks may be incorporated into a CRC and tail bits of a CDMA reverse fundamental channel in accordance with the present invention. An alternate embodiment proposes to intentionally corrupt, at some predetermined interval, the cyclic redundancy check (CRC) or a parity bit. CRCs and parity checks are used to protect packetized data transmissions from bit errors due to noise, interference, collisions, and multi-path in a given RF channel. By corrupting these checks periodically or a predetermined time, a receiver will receive transmission errors at some corresponding rate. If the error rate is as expected, a receiver can authenticate the source of the transmission. The absence of errors or receiving errors at some unexpected rate alerts a receiver that perhaps the transmitter is not a desired data source.

[0100] Figure 6 illustrates the frame structure of the CDMA reverse fundamental channel of Figure 5. The frame structure includes a reserved/erasure (R/E) indicator bit, information bits, a frame quality indicator (F), such as a CRC, and encoder tail bits T. The frame quality indicator (F) is

calculated on all bits within the frame, except the frame quality indicator itself and the encoder tail bits (T). The last eight bits of the encoder tail bits (T) are each typically set to zero.

[0101] Figure 7 illustrates a CDMA reverse fundamental channel and reverse supplemental channel structure in which watermarks may be incorporated into reserved bits, CRC and tail bits of the structure. The value of n is the length of the frame in multiples of 20 ms. For 37 to 72 encoder input bits per frame, n = 1 or 2. For more than 72 encoder input bits per frame, n = 1, 2 or 4.

[0102] **FSK modulation based watermarking with scrambling code jitter**

[0103] In SS systems, scrambling codes are used to separate terminals or base stations from each other. In one embodiment of the present invention, Figure 8 shows a spreader 800 for spreading CDMA data channels. The scrambling code, S_c, is applied and aligned with the radio frames, such that the first scrambling chip corresponds to the beginning of a radio frame. For watermarking, we apply slow scrambling code jitter with respect to the carrier frequency and FSK modulation of watermark information on top of this jitter by placing a low frequency drift on the carrier frequency, (i.e., by gradually incrementing the frequency, either in an upwards or downwards direction, in small frequency steps). Thus, the watermark information is hidden.

[0104] In the spreader 800 of Figure 8, an i-th data stream D_i is spread to chip rate by an associated channelization code C_i through a multiplier 805. The spread signal is then weighted by a gain factor, p_i, through a multiplier 810. In addition, a k-th data stream D_k is spread to chip rate by an associated channelization code C_k through a multiplier 815. The spread signal is then weighted by a gain factor, p_k, through a multiplier 820. The weighted spread signals are summed via an adder 825 to provide a summed chip sequence signal C_s, which is then scrambled by the scrambling code S_c through a multiplier 830, to provide a complex-valued chip sequence S. It should be noted that the physical layer parameters including the channelization code, gain factor, and scrambling

code, are used and/or modified to carry/represent watermark information in the present invention, as mentioned later.

[0105] Figure 9 shows a modulator 900 for modulating the complex-valued chip sequence S generated by the spreader 800 of Figure 8. A spreading sequence and a carrier frequency are modulated. The complex-valued chip sequence S is split into real and imaginary parts by a splitter 905. The real and imaginary parts, Re{S} and Im{S}, respectively, are then processed by the pulse shaping filters, 910 and 915, respectively, to meet the required spectrum regulation. The pulse-shaped chip sequences output by the filters 910 and 915 are modulated by the carrier frequency f_c via multipliers 920 and 925, respectively using cosine and sine signals, respectively, having a carrier frequency of f_c as a function of time t (i.e., radius/sec). Finally, the carrier modulated signals are summed by a summer 930, before being transmitted by an antenna or antenna array 935. As will be discussed below in more detail, the carrier frequency f_c is used to carry watermark information by adding or subtracting a frequency offset based on the watermark information.

[0106] Figure 10 illustrates an FSK modulation-based watermarking system 1000 using with scrambling code jitter. The watermark information W is mapped to a predefined frequency offset Δ. When jitter of the scrambling code S_c occurs, thus forming scrambling code jitter S_c', a local descrambler in the receiver has to be synchronized to generate the same descrambling code jitter. The watermark information W may be represented in the amount of the scrambling code jittering S_c' and frequency offset Δ, separately. In a simplified example, a single watermark bit is embedded in the carrier frequency f_c and/or scrambling code S_c. In this case, a watermark bit, "Zero", may lead the scrambling code, S_c, to jittering late by a predefined amount in chips to generate the jitter scrambling code S_c', while a watermark bit, "One", may lead the scrambling code to jitter early by the same amount. Similarly, the "Zero" watermark bit is represented as a negative predefined frequency offset, $-\Delta$, while the "Zero" watermark bit is represented a positive predefined frequency offset, $+\Delta$. The original carrier

frequency f_c is then biased by the frequency offset, $f_c \pm \Delta$, depending on the binary watermarking bit.

[0107] **Stealing scrambling code and/or channelization code chips for watermarking**

[0108] In this case, we select certain chips in the scrambling code (and/or channelization code) of Figure 8 and embed watermark information on these chips such that no change occurs if a stolen code chip is "0", and a flip occurs if a stolen code chip is "1" (i.e., change the stolen code chip from "1" to "0"). In this case, the selected chip locations are known at both transmitter and receiver. The locations may be changed slowly. With heavy channel coding this will make the information readable at the receiver. From the point of view of the uninformed, however, this will cause some signal-to-noise ratio (SNR) degradation, but the effect should be small, particularly if the SF is large. Alternatively, the watermark chip may be always set to "1" or "0" to indicate that the transmitter that sets it can be trusted.

[0109] **Utilizing (physical channel) configuration of channelization code and SF for watermarking**

[0110] In typical CDMA systems, the channelization codes of Figure 8 are OVSF codes that preserve the orthogonality between a user's different physical channels. The OVSF codes can be defined using the code tree of Figure 11. For a given data sequence to be sent, there are several possible configurations of channelization code and SF. For example, using 2 channelization codes with SF=32 is equivalent to using 1 channelization code with SF=64 in terms of the number of physical channel bits. In this case, the configuration of using 2 channelization codes with SF=32 may be used to represent one bit of the watermark information, while the configuration of using 1 channelization code with SF=16 may represent a zero bit. As a result, the watermark information can be mapped, in a subscriber unit, to the physical channel combinations according to a predefined rule established by a base station.

[0111] Figure 12 depicts a watermarking scheme utilizing channelization code and SF. It is simply assumed that all the OVSF channelization codes in the

OVSF tree of Figure 11 are available to transmit a user data stream. In addition, it is assumed that for transmitting a given user data, we have two channelization code configuration options: referring to Figure 11, the first is to use $\{C_{ch,2,o}, C_{ch,2,1}\}$ each having SF=2 and the other $\{C_{ch,4,o}, C_{ch,4,1}, C_{ch,4,2}, C_{ch,4,3}\}$ each having SF=4. It is also assumed to signal a single watermark bit. In this case, we define the mapping rule as follows: the "Zero" watermark bit is associated with the first option, $\{C_{ch,2,o}, C_{ch,2,1}\}$ each having SF=2, while the "One" watermark bit is associated with the second $\{C_{ch,4,o}, C_{ch,4,1}, C_{ch,4,2}, C_{ch,4,3}\}$ each having SF=4. As a consequence, for a given input single bit watermark information W, the mapping function 1200 selects which channelization code configuration option is used for transmitting the user data. The selected channelization codes are provided for the spreader of Figure 8. At the receiver, it is estimated/determined which channelization code configuration is used for the data transmission. The watermark information is extracted according to the estimation, assuming that the receiver knows the mapping rule a priori.

[0112] **Utilizing power (gain) ratios (or differences) between channelization codes for watermarking**

[0113] Figure 13 illustrates an example of the two spread and weighed data signals with the channelization codes C_i and C_k and gain factors, p_i and p_k. When multiple channelization codes are used for a given communication link, assuming to allow their transmit power to be separately adjustable subject to a given total power, watermark information may be represented as a relative gain (or power) offset between any pair of the multi-channelization codes, i.e., $\{C_i, C_k\}$ having respective gains (or power) p_i , p_k. The power in channelization codes an be alternated from frame-to-frame to create a signature. Furthermore, when two channelization codes are simultaneously used by the same subscriber unit, watermark information can be encoded on the alternating pattern of which code is higher/lower during this frame.

[0114] Figure 14 is a flow diagram of a process 1400 including method steps for utilizing a gain offset between a pair of channelization codes for watermarking. Here, the gain of a channelization code means the gain of the

CDMA data carried in the channelization code. In addition, we assume that the gain is calculated from a transmit power control algorithm. The watermarking based gain offset, B, is then applied on top of the calculated gain, if necessary. Multiple relative gain offsets may be used among different pairs of multiple channelization codes.

[0115] In step 1405, watermark information sequence w is input to a conversion block converting/mapping "w" to "B". In step 1410, a pair of channelization codes $\{C_i, C_k\}$ is determined. In step 1415, w is converted to a relative gain (or power) offset, B, between the pair of channelization codes, where $B \geq 0$, according to a predefined conversion/mapping table which is know at both the transmitter and receiver. In step 1420, based on the relative gain offset, B, adjust the gain amounts of the channelization codes, respectively, such that $p_i^{'} = p_i + B/2$; and $p_k^{'} = p_k - B/2$. In step 1425, the gains $p_i^{'}$ and $p_k^{'}$ are input to a gain multiplier (i.e., the multipliers 810 and 820 in the spreader 800 of Figure 8).

[0116] **Delay modulation based watermarking**

[0117] The principle of this idea is similar to the above (utilizing gain offsets of channelization codes for watermarking). But, for this case watermark information is mapped as a delay of a channelization code transmission where the delay is a time relative to reference channel transmission timing or a physical channel frame boundary. In the case of multi-code transmissions, the individual delays of each channelization code may be jointly used for watermark transmission. Higher layers may get involved in determining the individual delay(s). When delay-transmit diversity is employed, the relative delays among antennas may be used to represent watermark information.

[0118] **Stealing pilot/control/data symbols for watermarking**

[0119] Watermarks are embedded into pilot channel or control channel or data channel or combination channels in a predefined manner (predefined symbol positions) such that we pick certain pilot symbols in the pilot channel and embed watermark information on these (i.e., keep as is if 0, flip if 1).

[0120] **STBC transmit diversity**

[0121] Referring to Figures 1 and 15A, assuming that the TX TRU transmitter 20 shown in Figure 1 has four complex-valued data symbols, $\{\vec{d}_1, \vec{d}_2, \vec{d}_3, \vec{d}_4\}$, from a higher layer, one known STBC transmit diversity technique constructs the space-time codewords by simultaneously transmitting two different data symbols $\vec{d}_2$ and $\vec{d}_1^*$ from antenna 1 and diversity antenna 2, respectively, as shown in Figure 15A, during the first symbol period, where "*" denotes the conjugate operator of a complex scalar or vector. Then, symbols $\vec{d}_1$ and $-\vec{d}_2^*$ are sent from antennas 1 and 2, respectively, in the second symbol period. Similarly, in the third symbol period, $\vec{d}_4$ and $\vec{d}_3^*$ are transmitted from antennas 1 and 2, respectively, while symbols $\vec{d}_3$ and $-\vec{d}_4^*$ are sent from antennas 1 and 2, respectively, in the fourth symbol period. In this case, two watermark bits may be embedded into the symbols, every other symbol period. For example, if the first watermark bit is equal to "0", then flip the symbols in the second symbol period, such as from ($\vec{d}_1$ and $-\vec{d}_2^*$) to ($-\vec{d}_1$ and $\vec{d}_2^*$). Otherwise, if the first watermark bit is equal to "1", the symbols are kept as they are. Similarly, if the second watermark bit is equal to "0", then flip the symbols in the fourth symbol period such as from ($\vec{d}_3$ and $-\vec{d}_4^*$) to ($-\vec{d}_3$ and $\vec{d}_4^*$). Otherwise, the two symbols in the fourth symbol period remain the same.

[0122] **SFBC transmit diversity**

[0123] A similar watermarking process can be implemented in an SFBC encoder structure, as shown in Figure 15B. This transmit diversity techniques constructs a space-frequency codeword by simultaneously transmitting two different data symbols $\vec{d}_2$ and $\vec{d}_1^*$ from frequency sub-group 1 and diversity frequency sub-group 2, respectively, as shown in Figure 15B, during a first symbol period, where "*" denotes the conjugate operator of a complex scalar or vector. Then symbols $\vec{d}_1$ and $-\vec{d}_2^*$ are sent from frequency sub-groups 1 and 2, respectively, in the second symbol period. Similarly, in the third symbol period,

$\vec{d}_4$ and $\vec{d}_3^{\,*}$ are transmitted from frequency sub-groups 1 and 2, respectively, while symbols $\vec{d}_3$ and $-\vec{d}_4^{\,*}$ are sent from frequency sub-group 1 and diversity frequency sub-group 2, respectively, in the fourth symbol period. In the present embodiment, two watermark bits may be embedded into the symbols, every other symbol period, as follows: if the first watermark bit is equal to "zero", symbols in the second symbol period are flipped such as from ($\vec{d}_1$ and $-\vec{d}_2^{\,*}$) to ($-\vec{d}_1$ and $\vec{d}_2^{\,*}$). Otherwise, if the first watermark bit is "one", the symbols are kept as they are. Similarly, if the second watermark bit is equal to "zero", then symbols in the fourth symbol period are flipped such as from ($\vec{d}_3$ and $-\vec{d}_4^{\,*}$) to ($-\vec{d}_3$ and $\vec{d}_4^{\,*}$). Otherwise, the two symbols in the fourth symbol period remain same as they are.

[0124] **Introducing/defining a new physical channel or watermark field for watermarking**

[0125] Watermark information can be directly transported by defining a new physical channel or watermark field (similar to a control signaling (TFCI or TPC) field).

[0126] **DPC based watermarking**

[0127] Dirty paper coding (DPC) is a coding technique using side information which will be transmitted along with the encoded information, as described by Cox et al. in the IEEE article "Watermarking as Communications with Side Information." Imagine a sheet of paper covered with a Gaussian distributed pattern of "dirt". This dirt is a noise or interference source (side information above), which the transmitter can examine. The transmitter writes a message on this paper and sends it to a receiver. Costa describes, in an IEEE article entitled "Writing on Dirty Paper", theoretically showed that the noise/interference source (that is, dirty paper) has no effect on the information capacity. In accordance with the present invention, watermark information is regarded as the DPC encoded information, and any other CDMA signals (dedicated channel or control channel) are regarded as the noise/interference source (side information).

[0128] Figures 16A and 16B show two examples of DPC based watermarking systems. In Figure 16A, watermark information, w, is encoded (or pre-coded) through a DPC encoder 1600. An encoded watermark sequence 1605 is then added (or modularly summed) by an adder 1615 with the CDMA data stream 1610. The resulting signal 1620 goes to the spreader 800 (as shown in Figure 8). In Figure 16B, a watermark embedding device 30 (also shown in the system 100 of Figure 1) is used instead of the simple adder (or modular summer) 1615 as shown in Figure 16A. The watermark embedding device 30 is used to tailor the encoded watermark signal according to the CDMA data stream 1610 in an attempt to attain an optimal trade-off between estimates of perceptual fidelity and robustness where the perceptual fidelity and robustness are typical requirements for watermarking. DPC processing may be performed on a chip level at the spreader 800.

[0129] **Watermark embedded CRC**

[0130] Error detection is provided on transport blocks through a CRC. The 3GPP TS 25.212 entitled "Multiplexing and channel coding (FDD)" discloses that the size of the CRC is 24, 16, 12, 8 or 0 bits and it is signaled from higher layers what CRC size that should be used for each transport channel. The entire transport block is used to calculate the CRC parity bits for each transport block. The parity bits are generated by one of the following cyclic generator polynomials:

[0131] - $g_{CRC24}(D) = D^{24} + D^{23} + D^6 + D^5 + D + 1$;

[0132] - $g_{CRC16}(D) = D^{16} + D^{12} + D^5 + 1$;

[0133] - $g_{CRC12}(D) = D^{12} + D^{11} + D^3 + D^2 + D + 1$; and

[0134] - $g_{CRC8}(D) = D^8 + D^7 + D^4 + D^3 + D + 1$.

[0135] Figure 17 illustrates transport channel multiplexing structure for 3GPP uplink, showing where the CRC attachment is applied. Watermark information can be embedded in cyclic redundancy code in various ways. As shown in Figure 18, a modulo-2 adder may be used to combine CRC bits with watermark bits where the CRC bits are generated based on (dedicated or control) data. If the length of watermark bits is not the same as the CRC length, then

zero-bit padding or pruning may be used for the modulo-2 add operation. Alternatively, the shift register of the CRC generator may be initialized by one or more watermark bits prior to CRC generation for data.

[0136] **Watermark based FEC initialization**

[0137] In Figures 19A and 19B, rate 1/2 and rate 1/3 convolutional encoders used in 3GPP are shown. Typically, the initial values of the shift register of the coder shall be "all 0s" when starting to encode the input bits. Watermark information is used to initialize the shift register of the FEC encoder prior to channel coding for data.

[0138] **FEC redundant bits replacement for watermarking**

[0139] Some of the redundant bits of FEC output are replaced with watermark bits using puncturing, where watermark information w is inserted into the punctured locations known by the sender and receiver to provide a watermark embedded CRC output, as shown in Figure 20.

[0140] **FEC tail bit modification**

[0141] In convolutional type FEC, tail bits are appended after the encoded data sequence, in order to return the convolution encoder to a "zero state". For the convolutional encoder structures shown in Figures 19A and 19B, 8 tail bits with binary value 0 shall be added to the end of the coded block before encoding. The tail bits are encoded with watermarking information, rather than being set to all zeros.

[0142] Tail bits are inserted into a header in order to facilitate a reliable and timely detection of the data packet's Rate and Length fields. The header tail bits or the convolutional tail bits (or both) may be modified so as to encode them with watermark information. As an example, specific, predetermined tail bits can be flipped from zeros to ones in a predetermined pattern to form an embedded physical channel wherein the tail bit pattern represents a bit or bits of data.

[0143] Alternatively, either set of tail bits can be manipulated so as to generate an authorization signature. As long as both the transmitter and receiver know what known state the decoder wants to achieve, these tail bits can be manipulated without affecting the decoding function. As an example, a set of

tail bits can be flipped from all zeros to all ones.

[0144] **Watermark embedded FEC output**

[0145] Watermark information w is input to mask FEC outputs where the masking may be performed by a modulo-2 adder to provide a watermark embedded FEC output, as shown in Figure 21. If the length of watermark bits is not the same as the CRC length, then zero-bit padding or pruning or spreading (like rate matching) may be used for the modulo-2 add operation. Particularly, this watermark specific masking would work well with both convolutional coding and Turbo coding, taking into account their starting state and ending state known (zero state).

[0146] **Transport format configuration (TFC) based watermarking**

[0147] In this case, TFCI (channelization code, SF, timeslot/frame, rate matching, etc) is determined based on watermark information. Figure 22 shows a flow diagram of a process 2200 including method steps for configuring the transport format of a TrCH based on watermarking information and at least one mapping rule. When a transport channel is input (step 2205), a set of possible transport formats for the input TrCH is determined (step 2210). Watermark information and at least one mapping rule are input (step 2215). The input watermark information and the at least one mapping rule are used as a basis to select a transport format from the transport format set (step 2220). The selected transport format is used to transmit the TrCH (step 2225).

[0148] **Compressed mode**

[0149] Because wideband CDMA (WCDMA) uses continuous transmission and reception, a mobile TRU cannot make intersystem measurements with single receiver if there are no gaps generated between the WCDMA signals. Therefore, as shown in Figure 23, a compressed mode is used for performing both for inter-frequency and inter-system measurements. In compressed mode, one or more transmission gap pattern sequences are active. Therefore, some frames are compressed and contain transmission gaps such that watermark information may be transmitted therein.

[0150] **Discontinuous transmission (DTX) mode**

[0151] If no data is provided by higher layers for transmission during the second phase of the downlink dedicated channel, then DTX is applied. In this case, the transmitter determines whether the DTX status is "ON" (meaning no data from higher layers for transmission). Upon the "ON" DTX status (DTX mode of CDMA data), watermark information is sent during a DTX period using a predetermined transport format (including channelization code(s) and timeslot(s)).

[0152] Any combination among all the above-mentioned schemes may be considered for watermarking. For example, the scheme of stealing scrambling code chips for watermarking may be combined with the DPC based watermarking scheme.

[0153] Although the features and elements of the present invention are described in the preferred embodiments in particular combinations, each feature or element can be used alone without the other features and elements of the preferred embodiments or in various combinations with or without other features and elements of the present invention. Further, these elements may be implemented in a single IC, such as an application specific integrated circuit (ASIC), or in multiple ICs, discrete components, or a combination of discrete components and one or more ICs. Moreover, the present invention may be implemented in any type of wireless communication system.

[0154] While the present invention has been described in terms of the preferred embodiment, other variations which are within the scope of the invention as outlined in the claims below will be apparent to those skilled in the art.

* * *

CLAIMS

What is claimed is:

1. In a wireless code division multiple access (CDMA) communication system including a transmitter and a receiver, a method of protecting and authenticating wirelessly transmitted digital information, the method comprising:

(a) the transmitter steganographically embedding digital information in a CDMA communication signal;

(b) the transmitter wirelessly transmitting the CDMA communication signal;

(c) the receiver receiving the CDMA communication signal; and

(d) the receiver extracting the digital information from the received CDMA communication signal.

2. The method of claim 1 wherein step (a) further comprises:

(a1) the transmitter embedding the digital information in the CDMA communication signal as a watermark in a transmitting (TX) layer 2/3.

3. The method of claim 1 wherein step (a) further comprises:

(a1) the transmitter embedding the digital information in the CDMA communication signal as a watermark in a transmitting (TX) physical layer.

4. The method of claim 1 wherein step (a) further comprises:

(a1) the transmitter embedding the digital information in the CDMA communication signal as a watermark in a transmitting (TX) radio frequency (RF) layer.

5. The method of claim 1 wherein step (d) further comprises:

(d1) the receiver extracting the digital information from the CDMA communication signal using a receiving (RX) layer 2/3 processing device.

6. The method of claim 1 wherein step (d) further comprises:

(d1) the receiver extracting the digital information from the CDMA communication signal using a receiving (RX) physical layer processing device.

7. The method of claim 1 wherein step (d) further comprises:

(d1) the receiver extracting the digital information from the CDMA communication signal using a receiving (RX) radio frequency (RF) processing device.

8. The method of claim 1 wherein step (a) further comprises:

(a1) the transmitter embedding the digital information in a frame quality indicator.

9. The method of claim 8 wherein the frame quality indicator includes a cyclic redundancy check (CRC).

10. The method of claim 1 wherein step (a) further comprises:

(a1) the transmitter embedding the digital information in at least one encoder tail bit.

11. The method of claim 1 wherein step (a) further comprises:

(a1) the transmitter embedding the digital information in at least one reserved/erasure indicator.

12. The method of claim 1 wherein step (a) further comprises:

(a1) applying slow scrambled code jitter with respect to a carrier frequency and frequency-shift keying (FSK) modulation of the digital information placed on top of the jitter.

13. The method of claim 12 wherein step (a) further comprises:

(a2) mapping the digital information to a predefined frequency offset.

14. The method of claim 12 wherein step (d) further comprises:

(d1) synchronizing a local descrambler in the receiver to generate the same code jitter.

15. The method of claim 1 wherein step (a) further comprises:

(a1) selecting particular chips in at least one of a scrambling code and a channelization code; and

(a2) embedding the digital information in the selected chips.

16. The method of claim 15 wherein step (d) further comprises:

(d1) determining the particular chips; and

(d2) extracting the digital information from the chips determined in step (d1).

17. The method of claim 1 wherein step (a) further comprises:

(a1) mapping the digital information to physical channel combinations based on at least one channelization code and a spreading factor (SF) according to a predefined rule.

18. The method of claim 17 wherein the channelization code is an orthogonal variable spreading factor (OVSF) code.

19. The method of claim 1 wherein step (a) further comprises:

(a1) representing the digital information as a relative gain or power offset between any pair of channelization codes.

20. The method of claim 1 wherein step (a) further comprises:

(a1) mapping the digital information as a delay of a channelization code transmission.

21. The method of claim 1 wherein the digital information comprises at least one token.

22. The method of claim 1 wherein the digital information comprises at least one key.

23. The method of claim 1 wherein the digital information comprises at least one watermark.

24. The method of claim 1 wherein the digital information comprises at least one signature.

25. The method of claim 1 wherein step (a) further comprises:

(a1) the transmitter embedding the digital information in a pilot channel.

26. The method of claim 25 wherein step (a) further comprises:

(a2) the transmitter embedding the digital information in certain pilot symbols in the pilot channel.

27. The method of claim 26 wherein step (d) further comprises:

(d1) the receiver extracting the digital information from the certain pilot symbols in the pilot channel.

28. The method of claim 1 wherein step (a) further comprises:

(a1) the transmitter embedding the digital information in a control channel.

29. The method of claim 1 wherein step (a) further comprises:

(a1) the transmitter embedding the digital information in a data channel.

30. The method of claim 1 wherein the transmitter comprises two antennas, and step (a) further comprises:

(a1) the transmitter embedding the digital information in two different data symbols every other symbol period, wherein the two different data symbols are simultaneously transmitted by the respective ones of the two antennas.

31. The method of claim 1 wherein step (a) further comprises:

(a1) the digital information is directly transported by defining a new physical channel or field.

32. The method of claim 1 wherein step (a) further comprises:

(a1) treating the digital information as dirty paper coding (DPC) encoded information; and

(a2) treating any other CDMA signals as side information.

33. The method of claim 1 wherein step (a) further comprises:

(a1) combining bits of the digital information with bits of a cyclic redundancy check (CRC).

34. The method of claim 1 wherein step (a) further comprises:

(a1) using the digital information to initialize a shift register of a cyclic redundancy check (CRC) generator prior to CRC generation for data.

35. The method of claim 1 wherein step (a) further comprises:

(a1) using the digital information to initialize a shift register of a forward error correction (FEC) encoder prior to channel coding for data.

36. The method of claim 1 wherein step (a) further comprises:

(a1) puncturing bits of a forward error correction (FEC) output;

(a2) inserting bits of the digital information in locations of the FEC output punctured bits; and

(a3) providing a cyclic redundancy check (CRC) output embedded with the digital information bits.

37. The method of claim 36 wherein step (d) further comprises:

(d1) the receiver extracting the digital information from the punctured bit locations of the FEC output.

38. The method of claim 1 wherein tail bits of a forward error correction (FEC) output are encoded with the digital information rather than being set to a binary value of zero.

39. The method of claim 1 wherein step (a) further comprises:

(a1) using the digital information to mask a forward error correction (FEC) output.

40. The method of claim 1 wherein step (a) further comprises:

(a1) determining a set of transport formats for a transport channel (TrCH);

(a2) selecting a transport format from the transport format set based on the digital information and at least one mapping rule; and

(a3) using the selected transport format to transmit the TrCH.

41. The method of claim 1 wherein step (a) further comprises:

(a1) the transmitter sending the digital information during at least one transmission gap of the CDMA communication signal when it is in a compressed mode.

42. The method of claim 1 wherein step (a) further comprises:

(a1) the transmitter sending the digital information during a period of an activated discontinuous transmission mode using a predetermined transport format.

43. A wireless code division multiple access (CDMA) communication system for protecting and authenticating wirelessly transmitted digital information, the system comprising:

(a) a transmitter which steganographically embeds digital information in a CDMA communication signal and wirelessly transmits the CDMA communication signal; and

(b) a receiver which receives the CDMA communication signal and extracts the steganographically embedded digital information from the received CDMA communication signal.

44. The system of claim 43 wherein the transmitter embeds the digital information in a frame quality indicator.

45. The system of claim 44 wherein the frame quality indicator includes a cyclic redundancy check (CRC).

46. The system of claim 43 wherein the transmitter embeds the digital information in at least one encoder tail bit.

47. The system of claim 43 wherein the transmitter embeds the digital information in at least one reserved/erasure indicator.

48. The system of claim 43 wherein the transmitter applies slow scrambled code jitter with respect to a carrier frequency and frequency-shift keying (FSK) modulation of the digital information placed on top of the jitter.

49. The system of claim 48 wherein the transmitter maps the digital information to a predefined frequency offset.

50. The system of claim 48 wherein the receiver synchronizes a local descrambler to generate the same code jitter.

51. The system of claim 43 wherein the transmitter selects particular chips in at least one of a scrambling code and a channelization code, and embeds the digital information in the selected chips.

52. The system of claim 51 wherein the receiver determines the particular chips and extracts the digital information from the particular chips.

53. The system of claim 43 wherein the transmitter maps the digital information to physical channel combinations based on at least one channelization code and a spreading factor (SF) according to a predefined rule.

54. The system of claim 53 wherein the channelization code is an orthogonal variable spreading factor (OVSF) code.

55. The system of claim 43 wherein the transmitter represents the digital information as a relative gain or power offset between any pair of channelization codes.

56. The system of claim 43 wherein the transmitter maps the digital information as a delay of a channelization code transmission.

57. The system of claim 43 wherein the digital information comprises at least one token.

58. The system of claim 43 wherein the digital information comprises at least one key.

59. The system of claim 43 wherein the digital information comprises at least one watermark.

60. The system of claim 43 wherein the digital information comprises at least one signature.

61. The system of claim 43 wherein the transmitter embeds the digital information in a pilot channel.

62. The system of claim 61 wherein the transmitter embeds the digital information in certain pilot symbols in the pilot channel.

63. The system of claim 62 wherein the receiver extracts the digital information from the certain pilot symbols in the pilot channel.

64. The system of claim 43 wherein the transmitter embeds the digital information in a control channel.

65. The system of claim 43 wherein the transmitter embeds the digital information in a data channel.

66. The system of claim 43 wherein the transmitter comprises two antennas, whereby the transmitter embeds the digital information in two different data symbols every other symbol period, wherein the two different data symbols are simultaneously transmitted by the respective ones of the two antennas.

67. The system of claim 43 wherein the digital information is directly transported by defining a new physical channel or field.

68. The system of claim 43 wherein the digital information is treated as dirty paper coding (DPC) encoded information and any other CDMA signals are treated as side information.

69. The system of claim 43 wherein the transmitter combines bits of the digital information with bits of a cyclic redundancy check (CRC).

70. The system of claim 43 wherein the transmitter uses the digital information to initialize a shift register of a cyclic redundancy check (CRC) generator prior to CRC generation for data.

71. The system of claim 43 wherein the transmitter uses the digital information to initialize a shift register of a forward error correction (FEC) encoder prior to channel coding for data.

72. The system of claim 43 wherein the transmitter punctures bits of a forward error correction (FEC) output, inserts bits of the digital information in locations of the FEC output punctured bits and provides a cyclic redundancy check (CRC) output embedded with the digital information bits.

73. The system of claim 72 wherein the receiver extracts the digital information from the punctured bit locations of the FEC output.

74. The system of claim 43 wherein the transmitter encodes tail bits of a forward error correction (FEC) output with the digital information rather than setting the tail bits to a binary value of zero.

75. The system of claim 43 wherein the transmitter uses the digital information to mask a forward error correction (FEC) output.

76. The system of claim 43 wherein the transmitter determines a set of transport formats for a transport channel (TrCH), selects a transport format from the transport format set based on the digital information and at least one mapping rule, and uses the selected transport format to transmit the TrCH.

77. The system of claim 43 wherein the transmitter sends the digital information during at least one transmission gap of the CDMA communication signal when it is in a compressed mode.

78. The system of claim 43 wherein the transmitter sends the digital information during a period of an activated discontinuous transmission (DTX) mode using a predetermined transport format.

79. A wireless transmit/receive unit (WTRU) for protecting and authenticating wirelessly transmitted digital information, the WTRU comprising:

(a) a transmitter which steganographically embeds digital information in a code division multiple access (CDMA) communication signal and wirelessly transmits the CDMA communication signal; and

(b) a receiver which receives a CDMA communication signal and extracts steganographically embedded digital information from the received CDMA communication signal.

80. A base station for protecting and authenticating wirelessly transmitted digital information, the base station comprising:

(a) a transmitter which steganographically embeds digital information in a code division multiple access (CDMA) communication signal and wirelessly transmits the CDMA communication signal; and

(b) a receiver which receives a CDMA communication signal and extracts steganographically embedded digital information from the received CDMA communication signal.

81. An integrated circuit (IC) for protecting and authenticating wirelessly transmitted digital information, the IC comprising:

(a) a transmitter which steganographically embeds digital information in a code division multiple access (CDMA) communication signal and wirelessly transmits the CDMA communication signal; and

(b) a receiver which receives a CDMA communication signal and extracts steganographically embedded digital information from the received CDMA communication signal.

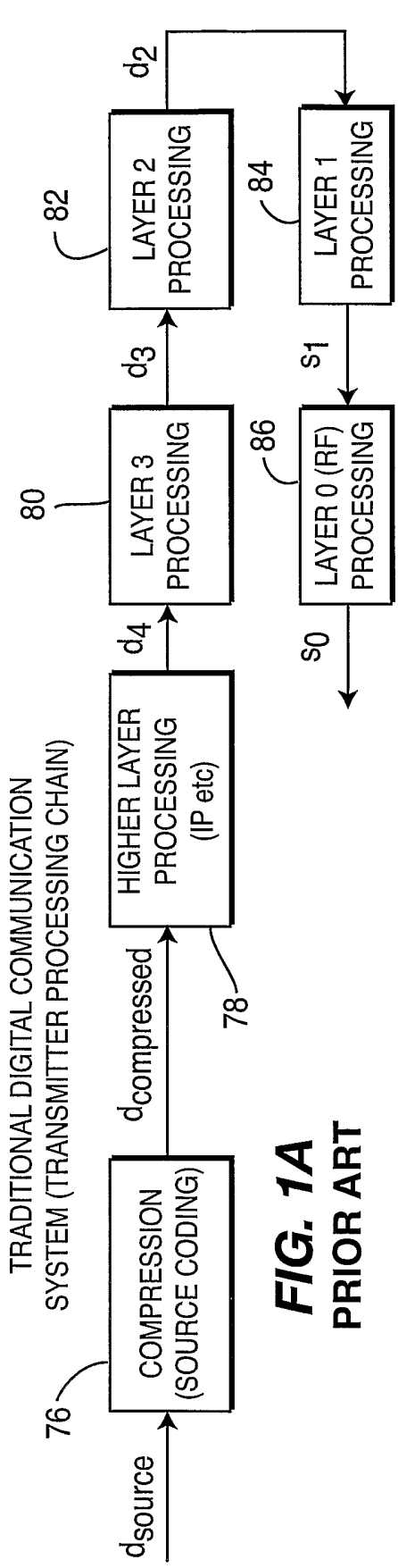


FIG. 1A
PRIOR ART

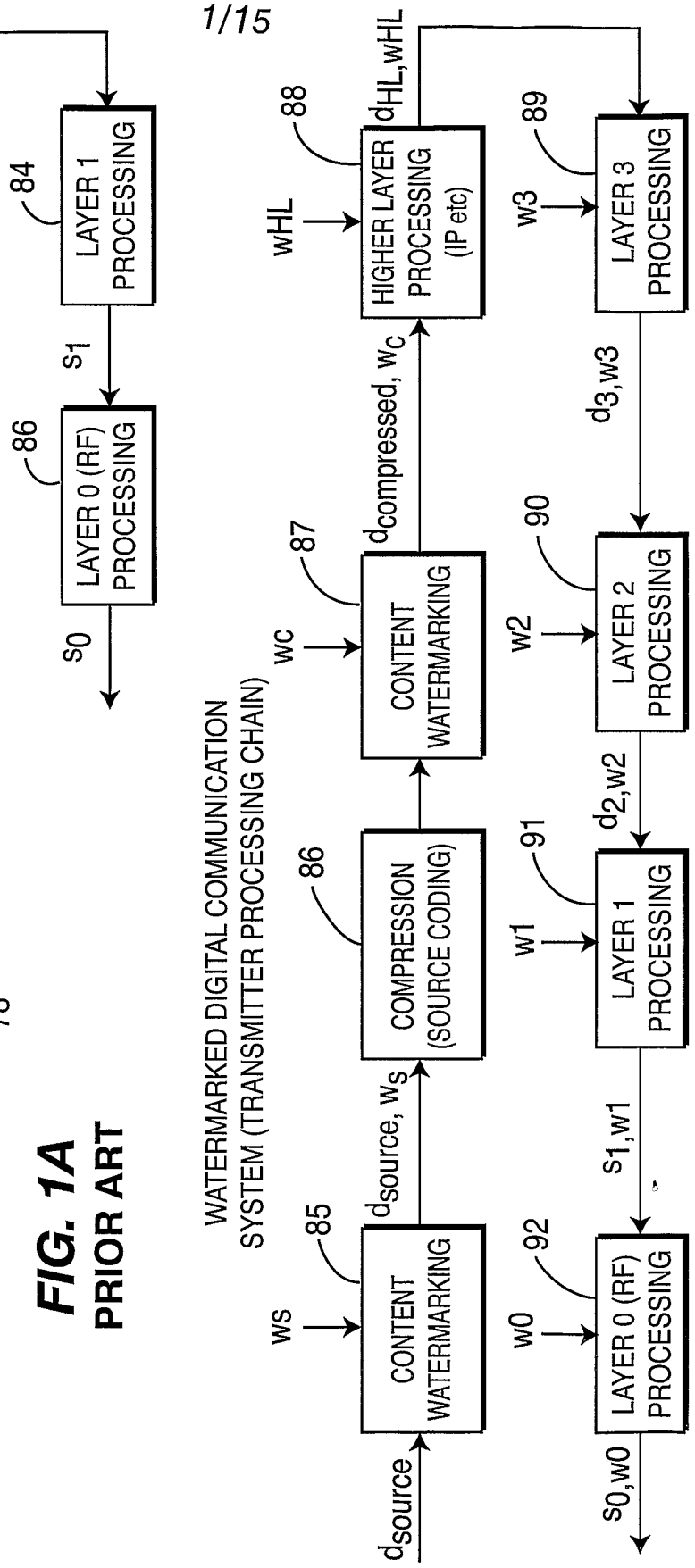


FIG. 1B

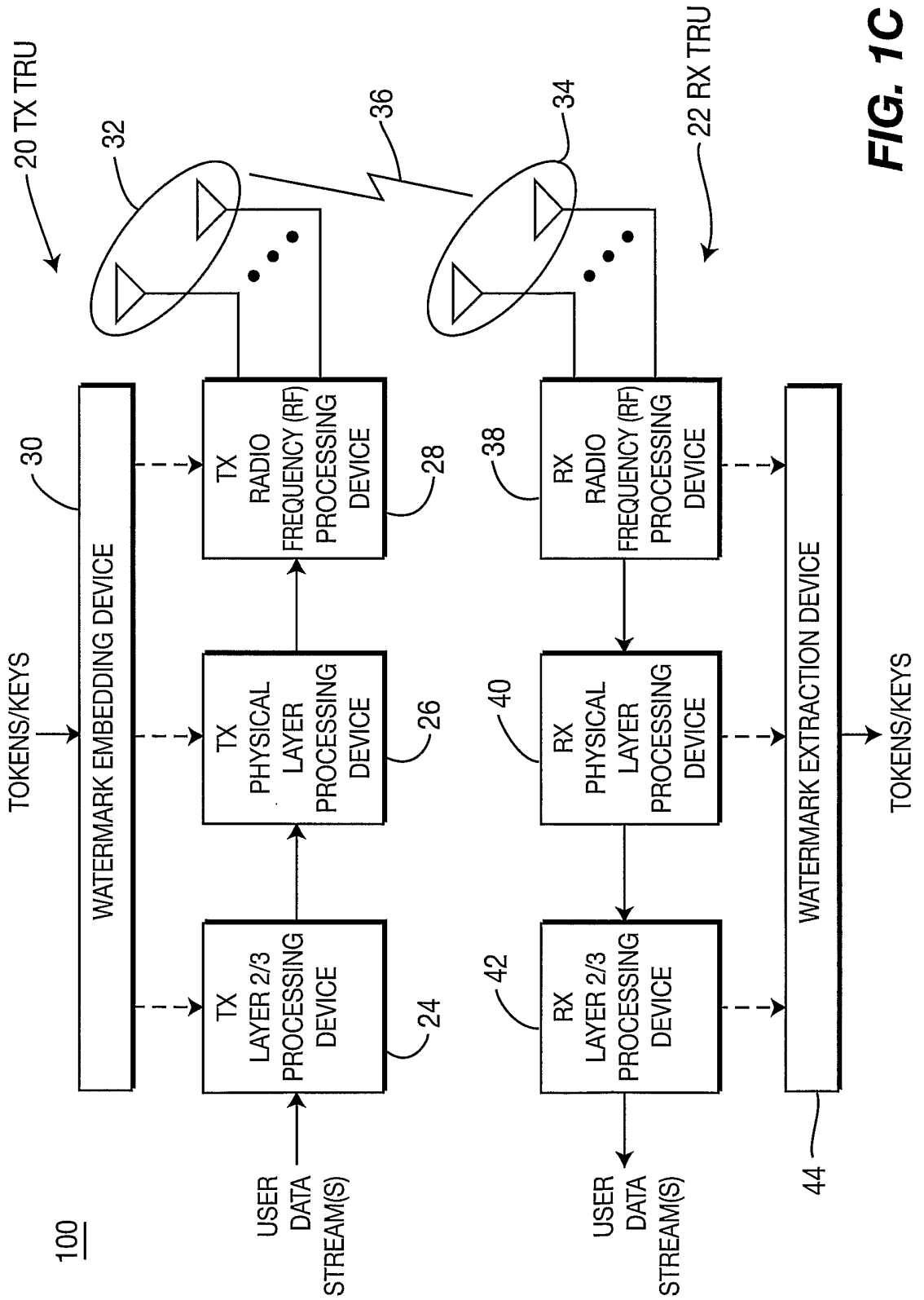

100
20 TX TRU
32
36
34
22 RX TRU
30
WATERMARK EMBEDDING DEVICE
TOKENS/KEYS
TX LAYER 2/3 PROCESSING DEVICE
24
TX PHYSICAL LAYER PROCESSING DEVICE
26
TX RADIO FREQUENCY (RF) PROCESSING DEVICE
28
USER DATA STREAM(S)
42
RX LAYER 2/3 PROCESSING DEVICE
40
RX PHYSICAL LAYER PROCESSING DEVICE
38
RX RADIO FREQUENCY (RF) PROCESSING DEVICE
WATERMARK EXTRACTION DEVICE
44
TOKENS/KEYS
USER DATA STREAM(S)

FIG. 1C

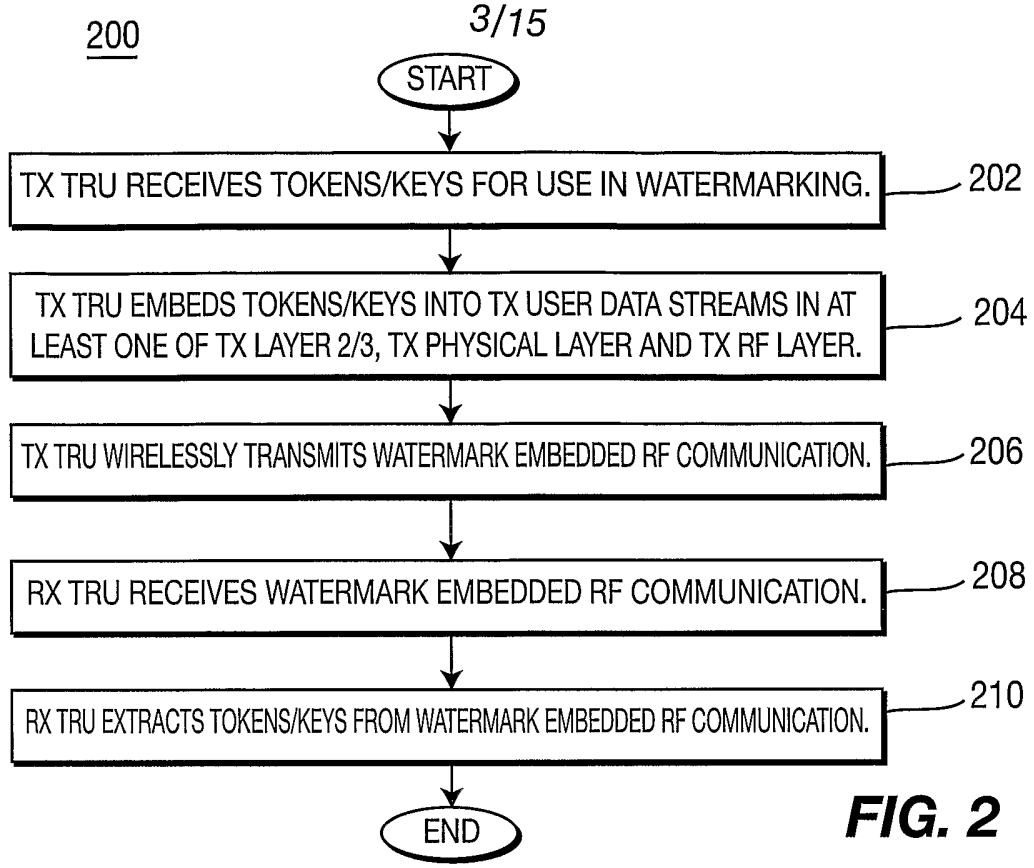

200
START
TX TRU RECEIVES TOKENS/KEYS FOR USE IN WATERMARKING.
202
TX TRU EMBEDS TOKENS/KEYS INTO TX USER DATA STREAMS IN AT LEAST ONE OF TX LAYER 2/3, TX PHYSICAL LAYER AND TX RF LAYER.
204
TX TRU WIRELESSLY TRANSMITS WATERMARK EMBEDDED RF COMMUNICATION.
206
RX TRU RECEIVES WATERMARK EMBEDDED RF COMMUNICATION.
208
RX TRU EXTRACTS TOKENS/KEYS FROM WATERMARK EMBEDDED RF COMMUNICATION.
210
END

FIG. 2

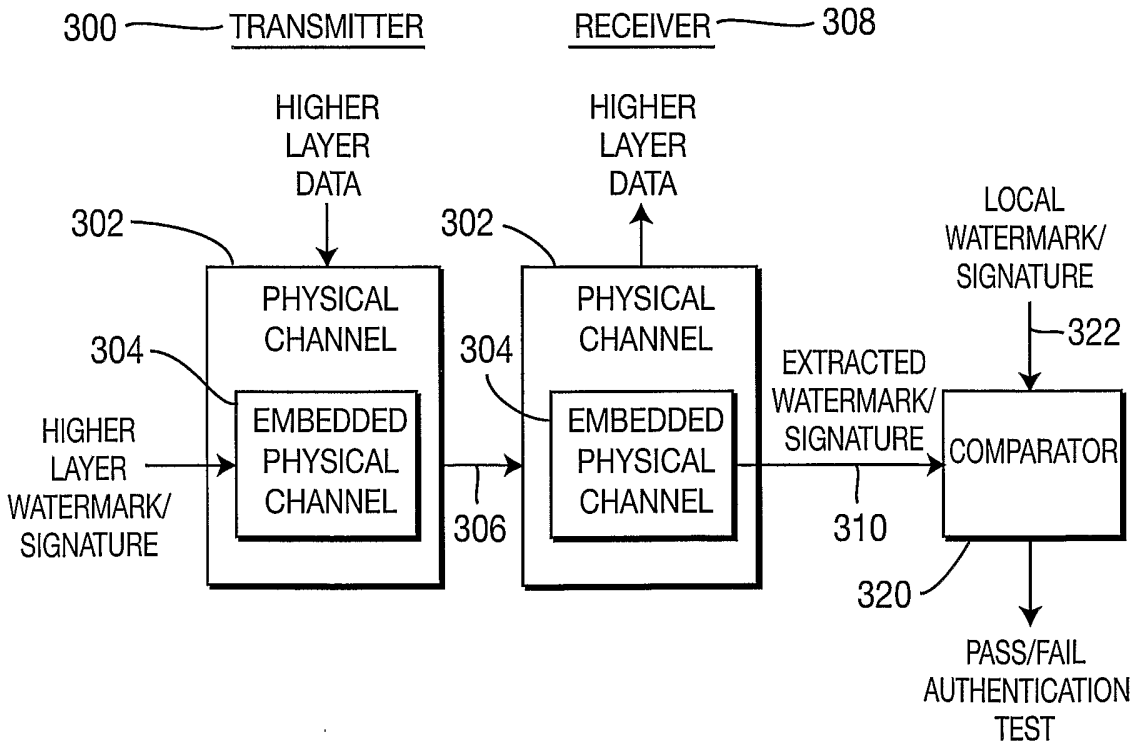

300
TRANSMITTER
RECEIVER
308
HIGHER LAYER DATA
HIGHER LAYER DATA
302
302
PHYSICAL CHANNEL
PHYSICAL CHANNEL
304
304
EMBEDDED PHYSICAL CHANNEL
EMBEDDED PHYSICAL CHANNEL
HIGHER LAYER WATERMARK/ SIGNATURE
306
EXTRACTED WATERMARK/ SIGNATURE
310
LOCAL WATERMARK/ SIGNATURE
322
COMPARATOR
320
PASS/FAIL AUTHENTICATION TEST

FIG. 3

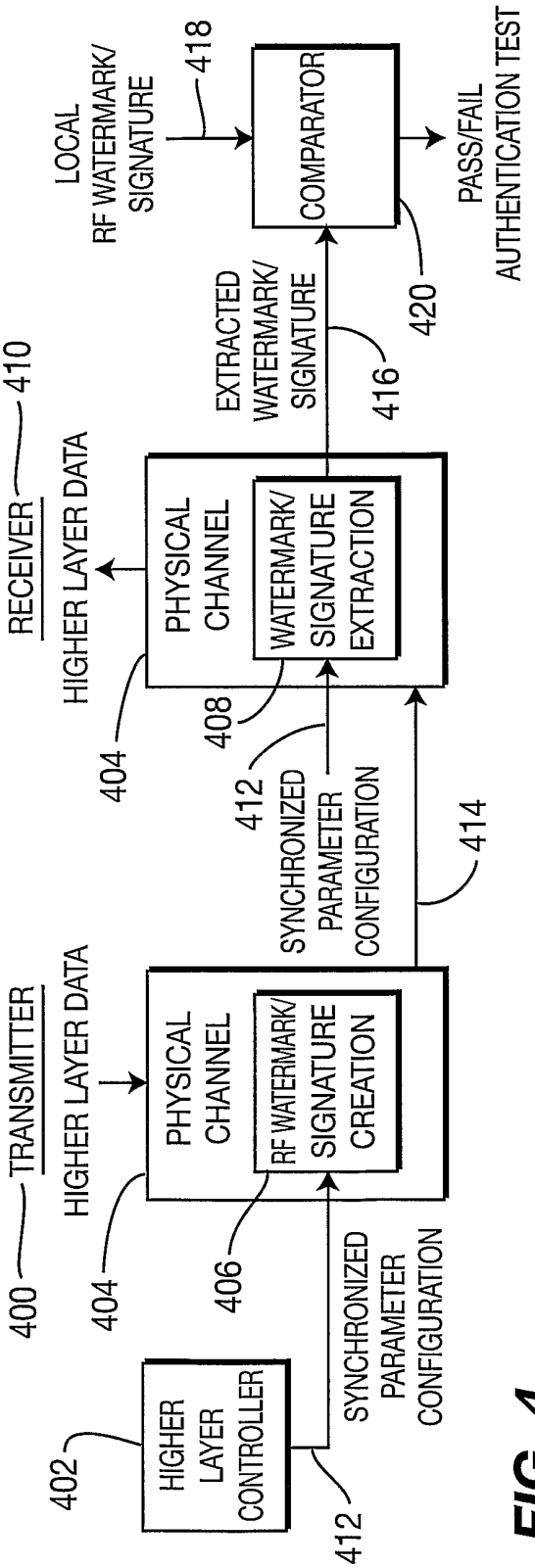

400
TRANSMITTER
HIGHER LAYER DATA
402
HIGHER LAYER CONTROLLER
404
PHYSICAL CHANNEL
406
RF WATERMARK/ SIGNATURE CREATION
412
SYNCHRONIZED PARAMETER CONFIGURATION
414
SYNCHRONIZED PARAMETER CONFIGURATION
410
RECEIVER
HIGHER LAYER DATA
404
PHYSICAL CHANNEL
408
WATERMARK/ SIGNATURE EXTRACTION
412
SYNCHRONIZED PARAMETER CONFIGURATION
416
EXTRACTED WATERMARK/ SIGNATURE
418
LOCAL RF WATERMARK/ SIGNATURE
420
COMPARATOR
PASS/FAIL AUTHENTICATION TEST

FIG. 4

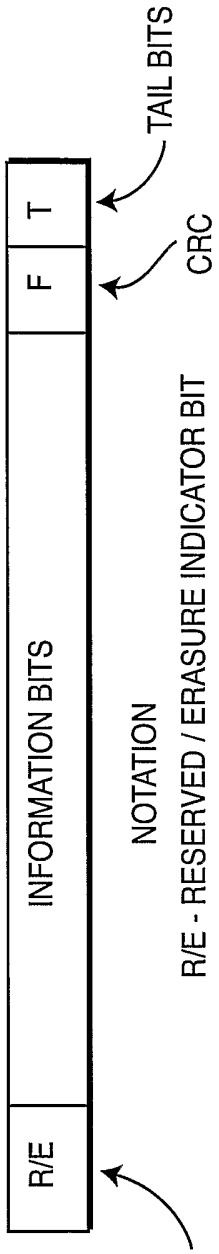

R/E
INFORMATION BITS
F
T
RESERVED
CRC
TAIL BITS
NOTATION
R/E - RESERVED / ERASURE INDICATOR BIT
F - FRAME QUALITY INDICATOR (CRC)
T - ENCODER TAIL BITS

FIG. 6

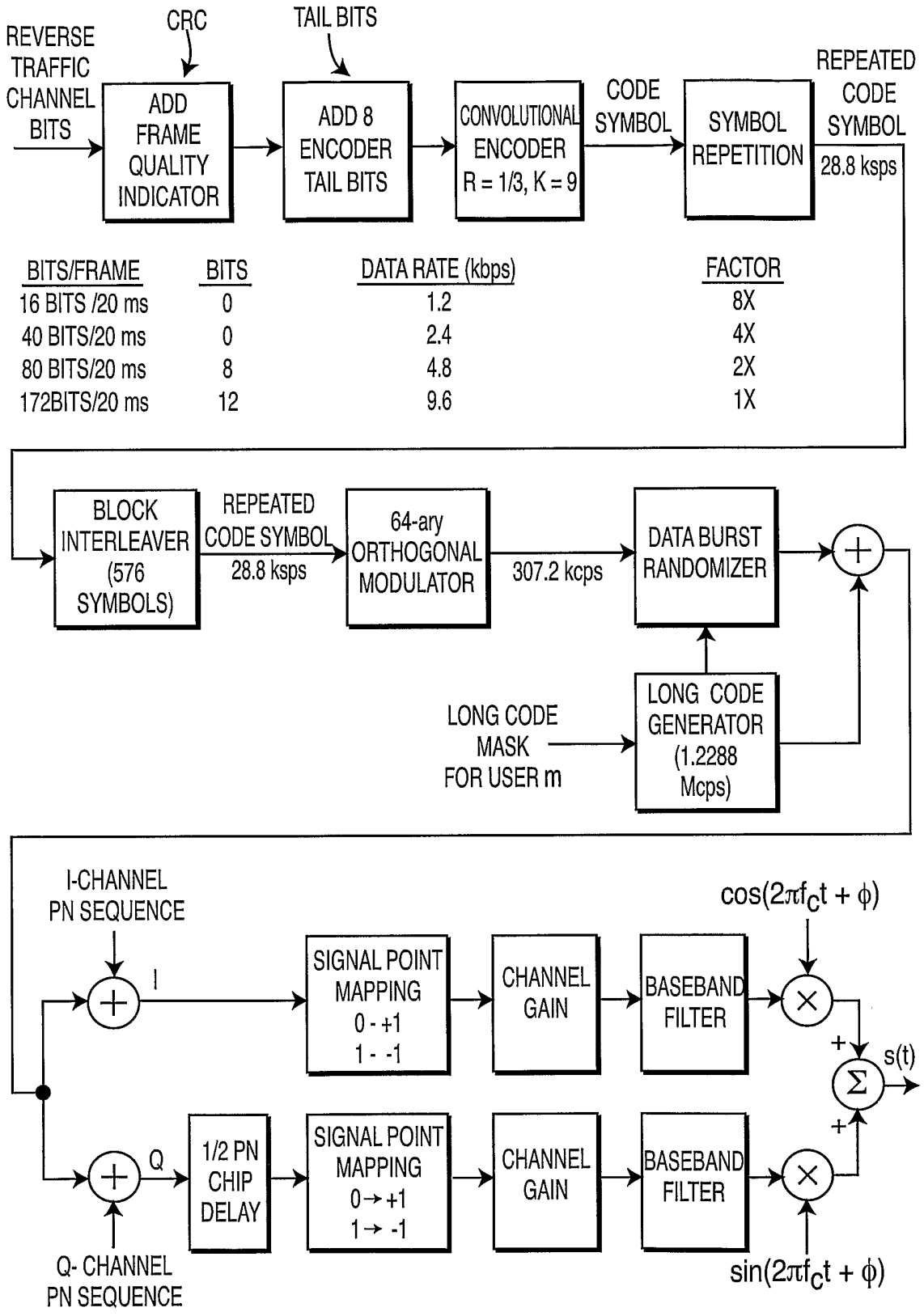
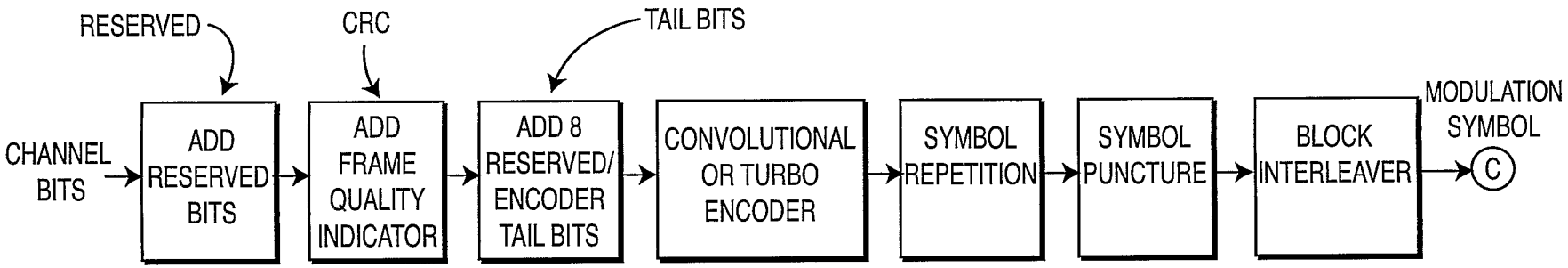

REVERSE TRAFFIC CHANNEL BITS
CRC
TAIL BITS
ADD FRAME QUALITY INDICATOR
ADD 8 ENCODER TAIL BITS
CONVOLUTIONAL ENCODER R = 1/3, K = 9
CODE SYMBOL
SYMBOL REPETITION
REPEATED CODE SYMBOL
28.8 ksps
BITS/FRAME BITS DATA RATE (kbps) FACTOR
16 BITS /20 ms 0 1.2 8X
40 BITS/20 ms 0 2.4 4X
80 BITS/20 ms 8 4.8 2X
172BITS/20 ms 12 9.6 1X
BLOCK INTERLEAVER (576 SYMBOLS)
REPEATED CODE SYMBOL
28.8 ksps
64-ary ORTHOGONAL MODULATOR
307.2 kcps
DATA BURST RANDOMIZER
LONG CODE MASK FOR USER m
LONG CODE GENERATOR (1.2288 Mcps)
I-CHANNEL PN SEQUENCE
I
SIGNAL POINT MAPPING 0 - +1 1 - -1
CHANNEL GAIN
BASEBAND FILTER
cos(2πf_c t + φ)
s(t)
Q
1/2 PN CHIP DELAY
SIGNAL POINT MAPPING 0→+1 1→ -1
CHANNEL GAIN
BASEBAND FILTER
Q- CHANNEL PN SEQUENCE
sin(2πf_c t + φ)

FIG. 5



BITS/ FRAME	BITS	BITS	DATA RATE (kbps)	R	FACTOR	DELETION	SYMBOLS	RATE (ksps)
24 BITS/ 5 ms	0	16	9.6	1/4	2x	NONE	384	76.8
21 BITS/20 ms	1	6	1.8	1/4	16x	8 of 24	1,536	76.8
55 BITS/20n ms	1	8	3.6 / n	1/4	8x	8 of 24	1,536	76.8 / n
125 BITS/20n ms	1	10	7.2 / n	1/4	4x	8 of 24	1,536	76.8 / n
267 BITS/20n ms	1	12	14.4 / n	1/4	2x	8 of 24	1,536	76.8 / n
552 BITS/20n ms	0	16	28.8 / n	1/4	1x	4 of 12	1,536	76.8 / n
1,128 BITS/20n ms	0	16	57.6 / n	1/4	1x	4 of 12	3,072	153.6 / n
2,280 BITS/20n ms	0	16	115.2 / n	1/4	1x	4 of 12	6,144	307.2 / n
4,584 BITS/20n ms	0	16	230.4 / n	1/4	1x	4 of 12	12,288	614.4 / n
1 TO 4,583 BITS/20n ms								

FIG. 7

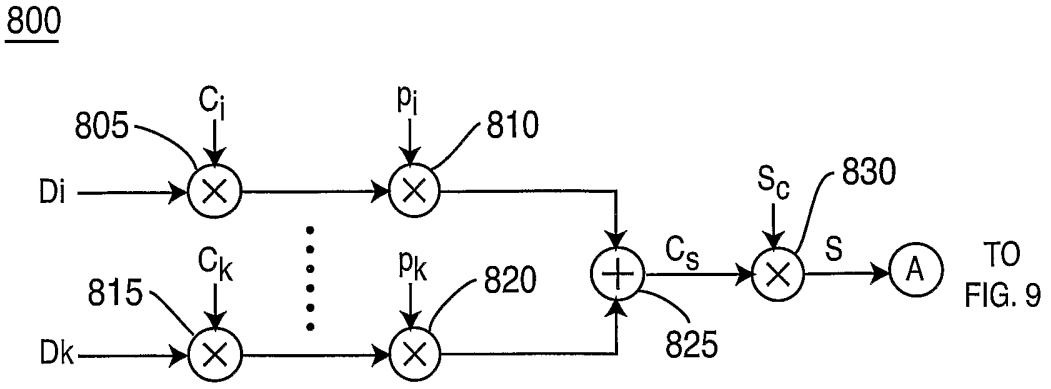


FIG. 8

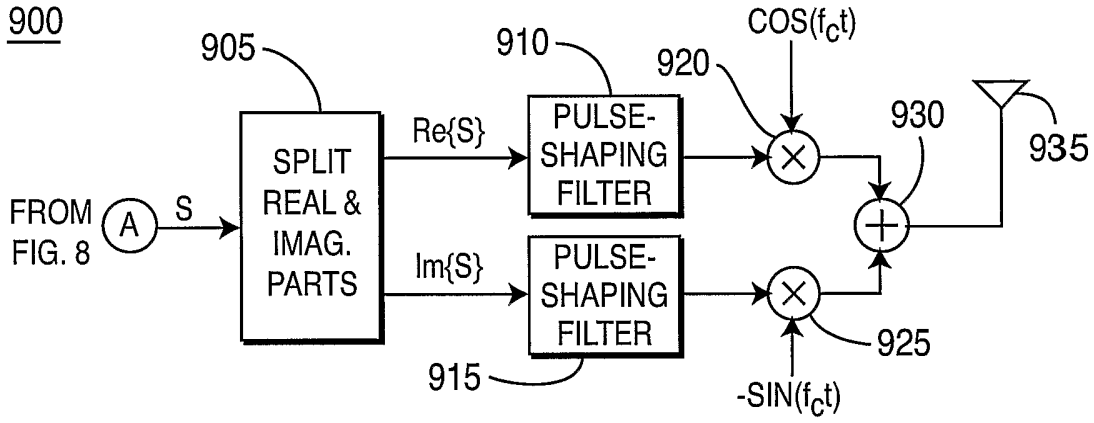


FIG. 9

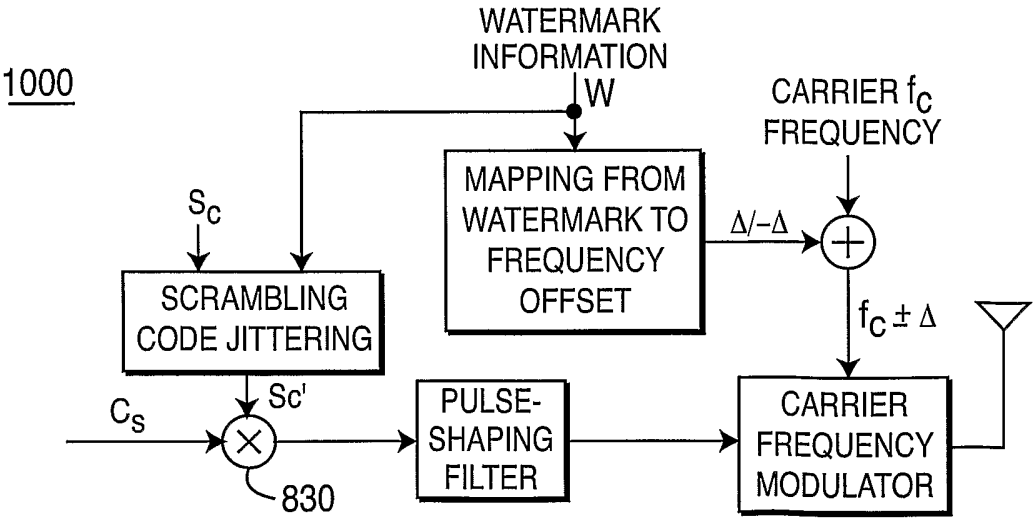


FIG. 10

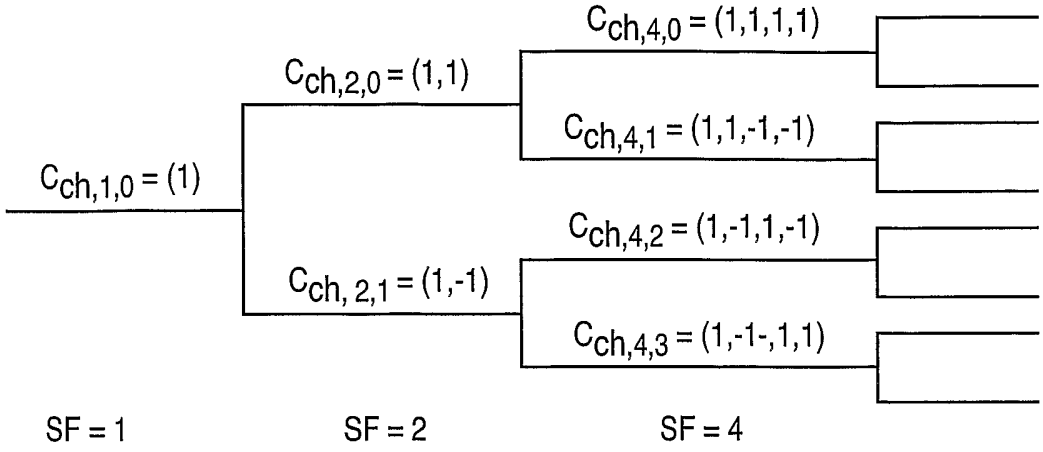


FIG. 11

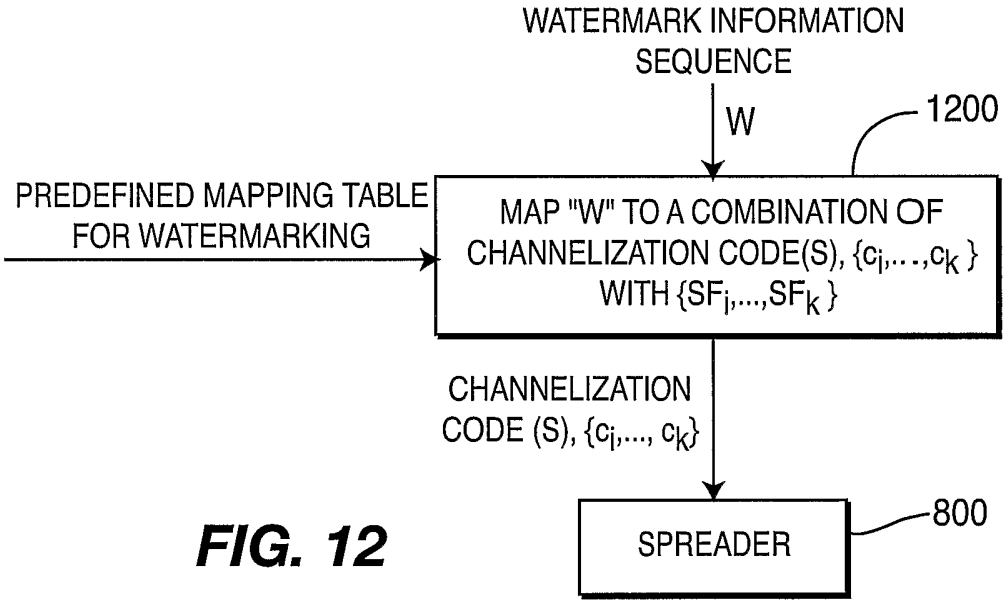


FIG. 12

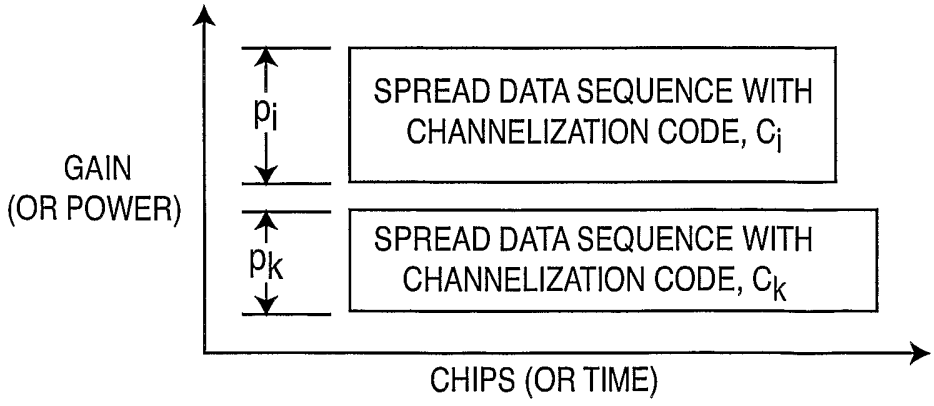


FIG. 13

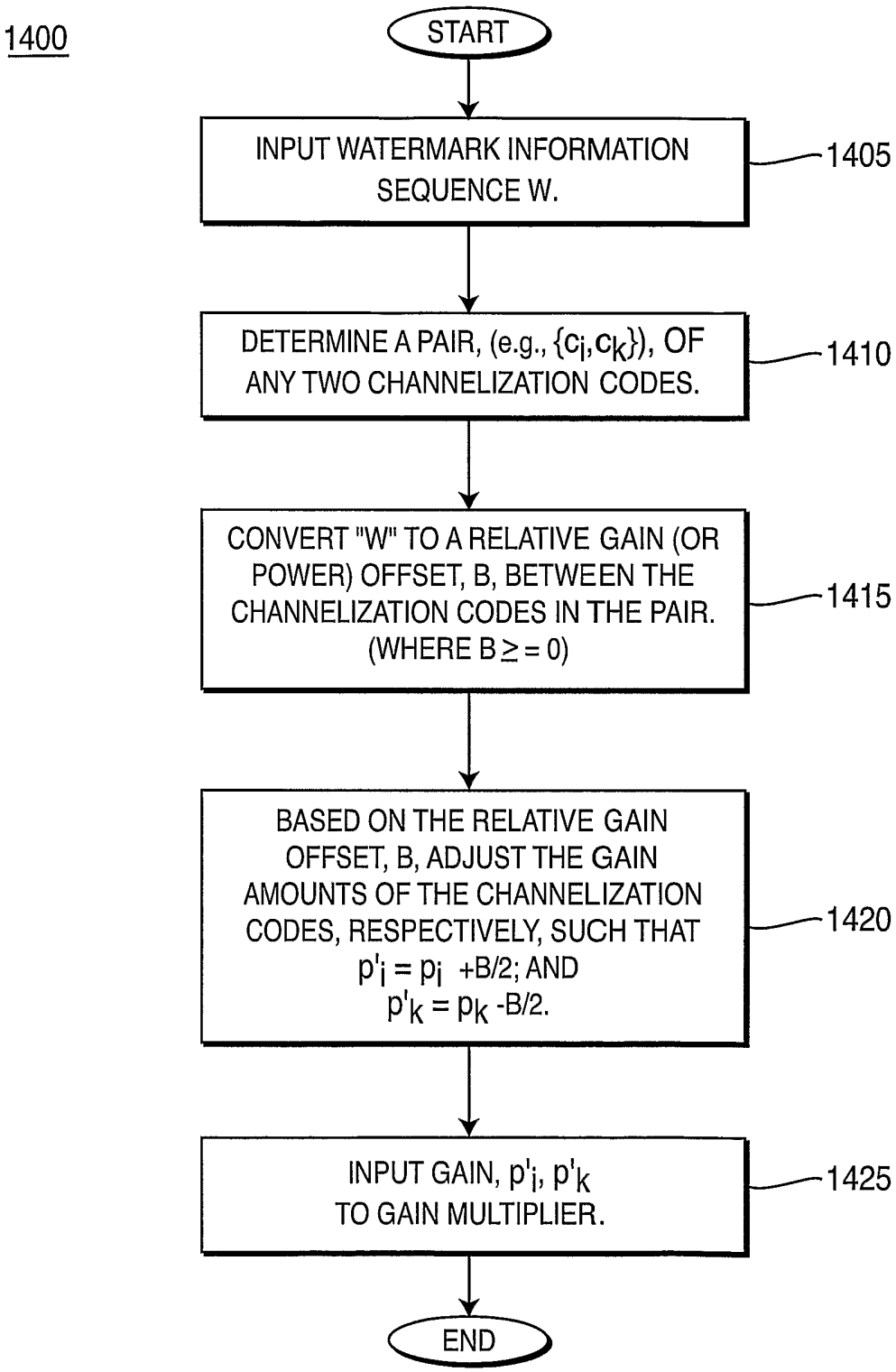

1400
START
INPUT WATERMARK INFORMATION SEQUENCE W.
1405
DETERMINE A PAIR, (e.g., {c_i,c_k}), OF ANY TWO CHANNELIZATION CODES.
1410
CONVERT "W" TO A RELATIVE GAIN (OR POWER) OFFSET, B, BETWEEN THE CHANNELIZATION CODES IN THE PAIR. (WHERE B ≥ = 0)
1415
BASED ON THE RELATIVE GAIN OFFSET, B, ADJUST THE GAIN AMOUNTS OF THE CHANNELIZATION CODES, RESPECTIVELY, SUCH THAT
$p'_i = p_i + B/2$; AND
$p'_k = p_k - B/2$.
1420
INPUT GAIN, p'_i, p'_k TO GAIN MULTIPLIER.
1425
END

FIG. 14

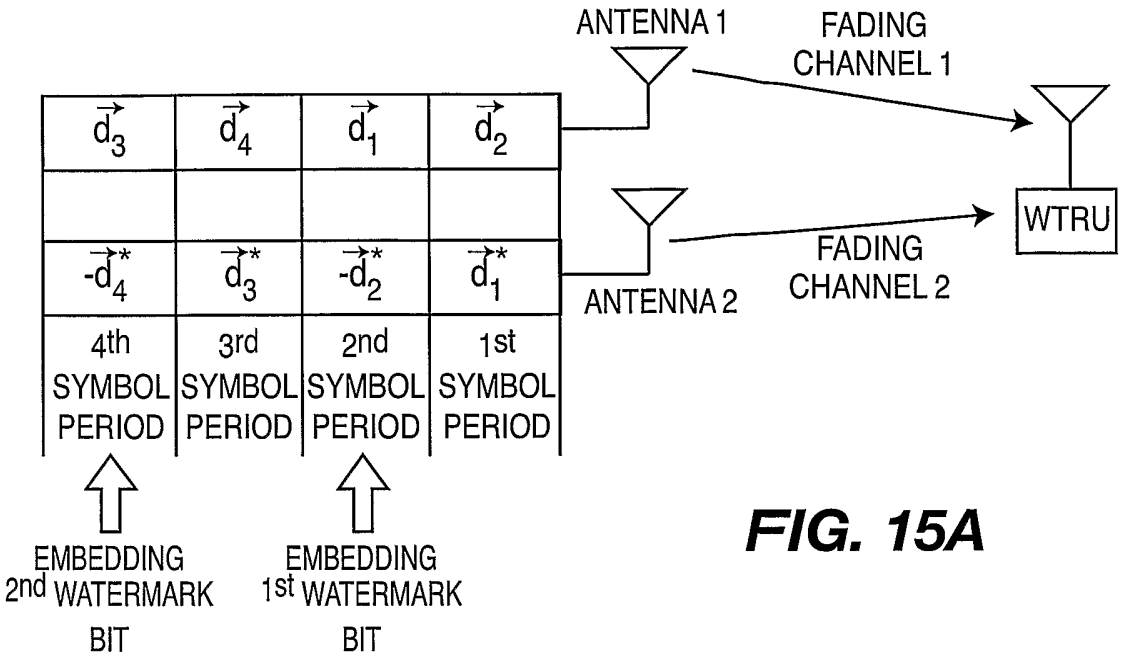


FIG. 15A

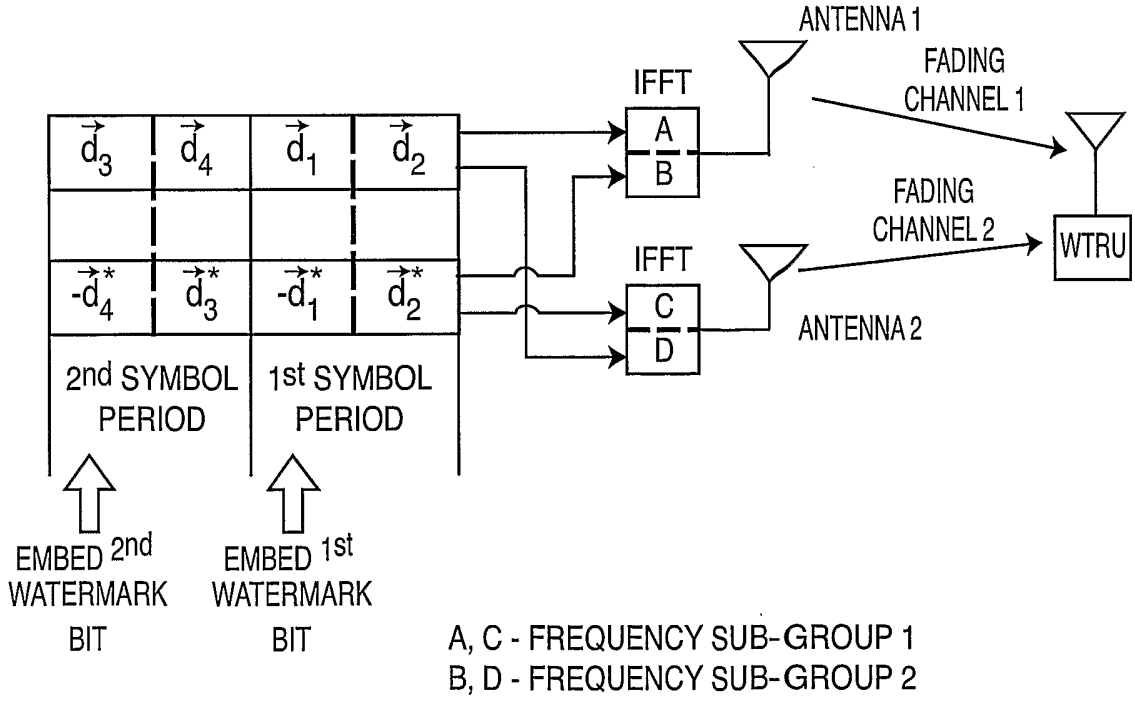


FIG. 15B

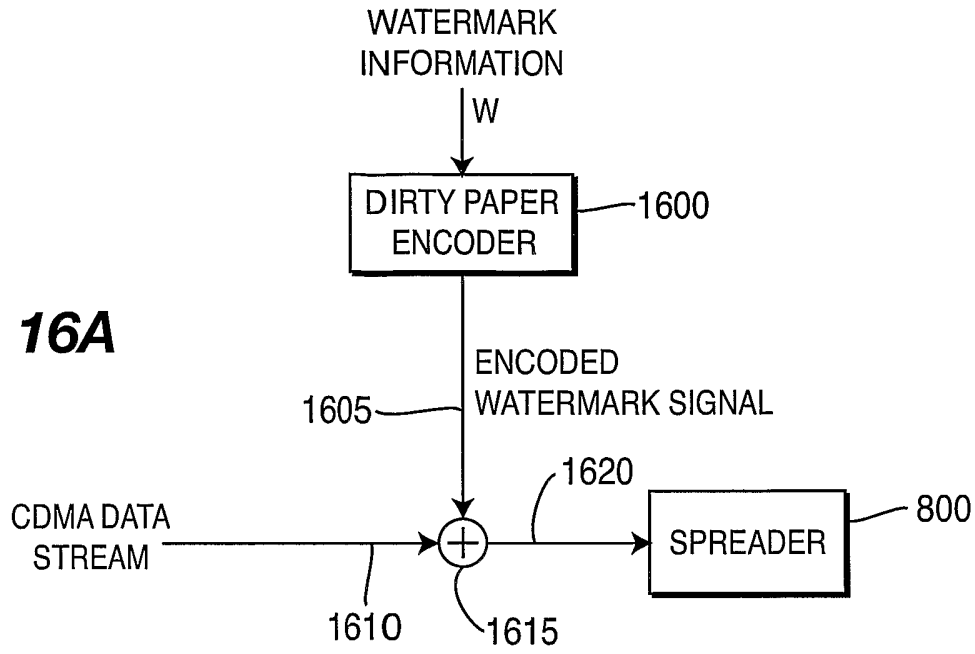


FIG. 16A

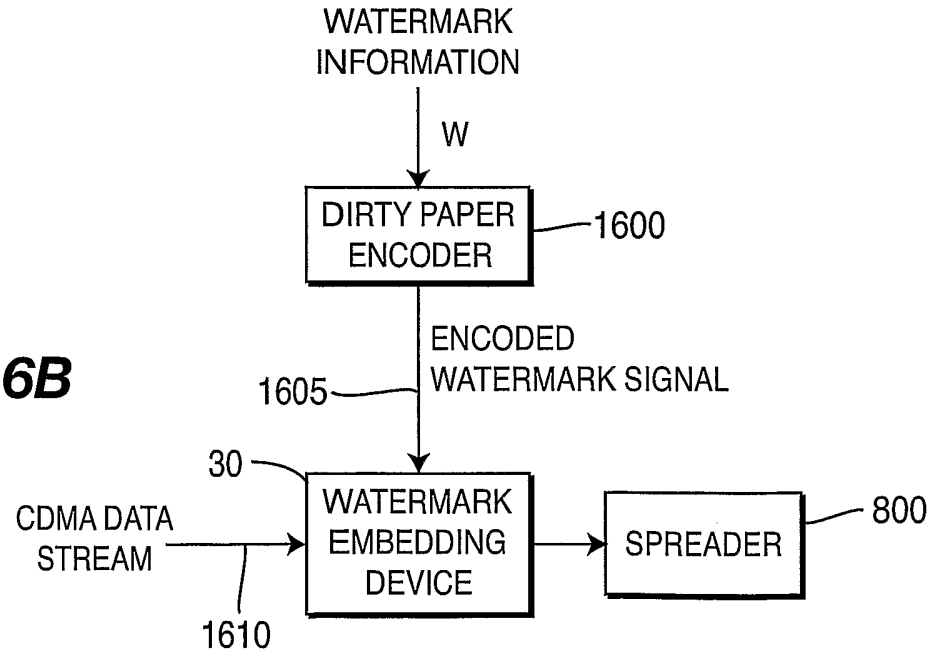


FIG. 16B

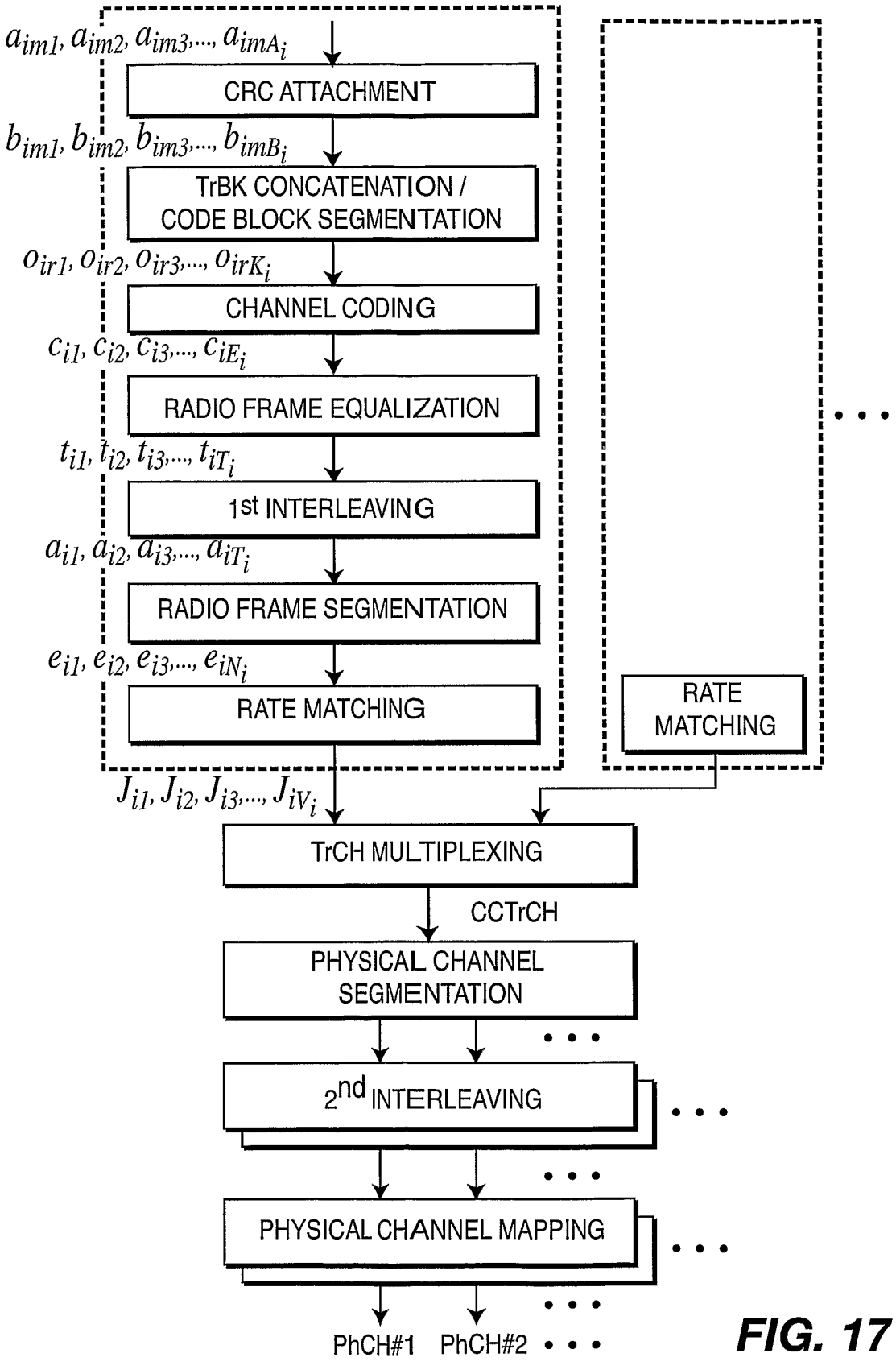

$a_{im1}, a_{im2}, a_{im3}, ..., a_{imA_i}$
CRC ATTACHMENT
$b_{im1}, b_{im2}, b_{im3}, ..., b_{imB_i}$
TrBK CONCATENATION / CODE BLOCK SEGMENTATION
$o_{ir1}, o_{ir2}, o_{ir3}, ..., o_{irK_i}$
CHANNEL CODING
$c_{i1}, c_{i2}, c_{i3}, ..., c_{iE_i}$
RADIO FRAME EQUALIZATION
$t_{i1}, t_{i2}, t_{i3}, ..., t_{iT_i}$
1st INTERLEAVING
$a_{i1}, a_{i2}, a_{i3}, ..., a_{iT_i}$
RADIO FRAME SEGMENTATION
$e_{i1}, e_{i2}, e_{i3}, ..., e_{iN_i}$
RATE MATCHING
RATE MATCHING
$J_{i1}, J_{i2}, J_{i3}, ..., J_{iV_i}$
TrCH MULTIPLEXING
CCTrCH
PHYSICAL CHANNEL SEGMENTATION
2nd INTERLEAVING
PHYSICAL CHANNEL MAPPING
PhCH#1
PhCH#2

FIG. 17

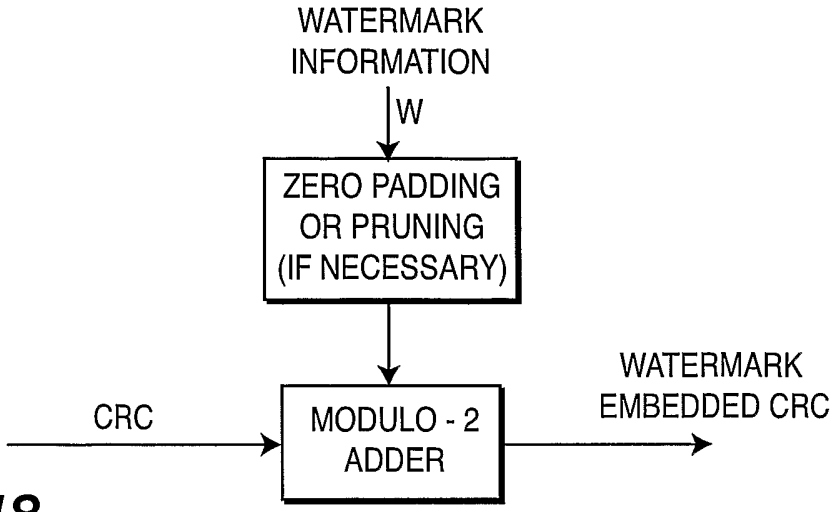


FIG. 18

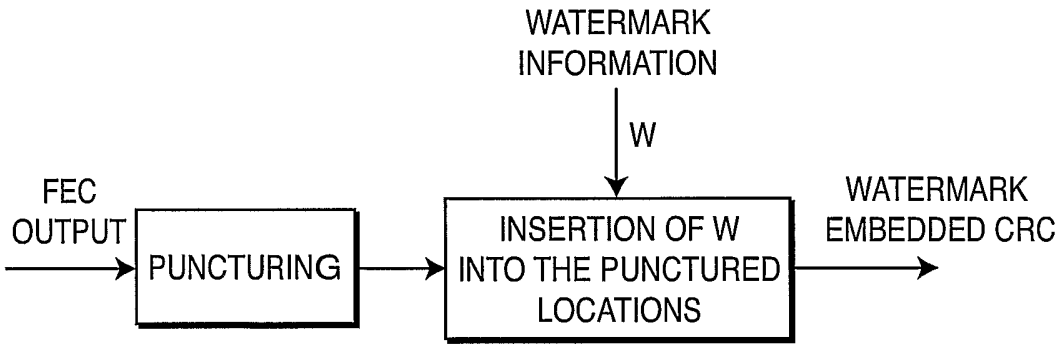


FIG. 20

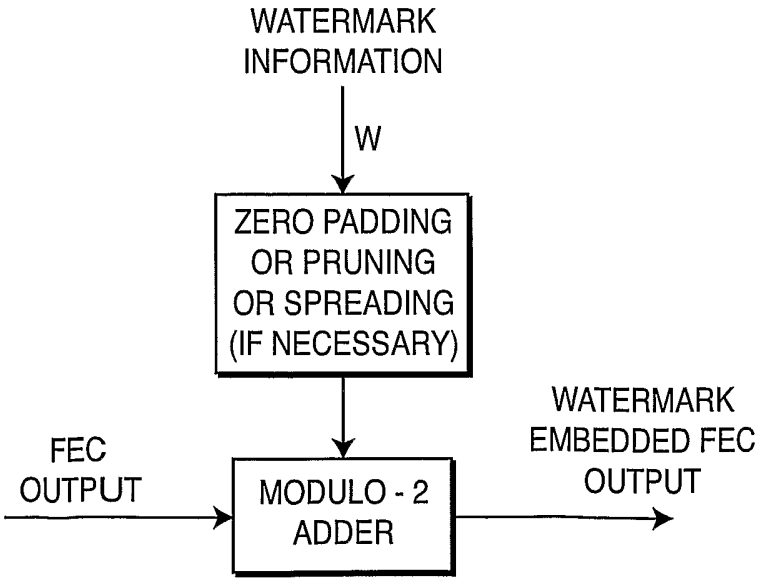


FIG. 21

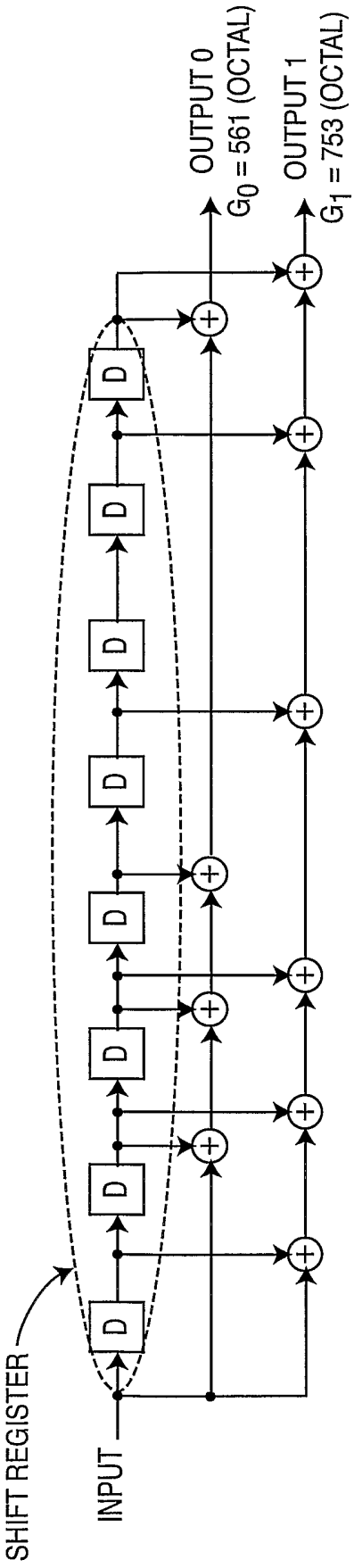


FIG. 19A

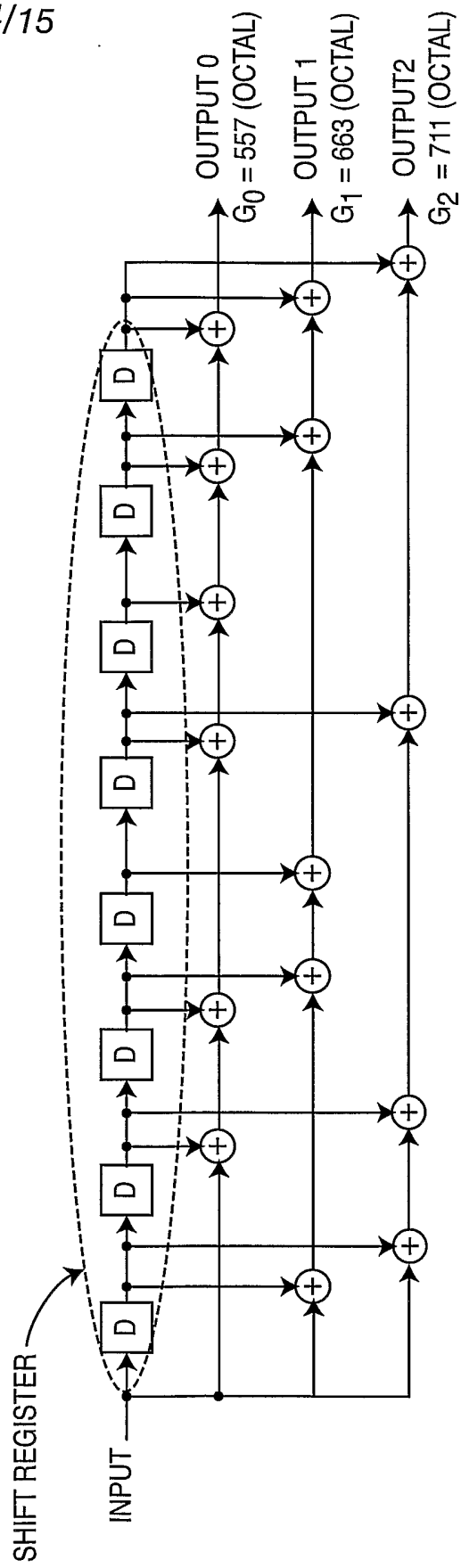


FIG. 19B

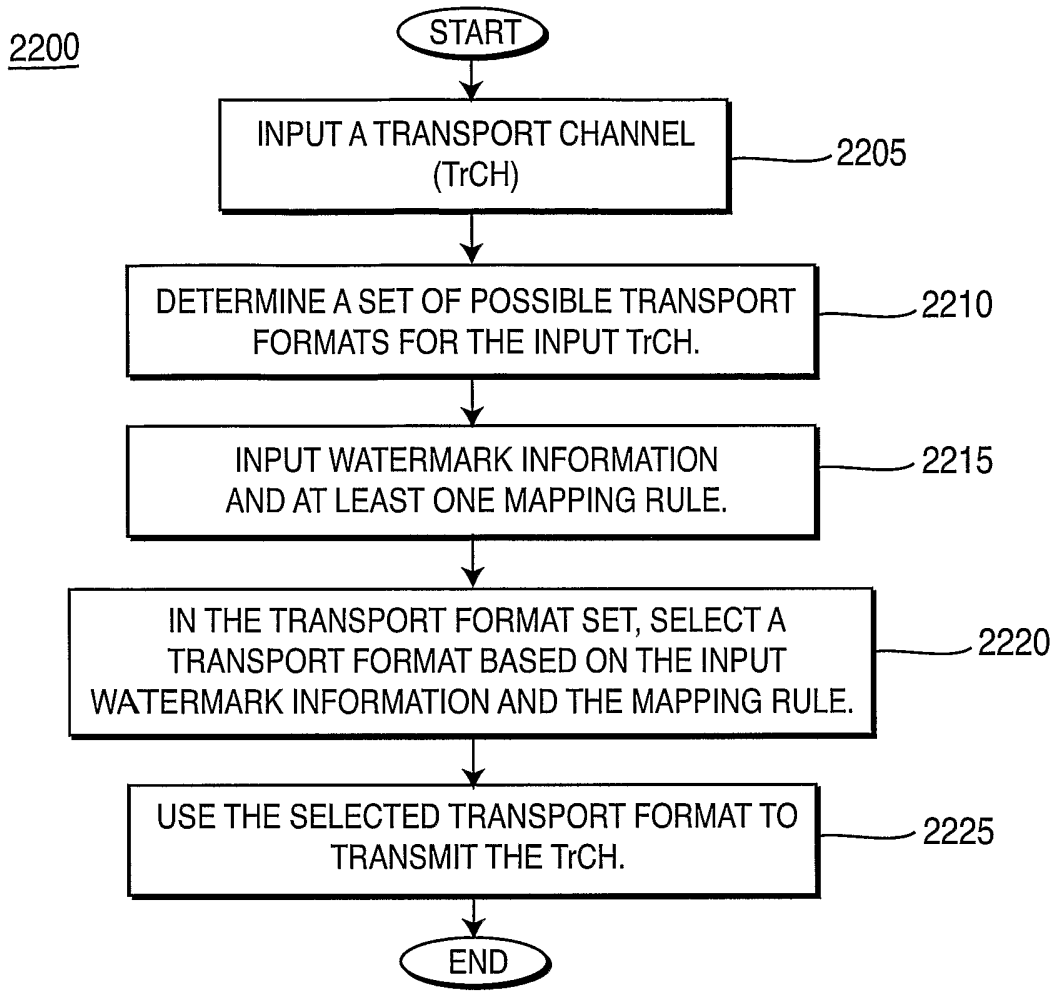

2200
START
INPUT A TRANSPORT CHANNEL (TrCH)
2205
DETERMINE A SET OF POSSIBLE TRANSPORT FORMATS FOR THE INPUT TrCH.
2210
INPUT WATERMARK INFORMATION AND AT LEAST ONE MAPPING RULE.
2215
IN THE TRANSPORT FORMAT SET, SELECT A TRANSPORT FORMAT BASED ON THE INPUT WATERMARK INFORMATION AND THE MAPPING RULE.
2220
USE THE SELECTED TRANSPORT FORMAT TO TRANSMIT THE TrCH.
2225
END

FIG. 22

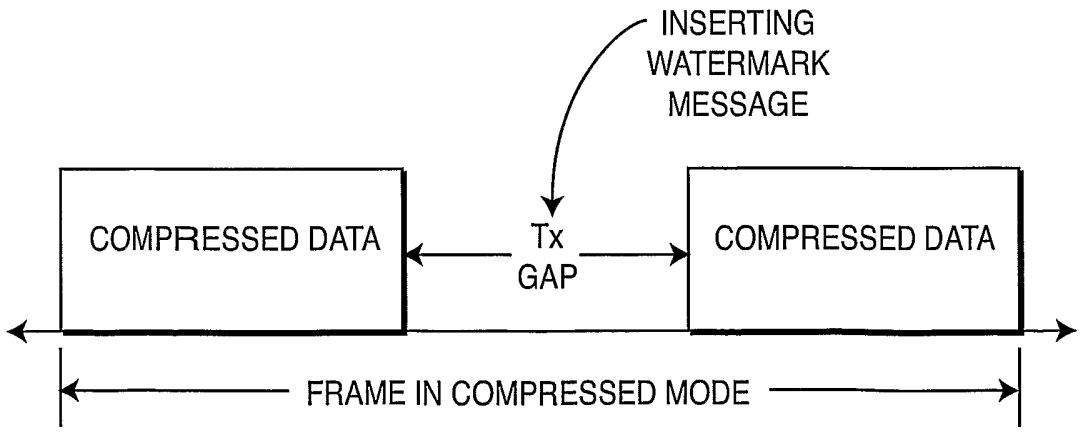

INSERTING WATERMARK MESSAGE
COMPRESSED DATA
Tx GAP
COMPRESSED DATA
FRAME IN COMPRESSED MODE

FIG. 23