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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 June 2006 (08.06.2006)

PCT

(10) International Publication Number
WO 2006/060362 A2

(51) International Patent Classification:
H04K 1/00 (2006.01)

(21) International Application Number:
PCT/US2005/043061

(22) International Filing Date:
28 November 2005 (28.11.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/633,222 3 December 2004 (03.12.2004) US
11/284,940 22 November 2005 (22.11.2005) US

(71) Applicant *(for all designated States except US)*: **INTERDIGITAL TECHNOLOGY CORPORATION** [US/US]; 300 Delaware Avenue, Suite 527, Wilmington, DE19801 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **SHARMA, Sanjeev, K.** [IN/US]; 1501 Maywood Lane, Pottsville, PA 19464 (US).

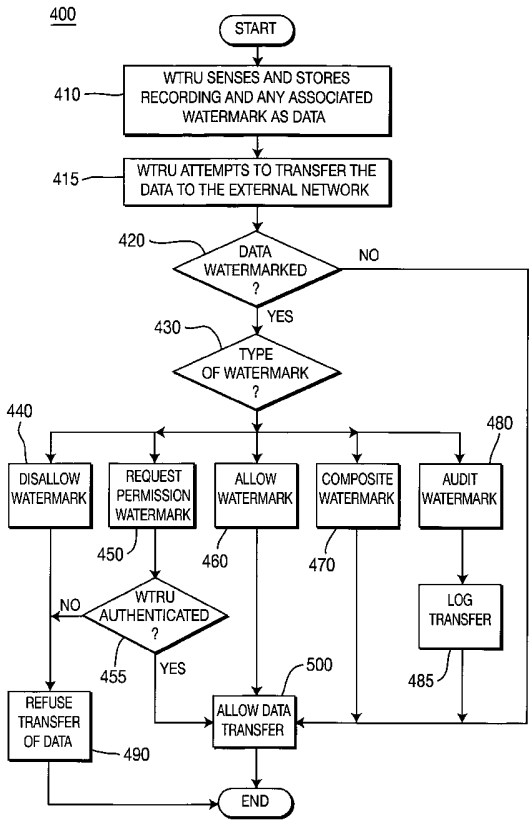
(74) Agent: **BALLARINI, Robert, J.**; Volpe and Koenig, P.C., United Plaza, Suite 1600, 30 South 17th Street, Philadelphia, PA 19103 (US).

(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, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, 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, LV, MC, NL, PL, PT,

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR PREVENTING UNAUTHORIZED DATA FROM BEING TRANSFERRED



(57) Abstract: A method and apparatus for preventing the transfer of unauthorized data among a wireless transmit/receive unit (WTRU), an external network, and at least one access point in a wireless communication system includes the WTRU recording a subject and storing the recording as data in a memory of the WTRU. The WTRU transmits the data to the access point. The access point examines the data to determine if the data is allowed for transfer to the external network.

WO 2006/060362 A2

RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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] METHOD AND APPARATUS FOR PREVENTING UNAUTHORIZED DATA FROM BEING TRANSFERRED

[0002] FIELD OF INVENTION

[0003] The present invention relates to sensed data. More particularly, the present invention relates to a method and apparatus for preventing unauthorized data from being transferred.

[0004] BACKGROUND

[0005] With ever increasing sophistication in available technology, piracy of intellectual property has become widespread. Pirated movies on DVD or VHS often appear concurrently with the first run of the movies in theaters. Making anti-piracy efforts even more difficult, sensing devices which used to be somewhat bulky have become miniaturized, such that their physical presence often escapes detection. These sensing devices such as cameras, microphones, video recorders, and sound recorders can now be embedded in phones, personal digital assistants (PDAs), watches, or any other wireless transmit/receive unit (WTRU) that a manufacturer desires. It has therefore become easier than ever to secrete a sensing device into an event such as a play, movie, and the like.

[0006] These sensing devices can record and/or transmit images and sounds that are not authorized to be recorded or transmitted by the individual recording them. Once a scene or a sound has been captured, the sensed data may be distributed fairly easily through a variety of channels, such as a cellular or other wireless communication network.

[0007] To combat this piracy, some businesses have attempted to regulate miniaturized sensing devices by either posting restrictions in restricted areas or by physically searching for their existence. However, these methods are often difficult to enforce, ineffective and inefficient.

[0008] Electronic control of sensing has been attempted with systems which broadcast radio frequency (RF) beacons that signal sensing devices to disable their sensing functionality. The problem, however, with electronically regulating sensing devices in such a manner is that a sensing device must be so

equipped in order to receive such RF signals, and a large number of sensing devices are not. In those devices that are so equipped, the RF receiving functionality can easily be modified by the user of the device whom may be able to hack into, and disable, the functionality preventing sensing.

[0009] Since modern WTRUs often come integrated with enhanced storage and transmission functionality, an ever increasing quantity of timely unauthorized data can be transferred by the WTRU. Accordingly, it is desirable to have a method and apparatus for preventing the transfer of unauthorized data over a wireless communication system.

[0010] SUMMARY

[0011] A method and apparatus for preventing the transfer of unauthorized data among a wireless transmit/receive unit (WTRU), an external network, and at least one access point in a wireless communication system includes the WTRU recording a subject and storing the recording as data in a memory of the WTRU. The WTRU transmits the data to the access point. The access point examines the data to determine if the data is permitted to be transferred to the external network.

[0012] BRIEF DESCRIPTION OF THE DRAWINGS

[0013] The foregoing summary, as well as the following detailed description of the preferred embodiments of the present invention will be better understood when read with reference to the appended drawings, wherein:

[0014] Figure 1 shows a wireless communication system configured in accordance with the present invention;

[0015] Figure 2 shows a block diagram of a WTRU and an access point configured to perform a method for preventing unauthorized data from being transferred;

[0016] Figure 3 shows a signal diagram of the WTRU and access point performing a method of preventing the transmission of unauthorized data in the wireless communication system of Figure 1; and

[0017] Figure 4 is a flow diagram depicting a preferred method of preventing the transmission of unauthorized data, in accordance with the present invention.

[0018] DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0019] Hereafter, the terminology "WTRU" includes, but is not limited to, a user equipment (UE), a computer, a mobile station, a fixed or mobile subscriber unit, a pager, or any other type of device capable of operating in a wireless environment. When referred to hereafter, an access point (AP) includes a base station or a radio network controller (RNC), including but not limited to a Node-B, site controller, or any other type of interfacing device in a wireless environment.

[0020] Figure 1 is a wireless communication system 100 configured in accordance with the present invention. The wireless communication system 100 includes a plurality of WTRUs 110 and at least one AP 120 in communication with the WTRUs 110. The AP 120 is in communication with an external network 210, and is therefore capable of permitting the WTRUs 110 to communicate with the external network 210 to transfer data.

[0021] The external network 210 may include the Internet, a plain old telephone service (POTS) network, a public switched telephone network (PSTN), or any other system known to one of ordinary skill in the art adapted to allow the transfer of data. Also shown is a subject S, which may be sensed, or recorded, by the WTRUs 110. Although not part of the present invention, a watermark may be imparted upon the subject S in a variety of ways. For example, the watermark may be generated by a watermark generator (not shown) in the environment where the subject S exists. That is, the watermark generator may project the watermark onto to the subject S from a location proximate to the subject S. The imparted watermark on the subject S may be utilized to regulate the transfer of any data containing the subject S in the WTRUs 110.

[0022] Figure 2 shows a block diagram of the WTRU 110 and the AP 120 configured to prevent the transfer of unauthorized data, in accordance with the present invention.

[0023] In addition to the nominal components included in a typical WTRU, the WTRU 110 includes a processor 115 configured to process sensed data, a receiver 116 in electrical communication with the processor 115, a transmitter 117 in electrical communication with the processor 115, a sensor 118 in electrical communication with the processor 115, a memory 119 in electrical communication with the processor 115, and an antenna 114 in electrical communication with both the receiver 116 and the transmitter 117 to facilitate the transferring and receiving of wireless data.

[0024] The sensor 118 in a preferred embodiment of the present invention may be a video or audio sensor to record video images or audio waves. However, the sensor 118 may be any sensor known to one of ordinary skill in the art that can be utilized to sense data such as the subject S or any watermark imparted upon the subject S. The receiver 116 and transmitter 117 of the WTRU 110 include any type of receiver and transmitter capable of wirelessly receiving and transmitting data, respectively, through the antenna 114.

[0025] In addition to the nominal components included in a typical access point, the AP 120 includes a processor 125 configured to prevent the transfer of unauthorized data from the WTRU 110, a receiver 126 in electrical communication with the processor 125, a transmitter 127 in electrical communication with the processor 125, a memory 129 in electrical communication with the processor 125, and an antenna 124 in electrical communication with both the receiver 126 and the transmitter 127 to facilitate the transferring and receiving of wireless data. In addition, the processor 125 is in communication with the external network 210.

[0026] The receiver 126 and transmitter 127 of the AP 120 include any type of receiver and transmitter capable of wirelessly receiving and transmitting data, respectively, through the antenna 124.

[0027] Figure 3 shows a signal diagram between the WTRU 110, the AP 120, and the external network 210 during an attempt by the WTRU 110 to transfer data to the external network 210 through the AP 120. In general, the sensor 118 of the WTRU 110 senses the subject S and any imparted watermark as data, which it transfers to the processor 115 of the WTRU 110 for transmission of the data (310) via the transmitter 117 and antenna 114 to the AP 120. The receiver 126 of the AP 120 receives the data from the WTRU 110 through the antenna 124 and transfers the data to the processor 125, which examines the data to determine whether to permit transfer of the data to the external network 210.

[0028] If the data contains no watermark or a watermark that permits transfer, then the processor 125 authorizes the data to be transferred to the external network 210 (320). If the data contains a watermark that does not permit transfer, then the data transfer will be refused (330) by the processor 125 of the AP 120. Depending on a sensitivity level of the watermark, which will be described in more detail below, the processor 125 may take additional action beyond simply permitting or refusing the transfer of the data (330).

[0029] Figure 4 is a flow diagram depicting a preferred method 400 of preventing the transmission of unauthorized data, in accordance with the present invention. In step 410, the sensor 118 of the WTRU 110 senses the subject S and transfers a recording thereof to the processor 115, which stores the sensed subject S, along with any watermark imparted thereon, as data in the memory 119 of the WTRU 110. The processor 115 of the WTRU 110 then attempts to transfer the data (step 415) from the memory 119 to the external network 210 by transmitting the data to the AP 120 through the transmitter 117 and antenna 114 of the WTRU 110.

[0030] The receiver 126 receives the data from the antenna 124, and transfers the data to the processor 125 of the AP 120. The processor 125 examines the data to determine if a watermark is imparted on it (step 420). If no watermark is present in the data, then the processor 125 permits the data to be transferred to the external network 210 (step 500). If a watermark is present in

the data, then the processor 125 of the AP 120 determines the type of watermark present in the data (step 430) and acts in accordance with Table 1 below.

[0031]

Table 1

WATERMARK TYPE	SENSITIVITY LEVEL	ACTION
None	N/A	Allow Data Transfer
Allow	N/A	Allow Data Transfer
Disallow	None	Refuse Data Transfer
Disallow	1	Refuse Data Transfer
Disallow	2	Refuse Data Transfer and Warn WTRU of Attempt to Transfer Unauthorized Data
Disallow	3	Refuse Data Transfer, Warn WTRU against Attempt to Transfer Unauthorized Data, and Place WTRU on a Blacklist
Disallow	4	Refuse Data Transfer, Warn WTRU of Attempt to Transfer Unauthorized Data, Place WTRU on a Blacklist, and Alert Security Personnel
Request Permission	N/A	Authenticate WTRU
Composite	N/A	Allow Data Transfer
Audit	N/A	Allow Data Transfer and Log Transfer

[0032] If an allow watermark (step 460) is present in the data, then the processor 125 of the AP 120 allows transfer of the data to the external network 210 (step 500).

[0033] If a disallow watermark (step 440) is present in the data, then the processor 125 refuses the transfer of the data to the external network 210 (step 490). Depending on the whether or not a sensitivity level is associated with the watermark, the processor 125 of the AP 120 may take additional actions.

[0034] If there is no sensitivity level associated with the disallow watermark, or a sensitivity level of 1 is associated with the watermark, then the processor 125 takes no additional action beyond refusing the transfer of the data.

[0035] If there is a sensitivity level of 2 associated with the watermark, then the processor 125 refuses the transfer of data to the external network 210 (step 490) and transmits a warning to the WTRU 110 attempting to transfer the

unauthorized data via the transmitter 127 and antenna 124 of the AP 120. This warning can be a visual or audible message transmitted to the WTRU 110 by the processor 125 of the AP 120, or any other warning known to one of ordinary skill in the art.

[0036] If there is a sensitivity level of 3 associated with the watermark, the processor 125 refuses the transfer of data to the external network 210 (step 490), transmits a warning to the WTRU 110 attempting to transfer the unauthorized data via the transmitter 127 and antenna 124 of the AP 120, and blacklists the WTRU 110 attempting to transfer the unauthorized data. The processor 125 may accomplish this by storing identifying information regarding the WTRU 110 in the memory 129 of the AP 120. This identifying information stored in the memory 129 may then be accessed at a later point in time by the processor 125 the next time the particular WTRU 110 associated with the identifying information attempts to transfers data to the external network 210. In a preferred embodiment of the present invention, the WTRU 110 would be subsequently prevented from transferring any data to the external network 210 once placed on the blacklist. Additionally, the WTRU 110 may be refused a connection the next time the WTRU 110 attempts to connect.

[0037] If there is a sensitivity level of 4 associated with the watermark, the processor 125 of the AP 120 refuses the transfer of data to the external network 210 (step 490), transmits a warning to the WTRU 110 attempting to transfer the unauthorized data via the transmitter 127 and antenna 124 of the AP 120, blacklists the WTRU 110 attempting to transfer the unauthorized data, and transmits an alert to security personnel via the transmitter 127 and the antenna 124 of the AP 120. The security personnel may receive this alert on WTRUs 110 that they possess. In a preferred embodiment of the present invention, the security personnel are local security personnel that may be able to apprehend the individual attempting unauthorized transfer of data. However, less local security personnel may be notified for a response at a later time.

[0038] Although only five security levels (none, 1, 2, 3, and 4) associated with the disallow watermark have been discussed, it can be seen by one of

ordinary skill in the art that any number of security levels can be associated with the disallow watermark. Moreover, a person of ordinary skill in the art can appreciate that additional actions to the ones described above can be undertaken, as well as varying the combination of actions described above. For example, the action taken for a disallow watermark having an associated sensitivity level of 3 can further include the action taken for a disallow watermark having an associated sensitivity level of 4.

[0039] If a request permission watermark is present in the data (step 450), then the processor 125 of the AP 120 attempts to authenticate the WTRU 110 that is attempting to transfer data to the external network 210 (step 455). If the processor 125 authenticates the WTRU 110, then the processor 125 allows the transfer of data to the external network (step 500). Otherwise, the transfer is refused (step 490).

[0040] An example of WTRU identification may be in the form of an identification code stored in the memory 119, associated with the particular WTRU 110 attempting to transfer the data being transmitted along with the data by the WTRU 110. For example, when the WTRU 110 desires to transfer the data to the external network 210, the processor 115 of the WTRU 110 extracts the authentication code from the memory 119 and transmits it, along with the data, to the AP 120 via the transmitter 117 and antenna 114 of the WTRU 110.

[0041] The receiver 125 of the AP 120 receives the data along with the identification code from the antenna 124 and transfers it to the processor 125. The processor 125 searches the memory 129 for valid identification codes to determine if the authentication code sent by the WTRU 110 is valid. If the authentication code sent by the WTRU 110 is valid, then the processor 125 allows transfer of the data to the external network 210 (step 500). If the authentication code is not valid, then the processor 125 refuses the data transfer to the external network 210 (step 490).

[0042] For example, a security office at an event might provide an access passcode as the identification code to some WTRU 110 users in order to enable

them to record and transfer data to the external network 210 during that particular session. Accordingly, the WTRUs 110 that can transmit the identification code will pass the authentication, while WTRUs not transmitting the identification code will not be able to do so, and thus will be refused transfer of data to the external network 210. In a preferred embodiment of the present invention, the identification code will expire after the session.

[0043] If a composite watermark is present in the data (step 470), then the processor 125 allows the transfer of the data to the external network 210 (step 500). In a preferred embodiment of the present invention, the composite watermark typically includes the disallow watermark introduced by the environment combined with the allow watermark. An example of the composite watermark may be a watermark that is contained on the WTRU of a security officer. This composite watermark may override any other watermark in order to allow the transfer of data to the external network 210 without any other restrictions.

[0044] If an audit watermark is present in the data (step 480), then the processor 125 of the AP 120 allows the transfer of the data to the external network 210 (step 500), and logs the transfer (step 485) in the memory 129 of the AP 120 for later access. For example, after allowing the transfer, the event can be logged for auditing purposes later, such as how many recordings were made of the subject, how many were transferred, or the like.

[0045] 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. For example, in a preferred embodiment of the present invention, the method may be performed by an application running on the processor of the access point, or alternatively, may be implemented as an integrated circuit (IC).

* * *

CLAIMS

What is claimed is:

1. A method for preventing the transfer of unauthorized data among a wireless transmit/receive unit (WTRU), an external network, and at least one access point in a wireless communication system, comprising:

the WTRU recording a subject and storing the recording as data in a memory of the WTRU;

the WTRU transmitting the data to the access point; and

the access point examining the data to determine if the data is allowed for transfer to the external network.

2. The method of claim 1, wherein the access point allows the transfer of the data to the external network if the data does not include a watermark.

3. The method of claim 1, wherein the data includes a watermark imparted on it.

4. The method of claim 3, wherein the watermark is an allow watermark.

5. The method of claim 4, wherein the access point allows the transfer of the data to the external network.

6. The method of claim 3, wherein the watermark is a disallow watermark.

7. The method of claim 6, wherein no sensitivity level is associated with the watermark and the access point refuses the transfer of the data to the external network.

8. The method of claim 6, wherein a sensitivity level is associated with the watermark and the access point refuses the transfer of the data to the external network.

9. The method of claim 8, wherein the access point warns the user of the WTRU of the attempt to transfer unauthorized data.

10. The method of claim 9, wherein the access point warning the user of the WTRU of the attempt to transfer unauthorized data includes transmitting a message to the user on the WTRU.

11. The method of claim 9, wherein the access point places the WTRU on a blacklist.

12. The method of claim 11, wherein the access point stores identifying information about the WTRU in a memory of the access point.

13. The method of claim 11, wherein the access point notifies security personnel of the attempt by the WTRU to transfer unauthorized data to the external network.

14. The method of claim 3, wherein the watermark is a composite watermark and the access point allows the transfer of the data to the external network.

15. The method of claim 3, wherein the watermark is an audit watermark and the access point allows the transfer of the data to the external network.

16. The method of claim 15, wherein the access point logs the transfer of the data to the external network by storing the transfer in a memory of the access point.

17. The method of claim 3, wherein the watermark is a request permission watermark.

18. The method of claim 17, wherein the access point authenticates the WTRU attempting to transfer the data to the external network.

19. The method of claim 18, wherein the access point allows the WTRU to transfer the data to the external network if the WTRU can authenticate itself and refuses the transfer of the data to the external network if the WTRU cannot authenticate itself.

20. The method of claim 19, wherein the WTRU attempting to transfer the data to the external network extracts an identification code from the memory of the WTRU and transmits the identification code along with the data.

21. The method of claim 20, wherein the access point compares the identification code transmitted by the WTRU to codes stored in a memory of the access point to determine if the WTRU has authenticated.

22. In a wireless communication system comprising a plurality of wireless transmit/receive units (WTRUs), an access point, and an external network, the access point comprising:

a transmitter;

a receiver; and

a processor in communication with the transmitter and the receiver, wherein an application for preventing the unauthorized transfer of data from the WTRUs to the external network in the wireless communication system runs on

the processor, the receiver receives an attempt from one of the WTRUs attempting to transfer data to the external network, the processor examines the data to determine if the transfer of data is authorized, and the processor transfers the data to the external network if the transfer is authorized.

23. The access point of claim 22, further comprising a memory in communication with the processor.

24. The access point of claim 22, further comprising an antenna in communication with the transmitter and receiver.

25. In a wireless communication system comprising a plurality of wireless transmit/receive units (WTRUs), an access point, and an external network, the access point including an integrated circuit (IC) comprising:

a transmitter;

a receiver; and

a processor in communication with the transmitter and the receiver, wherein an application for preventing the unauthorized transfer of data from the WTRUs to the external network in the wireless communication system runs on the processor, the receiver receives an attempt from one of the WTRUs attempting to transfer data to the external network, the processor examines the data to determine if the transfer of data is authorized, and the processor transfers the data to the external network if the transfer is authorized.

26. The IC of claim 25, further comprising a memory in communication with the processor.

27. The IC of claim 19, further comprising an antenna in communication with the transmitter and the receiver.

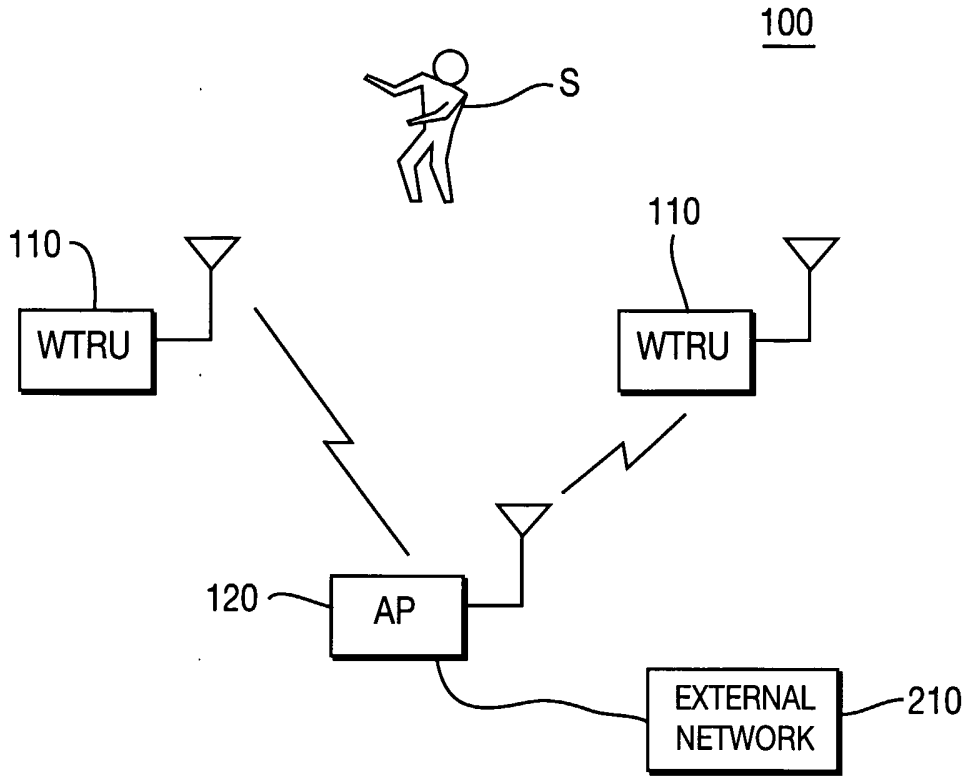

100
S
110
WTRU
110
WTRU
120
AP
EXTERNAL NETWORK
210

FIG. 1

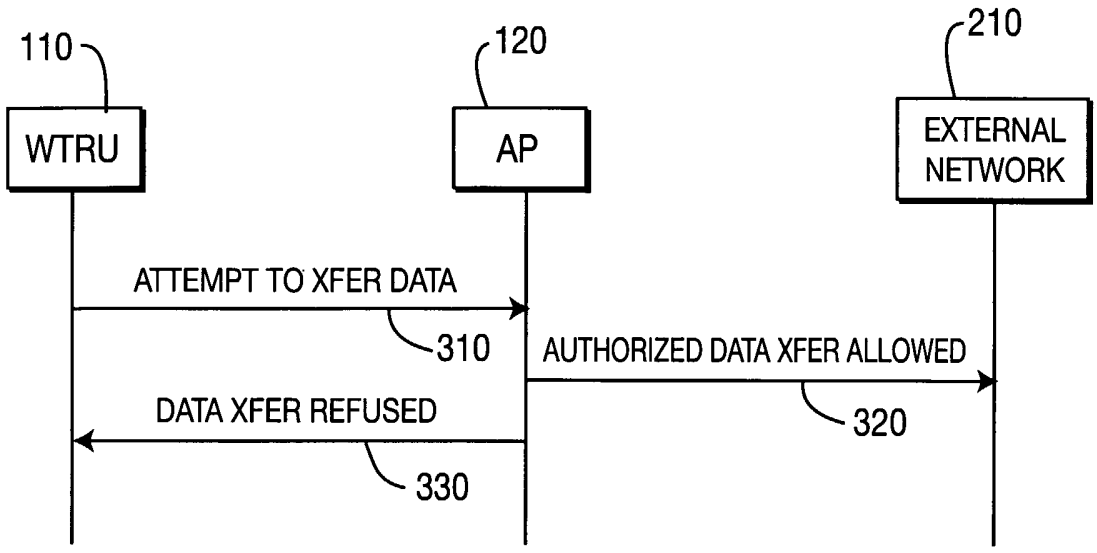

110
WTRU
120
AP
210
EXTERNAL NETWORK
ATTEMPT TO XFER DATA
310
AUTHORIZED DATA XFER ALLOWED
320
DATA XFER REFUSED
330

FIG. 3

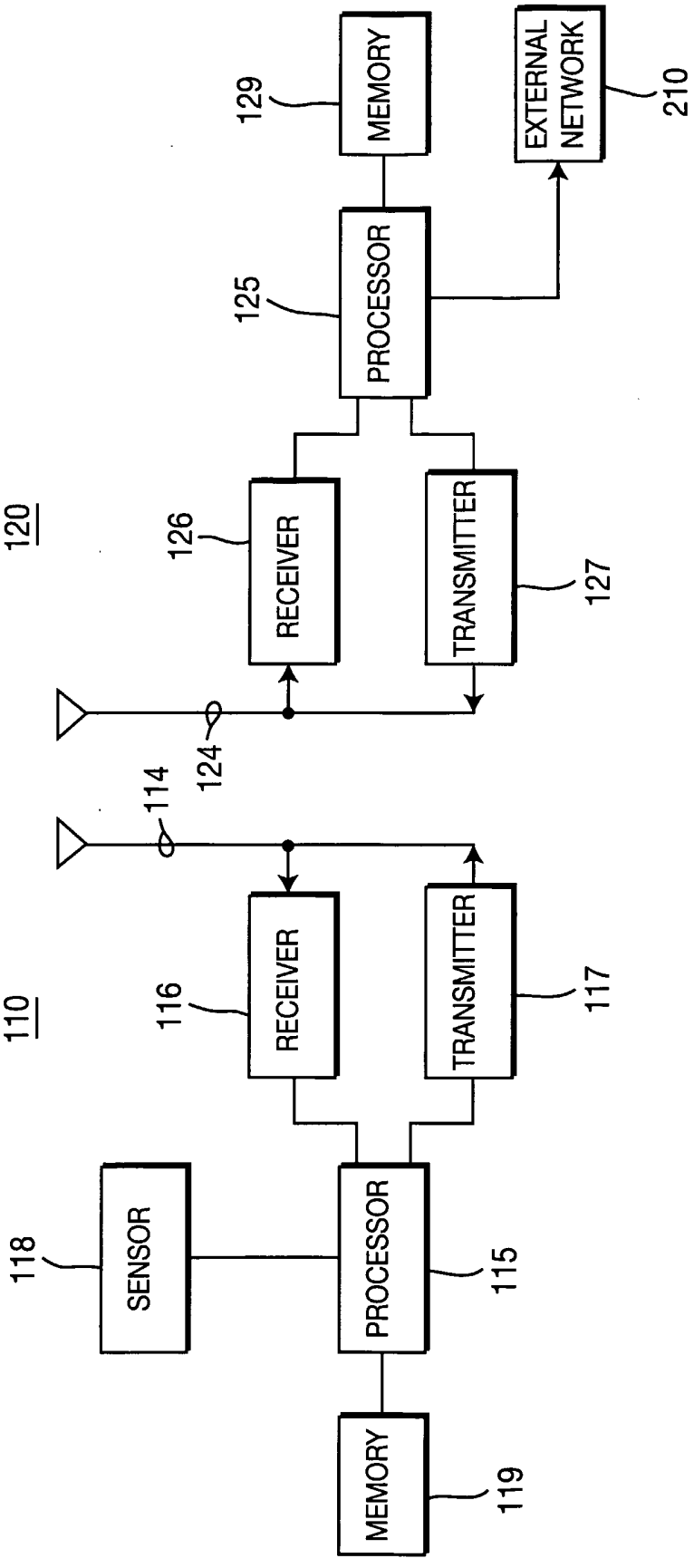

MEMORY
129
EXTERNAL NETWORK
210
PROCESSOR
125
120
RECEIVER
126
TRANSMITTER
127
124
114
110
RECEIVER
116
TRANSMITTER
117
SENSOR
118
PROCESSOR
115
MEMORY
119

FIG. 2

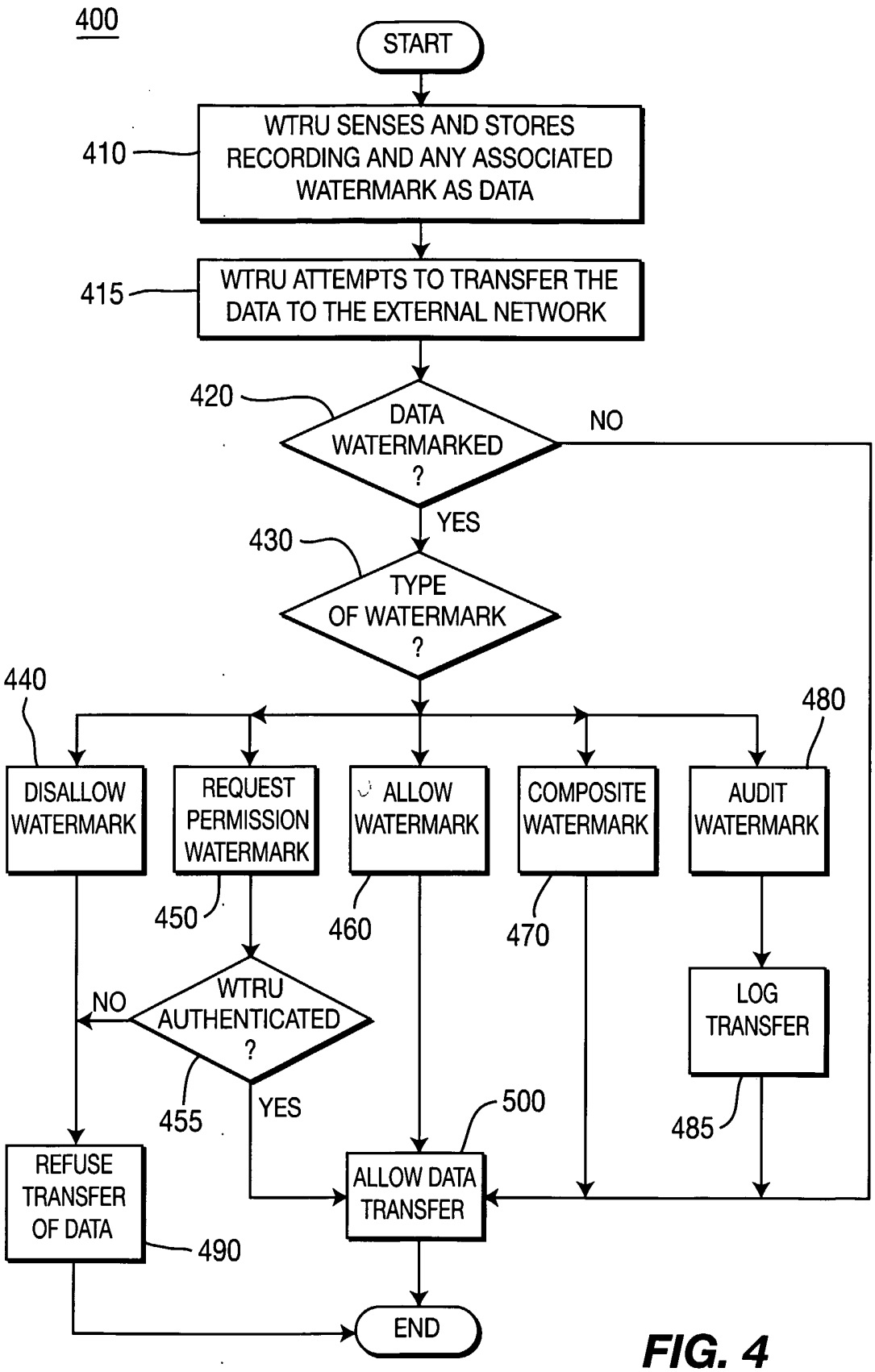

400
START
WTRU SENSES AND STORES RECORDING AND ANY ASSOCIATED WATERMARK AS DATA
410
WTRU ATTEMPTS TO TRANSFER THE DATA TO THE EXTERNAL NETWORK
415
420
DATA WATERMARKED ?
NO
YES
430
TYPE OF WATERMARK ?
440
480
DISALLOW WATERMARK
REQUEST PERMISSION WATERMARK
ALLOW WATERMARK
COMPOSITE WATERMARK
AUDIT WATERMARK
450
460
470
NO
WTRU AUTHENTICATED ?
LOG TRANSFER
455
YES
500
485
REFUSE TRANSFER OF DATA
ALLOW DATA TRANSFER
490
END

FIG. 4