Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2413881 C 2012/04/17

(11)(21) 2 413 881

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(22) Date de dépôt/Filing Date: 2002/12/11
(41) Mise à la disp. pub./Open to Public Insp.: 2003/07/02
(45) Date de délivrance/Issue Date: 2012/04/17
(30) Priorités/Priorities: 2002/01/02 (US10/038,217); 2002/01/02 (US10/038,032); 2002/01/02 (US10/037,914); 2002/01/02 (US10/037,499); 2002/01/02 (US10/037,498); 2002/02/08 (US60/355,326); 2002/04/16 (US60/372,901); 2002/10/18 (US10/273,903)

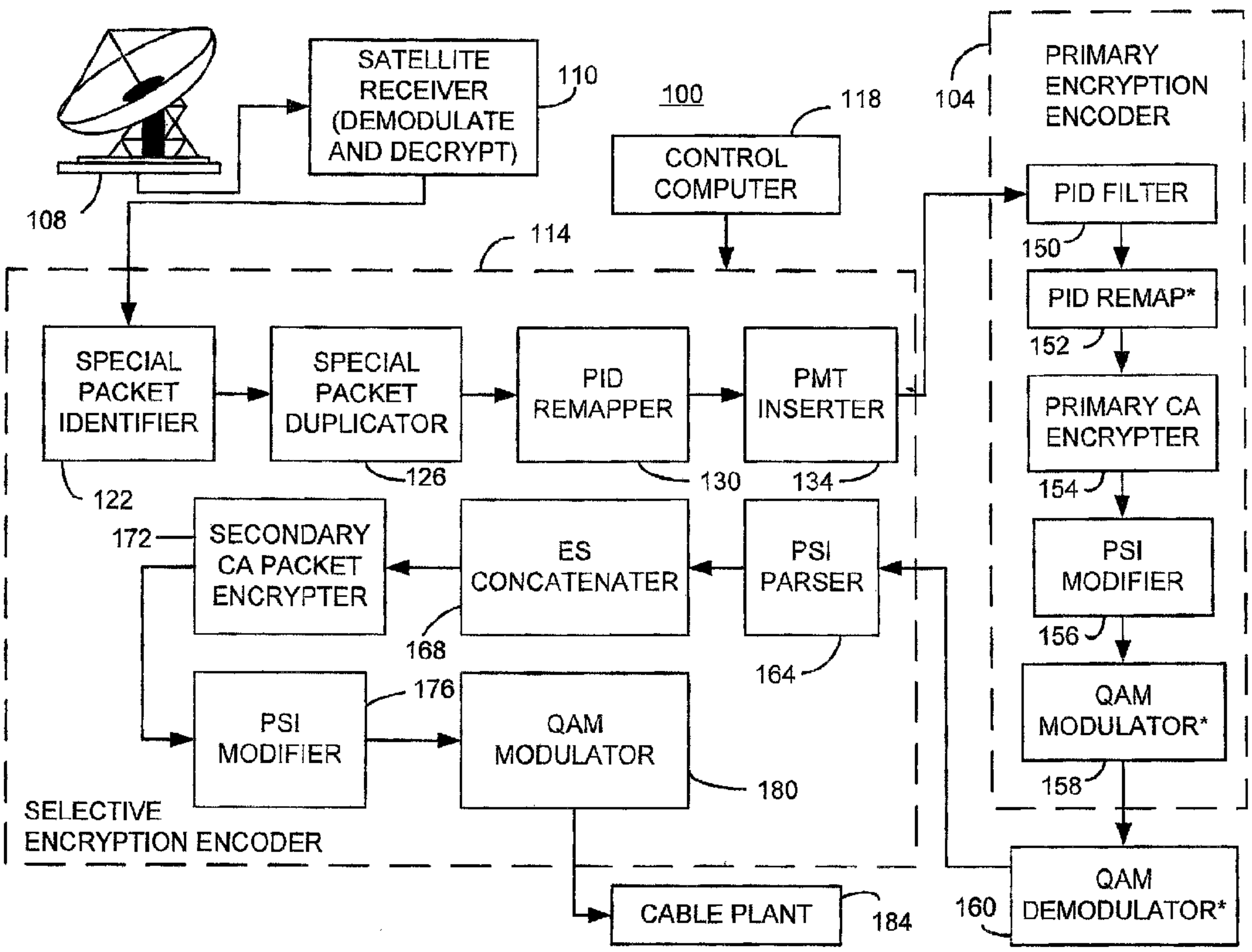
(51) Cl.Int./Int.Cl. *H04L 9/28* (2006.01), *H04L 12/56* (2006.01)

(72) Inventeurs/Inventors:
CANDELORE, BRANT L., US;
DEROVANESSIAN, HENRY, US;
PEDLOW, LEO M., JR., US

(73) Propriétaire/Owner:
SONY ELECTRONICS INC., US

(74) Agent: GOWLING LAFLEUR HENDERSON LLP

(54) Titre : CRYPTAGE PARTIEL DE MODELE DE DONNEES EN ETOILE
(54) Title: STAR PATTERN PARTIAL ENCRYPTION



(57) Abrégé/Abstract:
A selective encryption encoder consistent with certain embodiments of the invention has a packet identifier that identifies packets of a specified packet type, the specified packet type being defined by packets occurring in a star pattern approximately situated at an upper center of an image which contain intra- coded macroblocks. A packet duplicator duplicates the identified packets to produce first and second sets of the identified packets. The packets are sent to and from a primary encryption encoder to encrypt the first set of identified packets under a first encryption method. A secondary encrypter encrypts the second set of identified packets under a second encryption method.

ABSTRACT OF THE DISCLOSURE

A selective encryption encoder consistent with certain embodiments of the invention has a packet identifier that identifies packets of a specified packet type, the specified packet type being defined by packets occurring in a star pattern approximately situated at an upper center of an image which contain intra-coded macroblocks. A packet duplicator duplicates the identified packets to produce first and second sets of the identified packets. The packets are sent to and from a primary encryption encoder to encrypt the first set of identified packets under a first encryption method. A secondary encrypter encrypts the second set of identified packets under a second encryption method.

STAR PATTERN PARTIAL ENCRYPTION

CROSS REFERENCE TO RELATED DOCUMENTS

This application is a continuation in part of patent docket number SNY-R4646.01 entitled "Critical Packet Partial Encryption" to Unger et al., U.S. patent number 7,336,787; patent docket number SNY-R4646.02 entitled "Time Division Partial Encryption" to Candelore et al., U.S. patent number 7,139,398; docket number SNY-R4646.03 entitled "Elementary Stream Partial Encryption" to Candelore , U.S. patent number 7,124,303; docket number SNY-R4646.04 entitled "Partial Encryption and PID Mapping" to Unger et al., U.S. patent number 7,151,831; and docket number SNY-R4646.05 entitled "Decoding and Decrypting of Partially Encrypted Information" to Unger et al., U.S. patent number 7,127,619. These related patents will be hereinafter referred to as “patent documents”.

FIELD OF THE INVENTION

This invention relates generally to the field of encryption. More particularly, this invention relates to a dual encryption method and apparatus particularly useful for scrambling packetized video content such as that provided by cable and satellite television systems.

BACKGROUND OF THE INVENTION

The above-referenced commonly owned patent documents describe inventions relating to various aspects of methods generally referred to herein as partial encryption or selective encryption. More particularly, systems are described therein wherein selected portions of a particular selection of digital content are encrypted using two (or more) encryption techniques while other portions of the content are left unencrypted. By properly selecting the portions to be encrypted, the content can effectively be encrypted for use under multiple decryption systems without the necessity of encryption of the entire selection of content. In some embodiments, only a few percent of data overhead is needed to effectively encrypt the content using multiple encryption systems. This results in a cable or satellite system being able to utilize Set-top boxes or other implementations of conditional access (CA) receivers from multiple manufacturers in a single system - thus freeing the cable or satellite company to competitively shop for providers of Set-top boxes.

BRIEF DESCRIPTION OF THE DRAWINGS

The features of the invention believed to be novel are set forth with particularity in the appended claims. The invention itself however, both as to organization and method of operation, together with objects and advantages thereof, may be best understood by reference to the following detailed description of the invention, which describes certain exemplary embodiments of the invention, taken in conjunction with the accompanying drawings in which:

FIGURE 1 is a block diagram of an exemplary cable system head end consistent with certain embodiments of the present invention.

FIGURE 2 is an illustration of sample transport stream PSI consistent with certain embodiments of the present invention.

FIGURE 3 is a further illustration of sample transport stream PSI consistent with certain embodiments of the present invention.

FIGURE 4 is a block diagram of an illustrative control processor 100 consistent with certain embodiments of the present invention.

FIGURE 5 illustrates the slice structure of a frame of video data consistent with certain embodiments of the present invention.

FIGURE 6 illustrates a star pattern of encrypted packets consistent with certain embodiments of the present invention.

FIGURE 7 illustrates a television Set-top box that decrypts and decodes in a manner consistent with certain embodiments of the present invention.

FIGURE 8 is a flow chart broadly illustrating an encryption process consistent with embodiments of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

While this invention is susceptible of embodiment in many different forms, there is shown in the drawings and will herein be described in detail specific embodiments, with the understanding that the present disclosure is to be considered as an example of the principles of the invention and not intended to limit the invention to the specific embodiments shown and described. In the description below, like reference numerals are used to describe the same, similar or corresponding parts in the several views of the drawings.

The terms “scramble” and “encrypt” and variations thereof are used synonymously herein. Also, the term “television program” and similar terms can be interpreted in the normal conversational sense, as well as a meaning wherein the term means any segment of A/V content that can be displayed on a television set or similar monitor device. The term “video” is often used herein to embrace not only true visual information, but also in the conversational sense (e.g., “video tape recorder”) to embrace not only video signals but associated audio and data. The term “legacy” as used herein refers to existing technology used for existing cable and satellite systems. The exemplary embodiments disclosed herein are decoded by a television Set-Top Box (STB), but it is contemplated that such technology will soon be incorporated within television receivers of all types whether housed in a separate enclosure alone or in conjunction with recording and/or playback equipment or Conditional Access (CA) decryption module or within a television set itself. The present document generally uses the example of a “dual partial encryption” embodiment, but those skilled in the art will recognize that the present invention can be utilized to realize multiple partial encryption without departing from the invention. Partial encryption and selective encryption are used synonymously herein.

Turning now to **FIGURE 1**, a head end 100 of a cable television system suitable for use in practicing a dual encryption embodiment of the present invention is illustrated. Those skilled in the art will appreciate that the present invention could also be implemented using more than two encryptions systems without departing from the present invention. The illustrated head end 100 implements the dual partial encryption scenario of the present invention by adapting the operation of a conventional encryption encoder 104 (such as those provided by Motorola, Inc. and Scientific-Atlanta, Inc., and referred to herein as the primary encryption encoder) with additional equipment.

Head end 100 receives scrambled content from one or more suppliers, for example, using a satellite dish antenna 108 that feeds a satellite receiver 110. Satellite receiver 110 operates to demodulate and descramble the incoming content and supplies the content as a stream of clear (unencrypted) data to a selective encryption encoder 114. The selective encryption encoder 114, according to certain embodiments, uses two passes or two stages of operation, to encode the stream of data. Encoder 114 utilizes a secondary conditional access system (and thus a second encryption method) in conjunction with the primary encryption encoder 104 which operates using a primary conditional access system (and thus a primary encryption method). A user selection provided via a user interface on a control computer 118 configures the selective encryption encoder 114 to operate in conjunction with either a Motorola or Scientific Atlanta cable network (or other cable or satellite network).

It is assumed, for purposes of the present embodiment of the invention, that the data from satellite receiver 110 is supplied as MPEG (Moving Pictures Expert Group) compliant packetized data. In the first stage of operation the data is passed through a Special Packet Identifier (PID) 122. Special Packet Identifier 122 identifies specific programming that is to be dual partially encrypted according to the present invention. The Special Packet Identifier 122 signals the Special Packet Duplicator 126 to duplicate special packets. The Packet Identifier (PID) Remapper 130, under control of the computer 118, to remap the PIDs of the elementary streams (ES) (i.e., audio, video, etc.) of the programming that shall remain clear and the duplicated packets to new PID values. The payload of the elementary stream packets are not altered in any way by Special Packet Identifier 122, Special Packet Duplicator 126, or PID remapper 1306. This is done so that the primary encryption encoder 104 will not recognize the clear unencrypted content as content that is to be encrypted.

The packets may be selected by the special packet identifier 122 according to one of the selection criteria described in the above-referenced applications or may use another selection criteria such as those which will be described later herein. Once these packets are identified in the packet identifier 122, packet duplicator 126 creates two copies of the packet. The first copy is identified with the original PID so that the primary encryption encoder 104 will recognize that it is to be encrypted. The second copy is identified with a new and unused PID, called a "secondary PID" (or shadow PID) by the PID Remapper 122. This secondary PID will be used later by the selective encryption encoder 114 to determine which packets are to be encrypted according to the secondary encryption method. **FIGURE 2** illustrates an exemplary set of transport PSI tables 136 after this remapping with a PAT 138 defining two programs (10 and 20) with respective PID values 0100 and 0200. A first PMT 140 defines a PID=0101 for the video elementary stream and PIDs 0102 and 0103 for two audio streams for program 10. Similarly, a second PMT 142 defines a PID=0201 for the video elementary stream and PIDs 0202 and 0203 for two audio streams for program 20.

As previously noted, the two primary commercial providers of cable head end encryption and modulation equipment are (at this writing) Motorola, Inc. and Scientific-Atlanta, Inc. While similar in operation, there are significant differences that should be discussed before proceeding since the present selective encryption encoder 114 is desirably compatible with either system. In the case of Motorola equipment, the Integrated Receiver Transcoder (IRT), an unmodulated output is available and therefore there is no need to demodulate the output before returning a signal to the selective encryption encoder 114, whereas no such unmodulated output is available in a Scientific-Atlanta device. Also, in the case of current Scientific-Atlanta equipment, the QAM, the primary encryption encoder carries out a PID remapping function on received packets. Thus, provisions are made in the selective encryption encoder 114 to address this remapping.

In addition to the above processing, the Program Specific Information (PSI) is also modified to reflect this processing. The original, incoming Program Association Table (PAT) is appended with additional Program Map Table (PMT) entries at a PMT inserter 134. Each added PMT entry contains the new, additional streams (remapped & shadow PIDs) created as part of the selective encryption

(SE) encoding process for a corresponding stream in a PMT of the incoming transport. These new PMT entries will mirror their corresponding original PMTs. The program numbers will be automatically assigned by the selective encryption encoder 114 based upon open, available program numbers as observed from the program number usage in the incoming stream. The selective encryption System 114 system displays the inserted program information (program numbers, etc) on the configuration user interface of control computer 118 so that the Multiple System Operator (MSO, e.g., the cable system operator) can add these extra programs into the System Information (SI) control system and instruct the system to carry these programs in the clear.

The modified transport PSI is illustrated as 144 in **FIGURE 3** with two additional temporary PMTs 146 and 148 appended to the tables of transport PSI 136. The appended PMTs 146 and 148 are temporary. They are used for the primary encryption process and are removed in the second pass of processing by the secondary encryption encoder. In accordance with the MPEG standard, all entries in the temporary PMTs are marked with stream type "user private" with an identifier of 0xF0. These PMTs describe the remapping of the PIDs for use in later recovery of the original mapping of the PIDs in the case of a PID remapping in the Scientific-Atlanta equipment. Of course, other identifiers could be used without departing from the present invention.

In order to assure that the Scientific-Atlanta PID remapping issue is addressed, if the selective encryption encoder 114 is configured to operate with a Scientific-Atlanta system, the encoder adds a user private data descriptor to each elementary stream found in the original PMTs in the incoming data transport stream (TS) per the format below (of course, other formats may also be suitable):

Syntax	value	# of bits
private_data_indicator_descriptor() {		
descriptor_tag	0xF0	8
descriptor_length	0x04	8
private_data_indicator() {		
orig_pid	0x????	16
stream_type	0x??	8
reserved	0xFF	8
}		
}		

The selective encryption encoder 114 of the current embodiment also adds a user private data descriptor to each elementary stream placed in the temporary PMTs created as described above per the format below:

Syntax	value	# of bits
private_data_indicator_descriptor() {		
descriptor_tag	0xF0	8
descriptor_length	0x04	8
private_data_indicator() {		
orig_pid	0x????	16
stream_type	0x??	8
reserved	0xFF	8
}		
}		

The "???" in the tables above is the value of the "orig_pid" which is a variable while the "??" is a "stream_type" value. The data field for "orig_pid" is a variable that contains the original incoming PID or in the case of remap or shadow PIDs, the original PID that this stream was associated with. The data field "stream_type" is a variable that describes the purpose of the stream based upon the chart below:

Stream Type	Value
Legacy ES	0x00
Remapped ES	0x01
Shadow ES	0x02
Reserved	0x03 – 0xFF

These descriptors will be used later to re-associate the legacy elementary streams, which are encrypted by the Scientific-Atlanta, Inc. primary encryption encoder 104, with the corresponding shadow and remapped clear streams after PID remapping in the Scientific-Atlanta, Inc. modulator prior to the second phase of processing of the Selective Encryption Encoder. Those skilled in the art will appreciate that the above specific values should be considered exemplary and other specific values could be used without departing from the present invention.

In the case of a Motorola cable system being selected in the selective encryption encoder configuration GUI, the original PAT and PMTs can remain unmodified, providing the system does not remap PIDs within the primary encryption encoder. The asterisks in **FIGURE 1** indicate functional blocks that are not used in a Motorola cable system.

The data stream from selective encryption encoder 114 is passed along to the input of the primary encryption encoder 104 which first carries out a PID filtering process at 150 to identify packets that are to be encrypted. At 152, in the case of a Scientific-Atlanta device, a PID remapping may be carried out. The data are then passed along to an encrypter 154 that, based upon the PID of the packets encrypts certain packets (in accord with the present invention, these packets are the special packets which are mapped by the packet duplicator 130 to the original PID of the incoming data stream for the current program). The remaining packets are unencrypted. The data then passes through a PSI modifier 156 that modifies the PSI data to reflect changes made at the PID remapper. The data stream is then modulated by a quadrature amplitude modulation (QAM) modulator 158 (in the case of the Scientific-Atlanta device) and passed to the output thereof. This modulated signal is then demodulated by a QAM demodulator 160. The output of the demodulator 160 is directed back to the selective encryption encoder 114 to a PSI parser164.

The second phase of processing of the transport stream for selective encryption is to recover the stream after the legacy encryption process is carried out in the primary encryption encoder 104. The incoming Program Specific Information (PSI) is parsed at 164 to determine the PIDs of the individual elementary streams and their function for each program, based upon the descriptors attached in the first phase of processing. This allows for the possibility of PID remapping, as seen in Scientific-Atlanta primary encryption encoders. The elementary streams described in the original program PMTs are located at PSI parser 164 where these streams have been reduced to just the selected packets of interest and encrypted in the legacy CA system format in accord with the primary encryption method at encoder 104. The elementary streams in the temporary programs appended to the original PSI are also recovered at elementary stream concatenator 168. The packets in the legacy streams are appended to the remapped content, which is again remapped back to the PID of the legacy streams, completing the partial, selective encryption of the original elementary streams.

The temporary PMTs and the associated PAT entries are discarded and removed from the PSI. The user private data descriptors added in the first phase of processing are also removed from the remaining original program PMTs in the PSI. For a Motorola system, no PMT or PAT reprocessing is required and only the final secondary encryption of the transport stream occurs.

During the second phase of processing, the SE encoder 114 creates a shadow PSI structure that parallels the original MPEG PSI, for example, having at PAT origin at PID 0x0000. The shadow PAT will be located at a PID specified in the SE encoder configuration as indicated by the MSO from the user interface. The shadow PMT PIDs will be automatically assigned by the SE encoder 114 dynamically, based upon open, available PID locations as observed from PID usage of the incoming stream. The PMTs are duplicates of the original PMTs, but also have CA descriptors added to the entire PMT or to the elementary streams referenced within to indicate the standard CA parameters and optionally, shadow PID and the intended operation upon the associated elementary stream. The CA descriptor can appear in the descriptor1() or descriptor2() loops of the shadow PMT. If found in descriptor1(), the CA_PID called out in the CA descriptor contains the non-legacy ECM PID which would apply to an entire program. Alternatively, the ECM PID may be sent in descriptor2(). The CA descriptor should not reference the selective encryption elementary PID in the descriptor1() area.

CA_PID Definition	Secondary_CA_private_data Value
ECM PID	0x00
Replacement PID	0x01
Insertion PID	0x02
ECM PID	undefined (default)

This shadow PSI insertion occurs regardless of whether the selective encryption operation is for a Motorola or Scientific Atlanta cable network. The elementary streams containing the duplicated packets of interest that were also assigned to the temporary PMTs are encrypted during this second phase of operation at secondary packet encrypter in the secondary CA format based upon the configuration data of the CA system attached using the DVB (Digital Video Broadcasting) Simulcrypt™ standard.

The data stream including the clear data, primary encrypted data, secondary encrypted data and other information are then passed to a PSI modifier 176 that modifies the transport PSI information by deletion of the temporary PMT tables and incorporation of remapping as described above. The output of the PSI modifier 176 is modulated at a QAM modulator 180 and delivered to the cable plant 184 for distribution to the cable system's customers.

The control processor 100 may be a personal computer based device that is used to control the selective encryption encoder as described herein. An exemplary personal computer based controller 100 is depicted in **FIGURE 4**. Control processor 100 has a central processor unit (CPU) 210 with an associated bus 214 used to connect the central processor unit 210 to Random Access Memory 218 and Non-Volatile Memory 222 in a known manner. An output mechanism at 226, such as a display and possibly printer, is provided in order to display and/or print output for the computer user as well as to provide a user interface such as a Graphical User Interface (GUI). Similarly, input devices such as keyboard and mouse 230 may be provided for the input of information by the user at the MSO. Computer 100 also may have disc storage 234 for storing large amounts of information including, but not limited to, program files and data files. Computer system 100 also has an interface 238 for connection to the selective encryption encoder 114. Disc storage 234 can store any number of encryption methods that can be downloaded as desired by the MSO to vary the encryption on a regular basis to thwart hackers. Moreover, the encryption methods can be varied according to other criteria such as availability of bandwidth and required level of security.

The partial encryption process described above utilizes any suitable conditional access encryption method at encrypters 154 and 174. However, these encryption techniques are selectively applied to the data stream using a technique such as those described below or in the above-referenced patent applications. In general, but without the intent to be limiting, the selective encryption process utilizes intelligent selection of information to encrypt so that the entire program does not have to undergo dual encryption. By appropriate selection of appropriate data to encrypt, the program material can be effectively scrambled and hidden from those who desire to hack into the system and illegally recover commercial content without paying. The MPEG (or similar format) data that are used to represent the audio and video data does so using a high degree of reliance on the redundancy of information from frame to frame. Certain data can be transmitted as "anchor" data representing chrominance and luminance data. That data is then often simply moved about the screen to generate subsequent frames by sending motion vectors that describe the movement of the block. Changes in the chrominance and luminance data are also encoded as changes rather than a recoding of absolute anchor data.

The MPEG specification defines a slice as "... a series of an arbitrary number of consecutive macroblocks. The first and last macroblocks of a slice shall not be skipped macroblocks. Every slice shall contain at least one macroblock. Slices shall not overlap. The position of slices may change from picture to picture. The first and last macroblock of a slice shall be in the same horizontal row of macroblocks. Slices shall occur in the bitstream in the order in which they are encountered, starting at the upper-left of the picture and proceeding by raster-scan order from left to right and top to bottom...."

By way of example, to represent an entire frame of NTSC information, the frame (picture) is divided into 30 slices (but in general j slices may make up a full frame). Each slice contains 33 variable length macroblocks (but in general can include k variable length macroblocks) of information representing a 16x16 pixel region of the image. This is illustrated as frame 250 of **FIGURE 5** with each slice starting with a slice header (SH1-SH30) and each slice having 33 macroblocks (MB1-MB33). By appropriate selection of particular data representing the frame, the image can be scrambled beyond recognition in a number of ways as will be described below. By variation of the selection criteria for selective encryption, hackers can be thwarted on a continuing basis. Moreover, the selection criteria can be changed to adapt to bandwidth requirements as well as need for security of particular content (or other criteria).

It is noted that the portion of the picture that generally carries information of most interest to the viewer is approximately the center of the image. A suitable tradeoff between bandwidth and encryption security consistent with embodiments of the present invention involves encryption of selected portions of the image which can be deemed the "active region" of the image. This region is somewhat difficult to define and is somewhat content dependent. But, generally speaking it is approximately an upper central area of the frame. According to one embodiment consistent with the present invention, macroblocks in this active region are encrypted while macroblocks extending somewhat radially from this central region are encrypted with less frequency.

FIGURE 6 illustrates an embodiment of the invention in which slices in a central area of the frame 270 are encrypted with a star pattern 274 extending outward radially from the upper center of the frame. In this embodiment, macroblocks having intracoded data are encrypted if they fall within the shaded area of the star pattern 274. In one embodiment consistent with the present invention, intracoded macroblocks are encrypted if, for standard definition, they fall within the definition of the star pattern 274 given in the table below:

SLICE	ENCRYPTED INTRA-CODED MACROBLOCKS
1-6	14-21
7-12	11-23
13-18	1-33
19-21	11-23
22-30	14-21

For an interlaced high definition video image, the video frame is made up of 68 slices each carrying 120 macroblocks. For such an image, the table below is one embodiment of how a star pattern can be realized:

SLICE	ENCRYPTED INTRA-CODED MACROBLOCKS
1-12	50-77
13-27	40-84
28-41	1-120
42-48	40-84
49-60	50-77

For a progressive high definition video image, the video frame is made up of 45 slices each carrying 80 macroblocks. For such an image, the table below is one embodiment of how a star pattern can be realized:

SLICE	ENCRYPTED INTRA-CODED MACROBLOCKS
1-9	34-51
10-18	26-56
19-27	1-80
28-31	26-56
32-45	34-51

Similar star patterns can be devised for any other video frame definition without departing from the invention. Moreover, variations of star patterns in which varying numbers of rays extend in various directions from a central or upper central area of the frame at various angles can be devised without departing from the invention.

As defined above, star pattern 274 is slightly asymmetrical with a weighting of the central area of the star being situated approximately one slice above center. Star pattern 274 has rays or points of the star extending vertically and horizontally across the entire frame. The star pattern 274 further has rays defined by the corners of the central region that extend diagonally outward from the center.

Those skilled in the art will understand that the above definition of the star pattern 274 is but one such definition within the scope of the invention. The number of intracoded macroblocks per slice or number of slices in a particular section of the star can be varied without departing from the present invention. Moreover, other star-like patterns can be used in place of the squared off pattern 274 depicted in **FIGURE 6**, or the star pattern can be shifted within the image without departing from the invention. Such variations are considered equivalent and within the scope of the present invention so long as a central or active region of the image is encrypted with lower levels of encryption radiating outward from the active region.

Thus, in accordance with one embodiment consistent with the present invention, an packet containing an intra-coded macroblock in a star pattern such as that defined in the above table will be encrypted while the remaining packets will either be selectively encrypted according to another criterion, or transmitted in the clear. Depending upon the actual definition of the active region, the overhead required for dual encryption of a star pattern will vary. In other embodiments, all macroblocks within this star pattern can be encrypted.

In preferred embodiments, intra-coded macroblocks (or packets containing such macroblocks) are encrypted rather than all macroblocks within the star pattern, but this is not to be considered limiting. Intra-coded macroblocks contain anchor data such as absolute chrominance and/or luminance data used by inter-coded macroblocks to derive an image. By encryption of these intra-coded macroblocks, the inter-coded macroblocks are robbed of their point of reference and the image is substantially disrupted.

In this encryption technique, the active portion of the screen is deemed to be the area of most interest to the viewer. Although some intelligible video information may be present outside the star pattern, the encrypted star pattern is likely to produce a major annoyance to an unauthorized viewer. Moreover, the packetizing of the star pattern will likely result in additional data being encrypted. By encrypting the intra-coded blocks, inter-coded data will be deprived of a reference and thus produce the desired scrambling effect. This technique can be used alone or with other selective encryption techniques to produce low overhead encryption. Additionally, the present invention is suitable not only for multiple encryption scenarios, but also for single encryption of a video signal. In accordance with certain embodiments of the present invention, any technique that detects macroblocks containing intra-coded data within the star pattern can be used as a selection criterion for selecting data or data packets for encryption.

Multiple combinations of the encryption techniques are possible to produce encryption that has varying bandwidth requirements, varying levels of security and varying complexity. For example, the above star pattern could be encrypted along with packets containing slice headers, or the above star pattern could be encrypted along with packets containing slice headers and the first macroblock following each slice header.

Numerous other combinations of the above encryption techniques as well as those described in the above-referenced patent applications and other partial encryption techniques can be combined to produce a rich pallette of encryption techniques from which to select. In accordance with certain embodiments of the present invention, a selection of packets to encrypt can be made by the control computer 118 in order to balance encryption security with bandwidth and in order to shift the encryption technique from time to time to thwart hackers.

An authorized set-top box such as 300 illustrated in **FIGURE 7** operating under the secondary CA system decrypts and decodes the incoming program by recognizing both primary and secondary PIDs associated with a single program. The multiplexed video data stream containing both PIDs is directed to a demultiplexer 304. When a program is received that contains encrypted content that was encrypted by any of the above techniques, the demultiplexer directs encrypted packets containing encrypted content and secondary PIDS to a secondary CA decrypter 308. These packets are then decrypted at 308 and passed to a PID remapper 312. As illustrated, the PID remapper 312 receives packets that are unencrypted and bear the primary PID as well as the decrypted packets having the secondary PID. The PID remapper 312 combines the decrypted packets from decrypter 308 with the unencrypted packets having the primary PID to produce an unencrypted data stream representing the desired program. PID remapping is used to change either the primary or secondary PID or both to a single PID. This unencrypted data stream can then be decoded normally by decoder 316. Some or all of the components depicted in **FIGURE 7** can be implemented as program code running on a programmed processor running code stored on an electronic storage medium.

FIGURE 8 is a flow chart 400 that broadly illustrates the encryption process consistent with certain embodiments of the present invention starting at 404. At 408 the packet type that is to be encrypted is specified. In accordance with certain embodiments consistent with the present invention, the selected packet type may be packets representing a star pattern in the video frame. Packets are then examined at 412 to identify packets of the specified type. At 416, the identified packets are duplicated and at 420 one set of these packets is encrypted under a first encryption method. The other set of identified packets is encrypted at 424 under a second encryption method. The originally identified packets are then replaced in the data stream with the two sets of encrypted packets at 430 and the process ends at 436.

While the above embodiments describe encryption of packets containing the selected data type, it is also possible to encrypt the raw data prior to packetizing without departing from this invention and such encryption is considered equivalent thereto.

Those skilled in the art will recognize that the present invention has been described in terms of exemplary embodiments based upon use of a programmed processor (e.g., processor 118, processors implementing any or all of the elements of 114 or implementing any or all of the elements of 300). However, the invention should not be so limited, since the present invention could be implemented using hardware component equivalents such as special purpose hardware and/or dedicated processors which are equivalents to the invention as described and claimed. Similarly, general purpose computers, microprocessor based computers, micro-controllers, optical computers, analog computers, dedicated processors and/or dedicated hard wired logic may be used to construct alternative equivalent embodiments of the present invention.

Those skilled in the art will appreciate that the program steps and associated data used to implement the embodiments described above can be implemented using disc storage as well as other forms of storage such as for example Read Only Memory (ROM) devices, Random Access Memory (RAM) devices; optical storage elements, magnetic storage elements, magneto-optical storage elements, flash memory, core memory and/or other equivalent storage technologies without departing from the present invention. Such alternative storage devices should be considered equivalents.

The present invention, as described in embodiments herein, is implemented using a programmed processor executing programming instructions that are broadly described above form that can be stored on any suitable electronic storage medium or transmitted over any suitable electronic communication medium or otherwise be present in any computer readable or propagation medium. However, those skilled in the art will appreciate that the processes described above can be implemented in any number of variations and in many suitable programming languages without departing from the present invention. For example, the order of certain operations carried out can often be varied, additional operations can be added or operations can be deleted without departing from the invention. Error trapping can be added and/or enhanced and variations can be made in user interface and information presentation without departing from the present invention. Such variations are contemplated and considered equivalent.

Software code and/or data embodying certain aspects of the present invention may be present in any computer readable medium, transmission medium, storage medium or propagation medium including, but not limited to, electronic storage devices such as those described above, as well as carrier waves, electronic signals, data structures (e.g., trees, linked lists, tables, packets, frames, etc.) optical signals, propagated signals, broadcast signals, transmission media (e.g., circuit connection, cable, twisted pair, fiber optic cables, waveguides, antennas, etc.) and other media that stores, carries or passes the code and/or data. Such media may either store the software code and/or data or serve to transport the code and/or data from one location to another. In the present exemplary embodiments, MPEG compliant packets, slices, tables and other data structures are used, but this should not be considered limiting since other data structures can similarly be used without departing from the present invention.

While the invention has been described in conjunction with specific embodiments, it is evident that many alternatives, modifications, permutations and variations will become apparent to those skilled in the art in light of the foregoing description. Accordingly, it is intended that the present invention embrace all such alternatives, modifications and variations as fall within the scope of the appended claims.

What is claimed is:

1. A selective encryption decoder, for decrypting and decoding a selectively encrypted digital video signal, comprising:

a demultiplexer that receives packets of digital video, certain of the packets being unencrypted and certain of the packets being encrypted, wherein certain of the encrypted packets carry data arranged in a star pattern within a video frame;

the unencrypted packets having a first packet identifier (PID) and the encrypted packets having a second packet identifier (PID);

a decrypter receiving the encrypted packets having the second PID and decrypting the encrypted packets using a first encryption method to produce decrypted packets;

a PID remapper that changes at least one of the first and second PIDs so that the unencrypted packets and the decrypted packets have the same PID; and

a decoder that decodes the unencrypted and decrypted packets to produce a decoded video signal.

2. The selective encryption decoder according to claim 1, wherein wherein the specified packet type further comprises packets containing an intra-coded macroblock within the star pattern.

3. The selective encryption decoder according to claim 1, wherein a video frame comprises 30 slices each having 33 macroblocks, and wherein the star pattern is defined by: macroblocks 14-21 in slices 1-6 and 22-30, macroblocks 11-23 of slices 7-12 and 19-21 and macroblocks 1-33 of slices 13-18.

4. The selective encryption decoder according to claim 1, wherein a video frame comprises 45 slices each having 80 macroblocks, and wherein the star pattern is defined by: macroblocks 34-51 in slices 1-9 and 32-45, macroblocks 26-56 of slices 10-18 and 28-31 and macroblocks 1-80 of slices 19-27.

5. The selective encryption decoder according to claim 1, wherein a video frame comprises 68 slices each having 120 macroblocks, and wherein the star pattern is defined by: macroblocks 50-77 in slices 1-12 and 49-60, macroblocks 40-84 of slices 13-27 and 42-48 and macroblocks 1-120 of slices 28-41.

6. The selective encryption decoder according to claim 1, wherein the star pattern is centered above a true center of the image.

7. The selective encryption decoder according to claim 1 wherein the star pattern has rays extending horizontally across a full width of the image.

8. The selective encryption decoder according to claim 1, wherein the star pattern has rays extending vertically across a full height of the image.

9. The selective encryption decoder according to claim 1, wherein the star pattern has a rectangular central region centered approximately one slice above a center of the image.

10. A method of decrypting and decoding a selectively encrypted digital video signal, comprising:

receiving packets of digital video, certain of the packets being unencrypted and certain of the packets being encrypted, wherein certain of the encrypted packets carry data arranged in a star pattern within a video frame;

the unencrypted packets having a first packet identifier (PID) and the encrypted packets having a second packet identifier (PID);

decrypting the encrypted packets having the second PID to produce decrypted packets;

remapping at least one of the first and second PIDs so that the unencrypted packets and the decrypted packets have the same PID; and

decoding the unencrypted and decrypted packets to produce a decoded video signal.

11. The method according to claim 10, wherein the specified packet type further comprises packets containing an intra-coded macroblock within the star pattern.

12. The method according to claim 10, wherein a video frame comprises 30 slices each having 33 macroblocks, and wherein the star pattern is defined by: macroblocks 14-21 in slices 1-6 and 22-30, macroblocks 11-23 of slices 7-12 and 19-21 and macroblocks 1-33 of slices 13-18.

13. The method according to claim 10, wherein a video frame comprises 45 slices each having 80 macroblocks, and wherein the star pattern is defined by: macroblocks 34-51 in slices 1-9 and 32-45, macroblocks 26-56 of slices 10-18 and 28-31 and macroblocks 1-80 of slices 19-27.

14. The method according to claim 10, wherein a video frame comprises 68 slices each having 120 macroblocks, and wherein the star pattern is defined by: macroblocks 50-77 in slices 1-12 and 49-60, macroblocks 40-84 of slices 13-27 and 42-48 and macroblocks 1-120 of slices 28-41.

15. The method according to claim 10, wherein the star pattern is centered above a true center of the image.

16. The method according to claim 10, wherein the star pattern has rays extending horizontally across a full width of the image.

17. The method according to claim 10, wherein the star pattern has rays extending vertically across a full height of the image.

18. The method according to claim 10, wherein the star pattern has a

rectangular central region centered approximately one slice above a center of the image.

19. A computer readable medium storing instructions which, when executed on a programmed processor, carry out the method of encrypting a digital video signal according to claim 10.

20. The computer readable medium of claim 19, wherein the medium comprises an electronic storage medium.

21. A computer readable medium that carries instructions that when executes on a programmed processor to facilitate operation of a video receiver device to decrypt and decode a selectively encoded digital video signal wherein the instructions comprise:

a code segment that controls a demultiplexer that receives packets of digital video, certain of the packets being unencrypted and certain of the packets being encrypted, wherein certain of the encrypted packets carry data arranged in a star pattern within a video frame, the unencrypted packets having a first packet identifier (PID) and the encrypted packets having a second packet identifier (PID);

a code segment that controls decryption of the encrypted packets to produce decrypted packets;

a code segment that controls remapping at least one of the first and second PIDs so that the unencrypted packets and the decrypted packets have the same PID; and

a code segment that controls decoding the unencrypted and decrypted packets to produce a decoded video signal.

22. The computer readable medium of claim 21, wherein the medium comprises an electronic storage medium.

23. The computer readable medium according to claim 21, wherein the specified packet type further comprises packets containing an intra-coded macroblock within the star pattern.

24. The computer readable medium according to claim 21, wherein a video frame comprises 30 slices each having 33 macroblocks, and wherein the star pattern is defined by: macroblocks 14-21 in slices 1-6 and 22-30, macroblocks 11-23 of slices 7-12 and 19-21 and macroblocks 1-33 of slices 13-18.

25. The computer readable medium according to claim 21, wherein a video frame comprises 45 slices each having 80 macroblocks, and wherein the star pattern is defined by: macroblocks 34-51 in slices 1-9 and 32-45, macroblocks 26-56 of slices 10-18 and 28-31 and macroblocks 1-80 of slices 19-27.

26. The computer readable medium according to claim 21, wherein a video frame comprises 68 slices each having 120 macroblocks, and wherein the star pattern is defined by: macroblocks 50-77 in slices 1-12 and 49-60, macroblocks 40-84 of slices 13-27 and 42-48 and macroblocks 1-120 of slices 28-41.

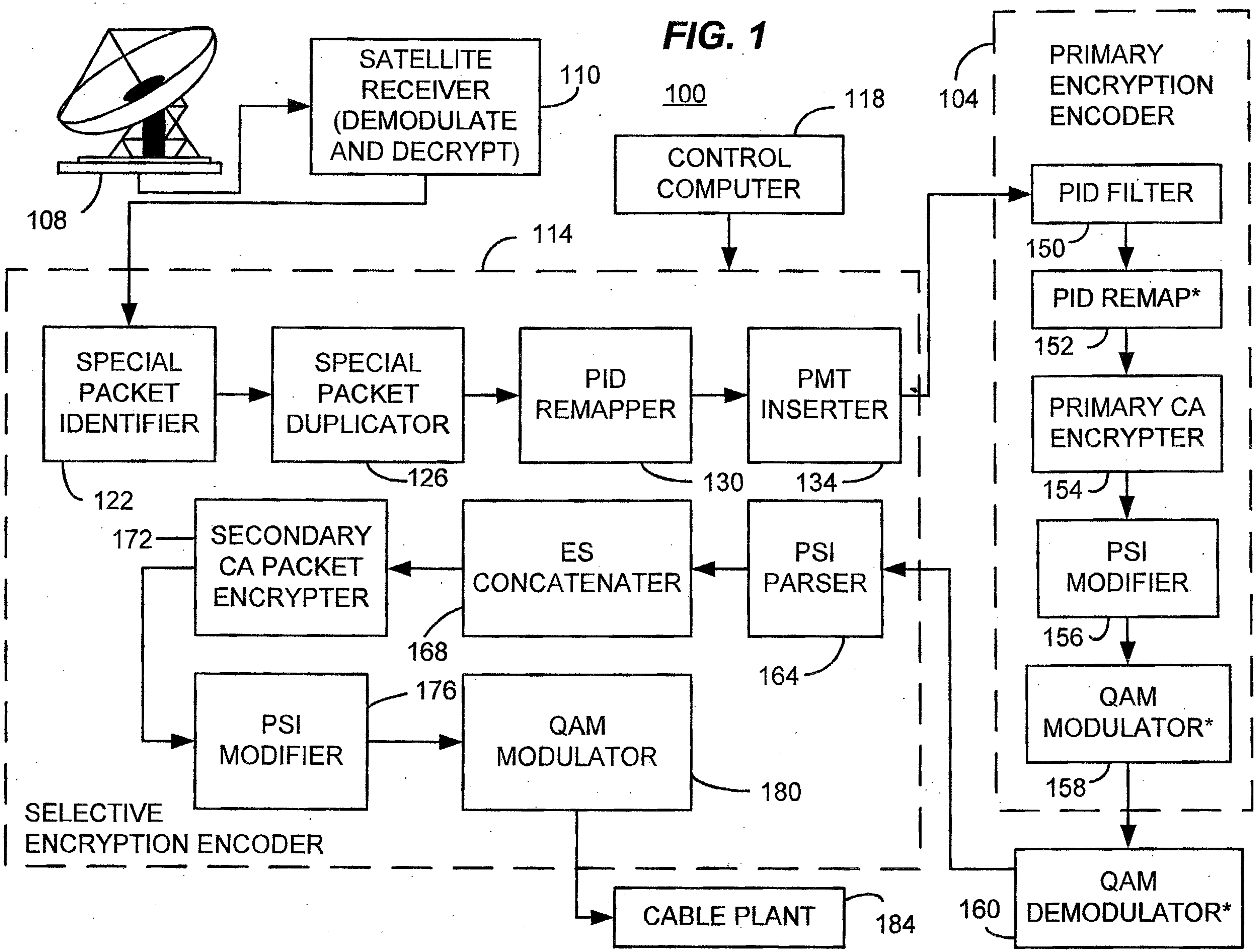
27. The computer readable medium according to claim 21, wherein the star pattern is centered above a true center of the image.

28. The computer readable medium according to claim 21, wherein the star pattern has rays extending horizontally across a full width of the image.

29. The computer readable medium according to claim 21, wherein the star pattern has rays extending vertically across a full height of the image.

30. The computer readable medium according to claim 21, wherein the star pattern has a rectangular central region centered approximately one slice above a center of the image.

FIG. 1



Gowling Lafleur Henderson LLP

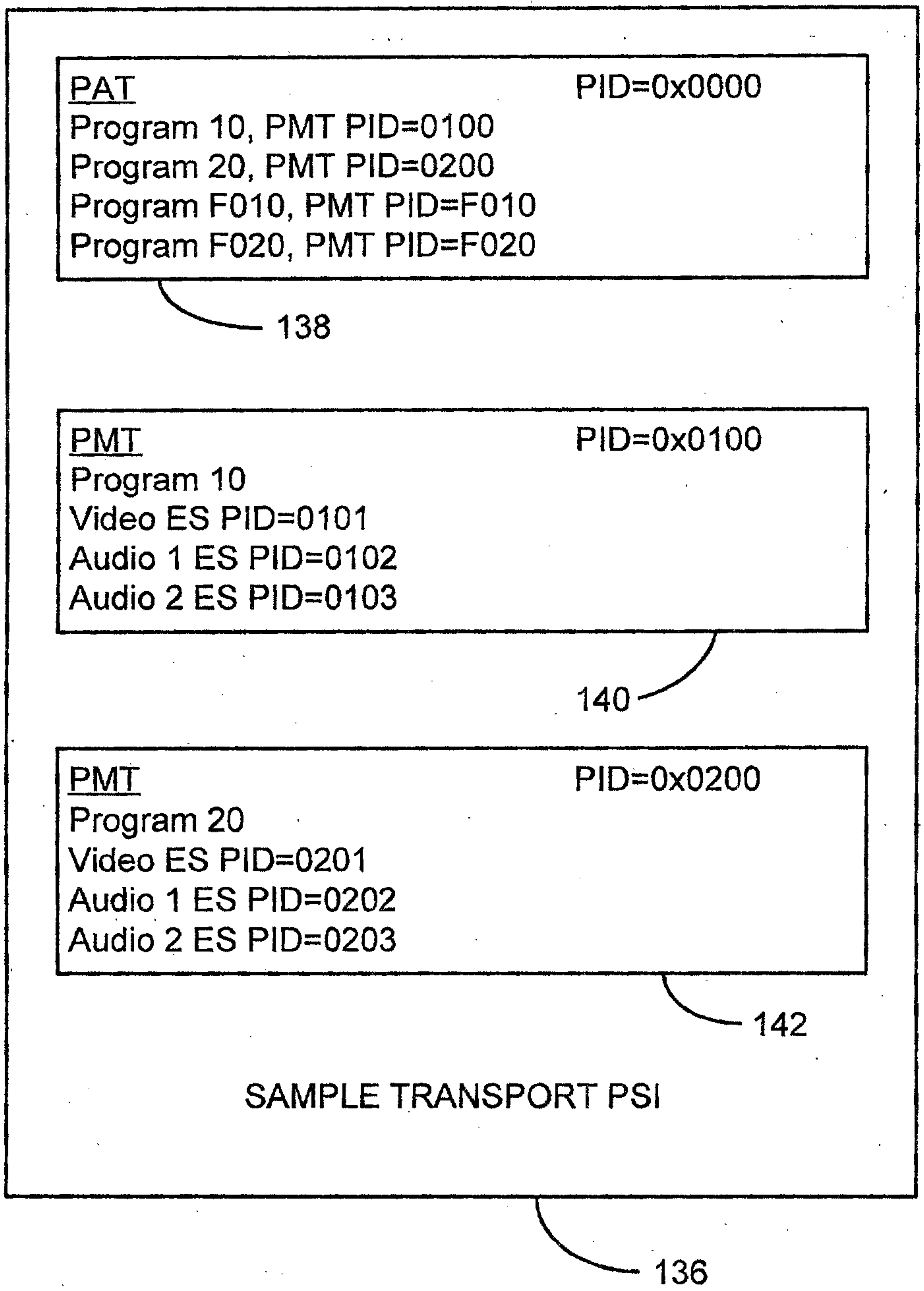

PAT
PID=0x0000
Program 10, PMT PID=0100
Program 20, PMT PID=0200
Program F010, PMT PID=F010
Program F020, PMT PID=F020
138
PMT
PID=0x0100
Program 10
Video ES PID=0101
Audio 1 ES PID=0102
Audio 2 ES PID=0103
140
PMT
PID=0x0200
Program 20
Video ES PID=0201
Audio 1 ES PID=0202
Audio 2 ES PID=0203
142
SAMPLE TRANSPORT PSI
136

FIG. 2

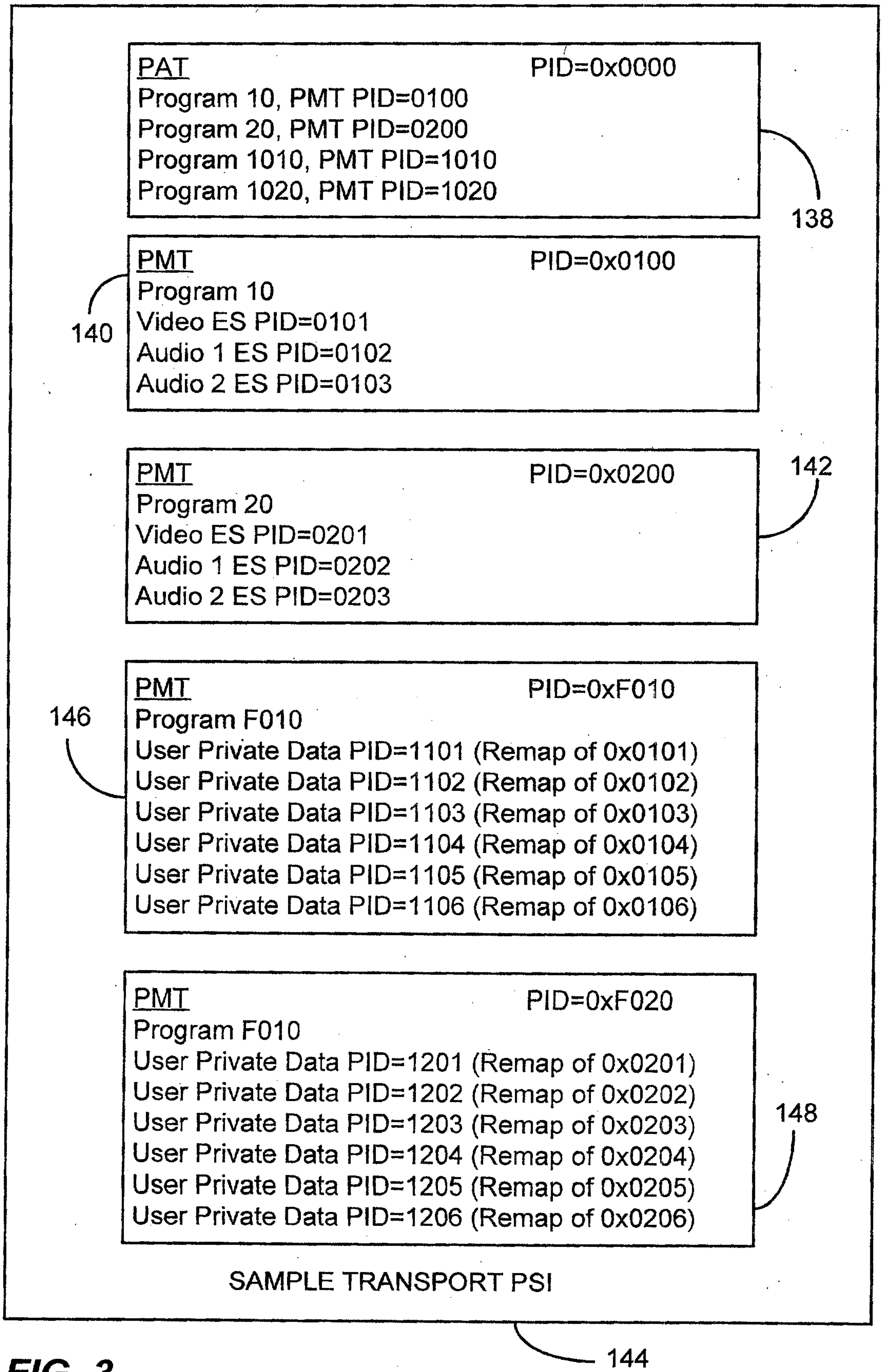

PAT PID=0x0000
Program 10, PMT PID=0100
Program 20, PMT PID=0200
Program 1010, PMT PID=1010
Program 1020, PMT PID=1020
138
PMT PID=0x0100
Program 10
Video ES PID=0101
Audio 1 ES PID=0102
Audio 2 ES PID=0103
140
PMT PID=0x0200
Program 20
Video ES PID=0201
Audio 1 ES PID=0202
Audio 2 ES PID=0203
142
PMT PID=0xF010
Program F010
User Private Data PID=1101 (Remap of 0x0101)
User Private Data PID=1102 (Remap of 0x0102)
User Private Data PID=1103 (Remap of 0x0103)
User Private Data PID=1104 (Remap of 0x0104)
User Private Data PID=1105 (Remap of 0x0105)
User Private Data PID=1106 (Remap of 0x0106)
146
PMT PID=0xF020
Program F010
User Private Data PID=1201 (Remap of 0x0201)
User Private Data PID=1202 (Remap of 0x0202)
User Private Data PID=1203 (Remap of 0x0203)
User Private Data PID=1204 (Remap of 0x0204)
User Private Data PID=1205 (Remap of 0x0205)
User Private Data PID=1206 (Remap of 0x0206)
148
SAMPLE TRANSPORT PSI
144

FIG. 3

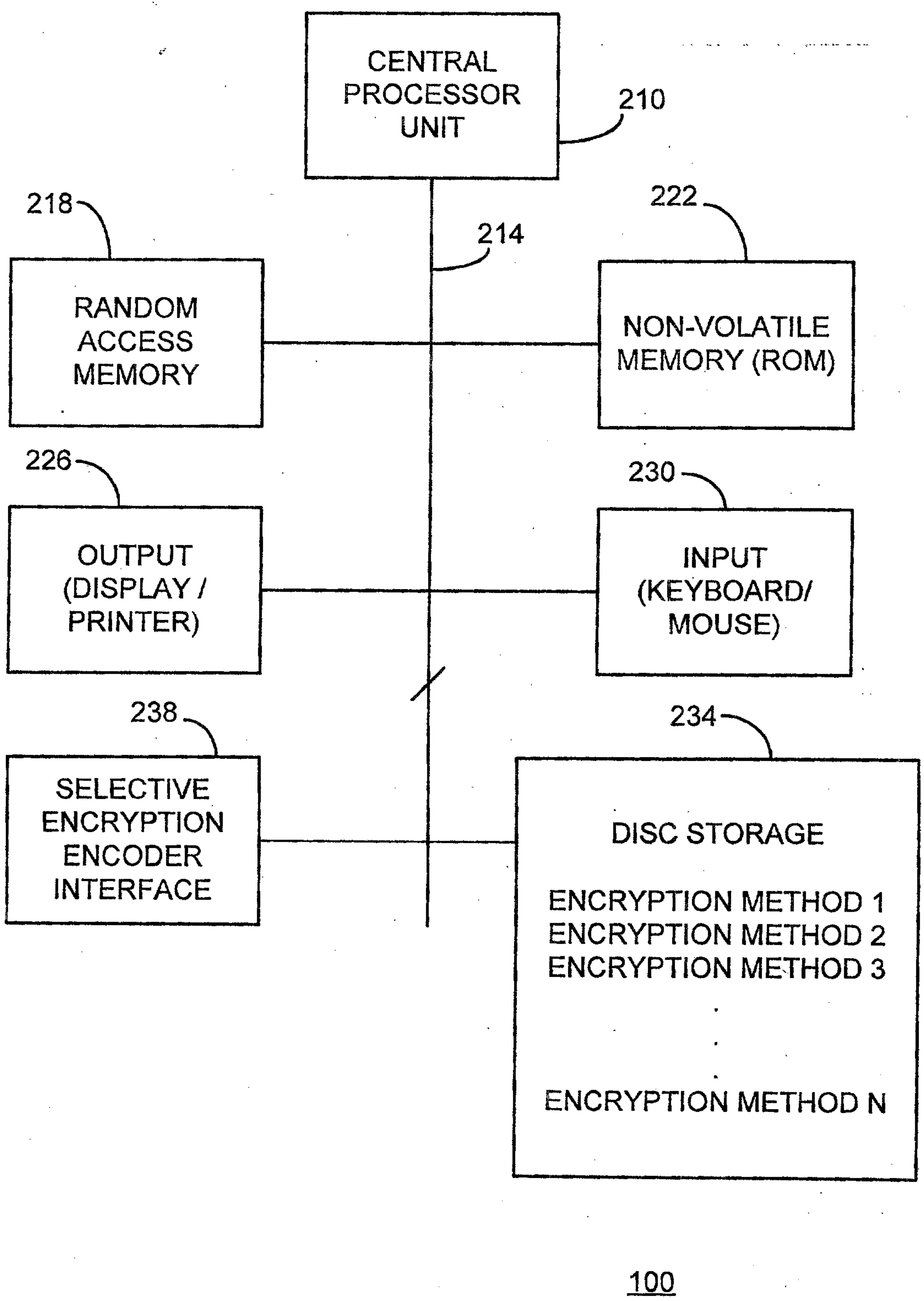

CENTRAL PROCESSOR UNIT
210
214
218
RANDOM ACCESS MEMORY
222
NON-VOLATILE MEMORY (ROM)
226
OUTPUT (DISPLAY / PRINTER)
230
INPUT (KEYBOARD/ MOUSE)
238
SELECTIVE ENCRYPTION ENCODER INTERFACE
234
DISC STORAGE
ENCRYPTION METHOD 1
ENCRYPTION METHOD 2
ENCRYPTION METHOD 3
ENCRYPTION METHOD N
100

FIG. 4

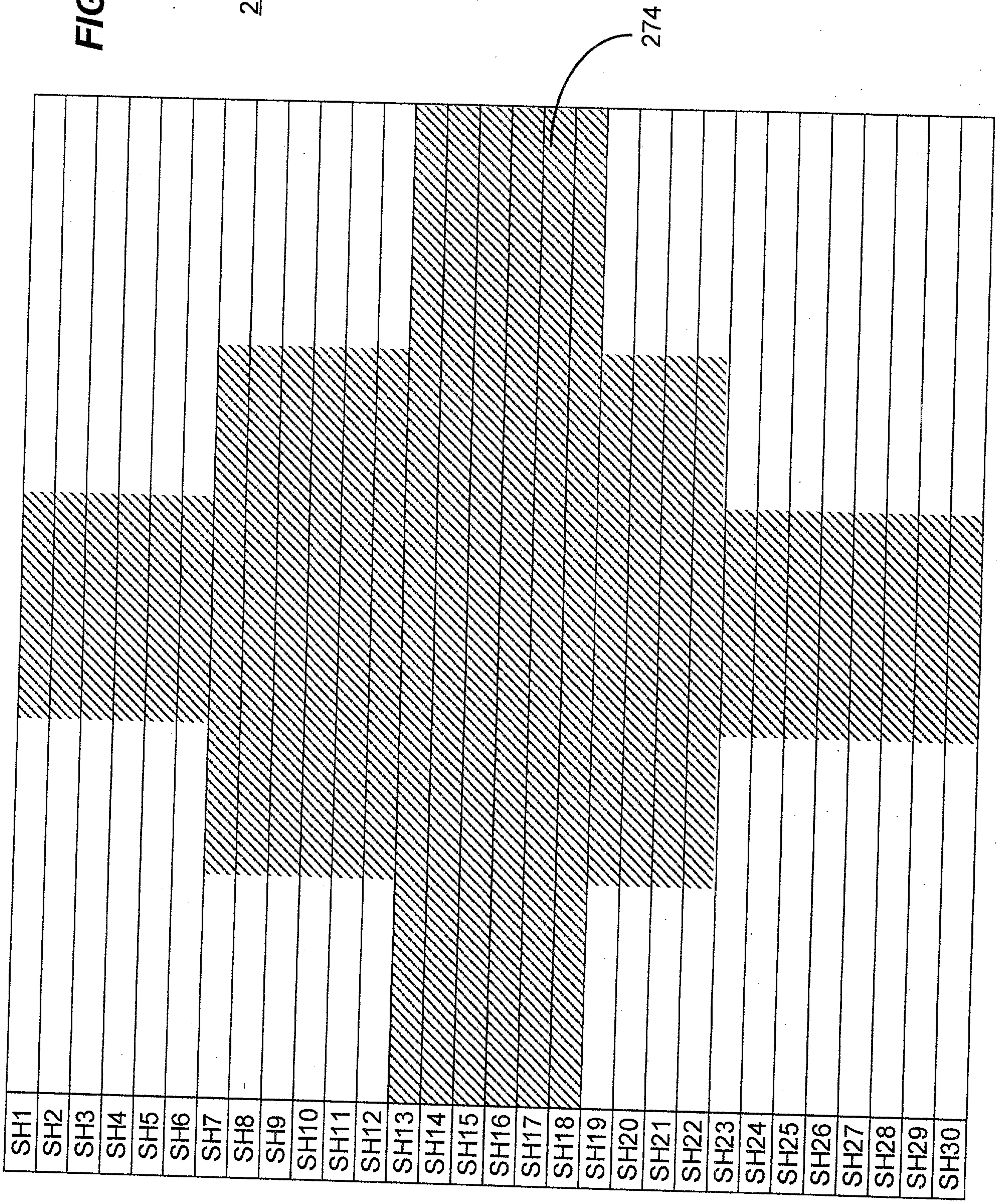
FIG. 5

250

SH1	MB1	MB2	...	MB32	MB33
SH2	MB1	MB2	...	MB32	MB33
SH3	MB1	MB2	...	MB32	MB33
SH4	MB1	MB2	...	MB32	MB33
SH5	MB1	MB2	...	MB32	MB33
SH6	MB1	MB2	...	MB32	MB33
SH7	MB1	MB2	...	MB32	MB33
SH8	MB1	MB2	...	MB32	MB33
SH9	MB1	MB2	...	MB32	MB33
SH10	MB1	MB2	...	MB32	MB33
SH11	MB1	MB2	...	MB32	MB33
SH12	MB1	MB2	...	MB32	MB33
SH13	MB1	MB2	...	MB32	MB33
SH14	MB1	MB2	...	MB32	MB33
SH15	MB1	MB2	...	MB32	MB33
SH16	MB1	MB2	...	MB32	MB33
SH17	MB1	MB2	...	MB32	MB33
SH18	MB1	MB2	...	MB32	MB33
SH19	MB1	MB2	...	MB32	MB33
SH20	MB1	MB2	...	MB32	MB33
SH21	MB1	MB2	...	MB32	MB33
SH22	MB1	MB2	...	MB32	MB33
SH23	MB1	MB2	...	MB32	MB33
SH24	MB1	MB2	...	MB32	MB33
SH25	MB1	MB2	...	MB32	MB33
SH26	MB1	MB2	...	MB32	MB33
SH27	MB1	MB2	...	MB32	MB33
SH28	MB1	MB2	...	MB32	MB33
SH29	MB1	MB2	...	MB32	MB33
SH30	MB1	MB2	...	MB32	MB33

FIG. 6

270


274
SH1
SH2
SH3
SH4
SH5
SH6
SH7
SH8
SH9
SH10
SH11
SH12
SH13
SH14
SH15
SH16
SH17
SH18
SH19
SH20
SH21
SH22
SH23
SH24
SH25
SH26
SH27
SH28
SH29
SH30

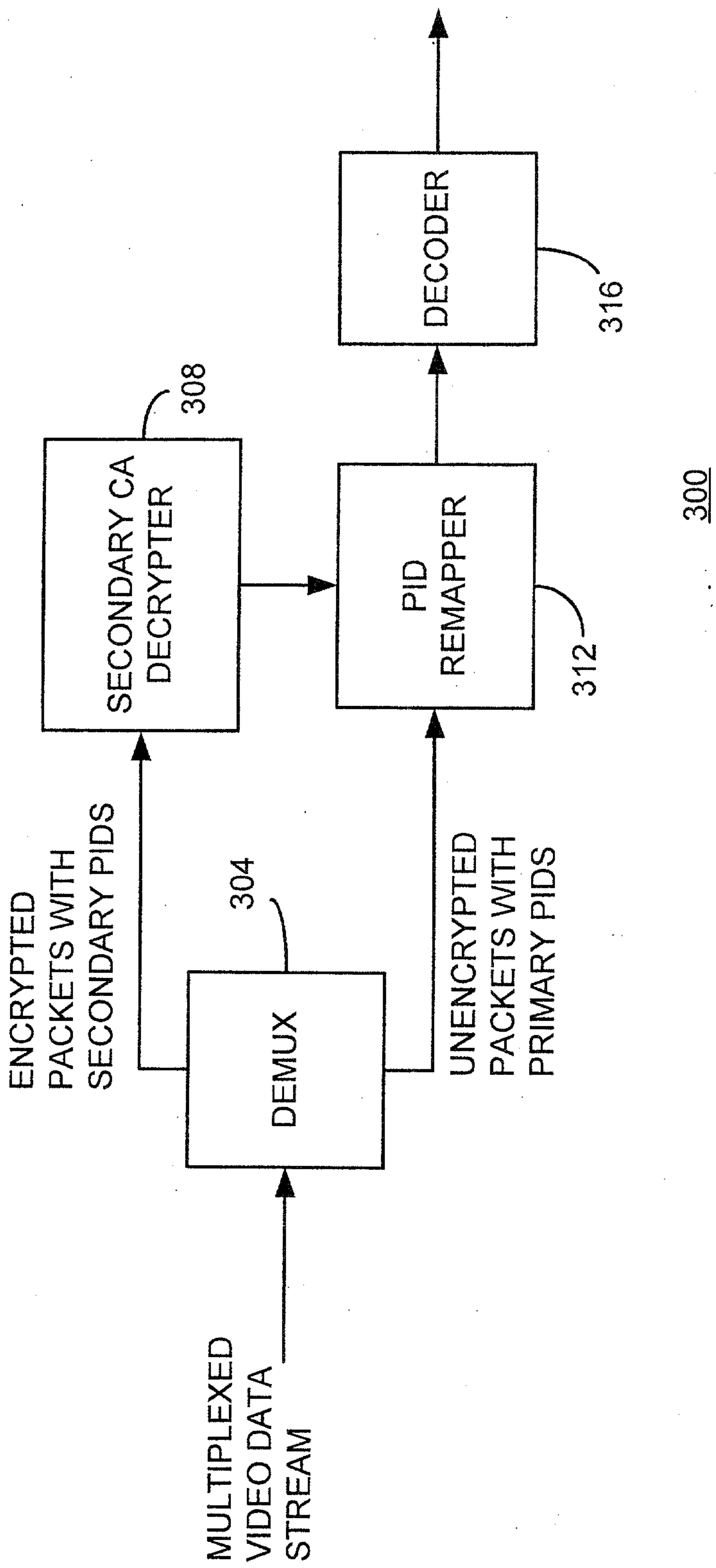

MULTIPLEXED VIDEO DATA STREAM
DEMUX
304
ENCRYPTED PACKETS WITH SECONDARY PIDS
UNENCRYPTED PACKETS WITH PRIMARY PIDS
SECONDARY CA DECRYPTER
308
PID REMAPPER
312
DECODER
316
300

FIG. 7

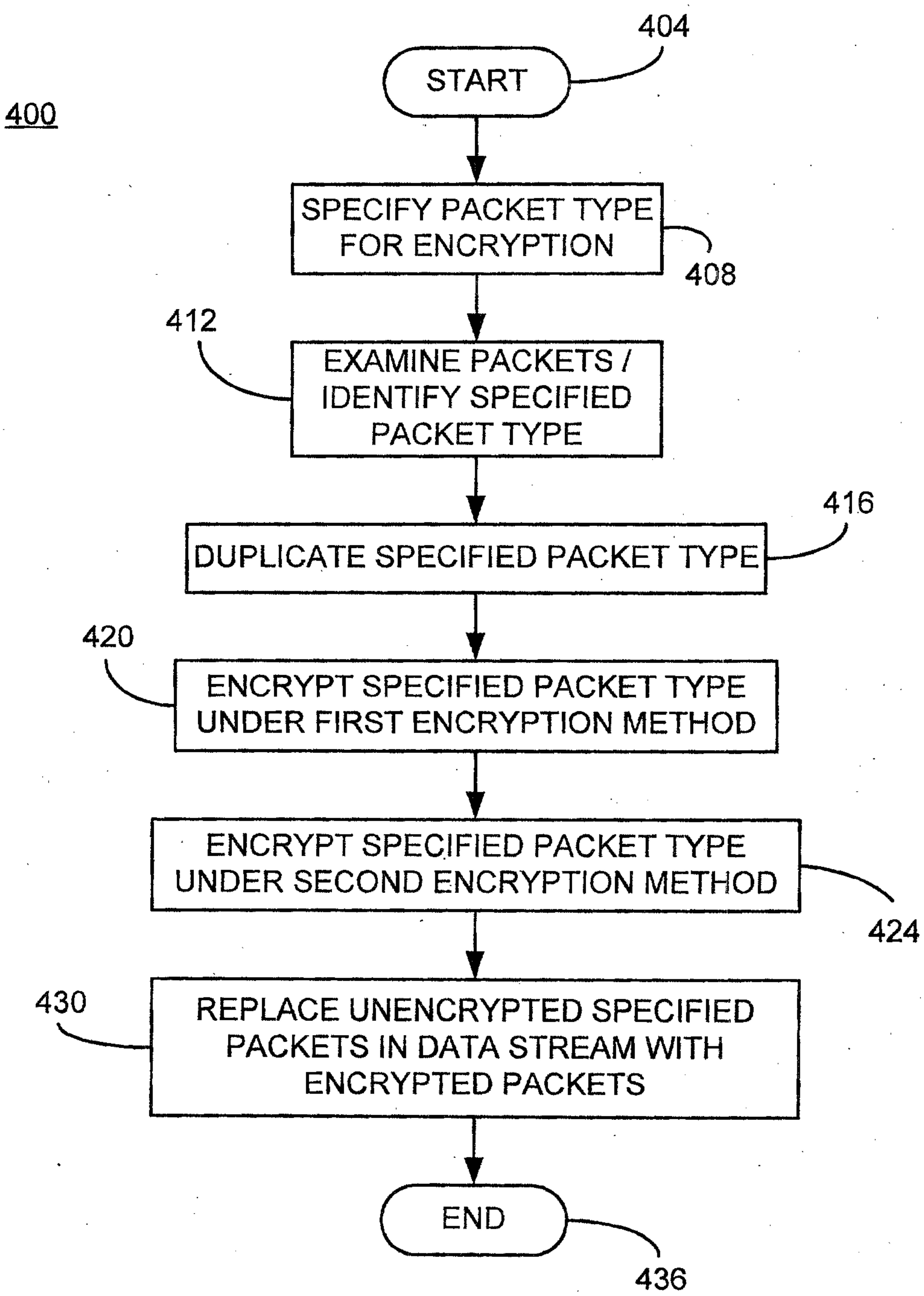
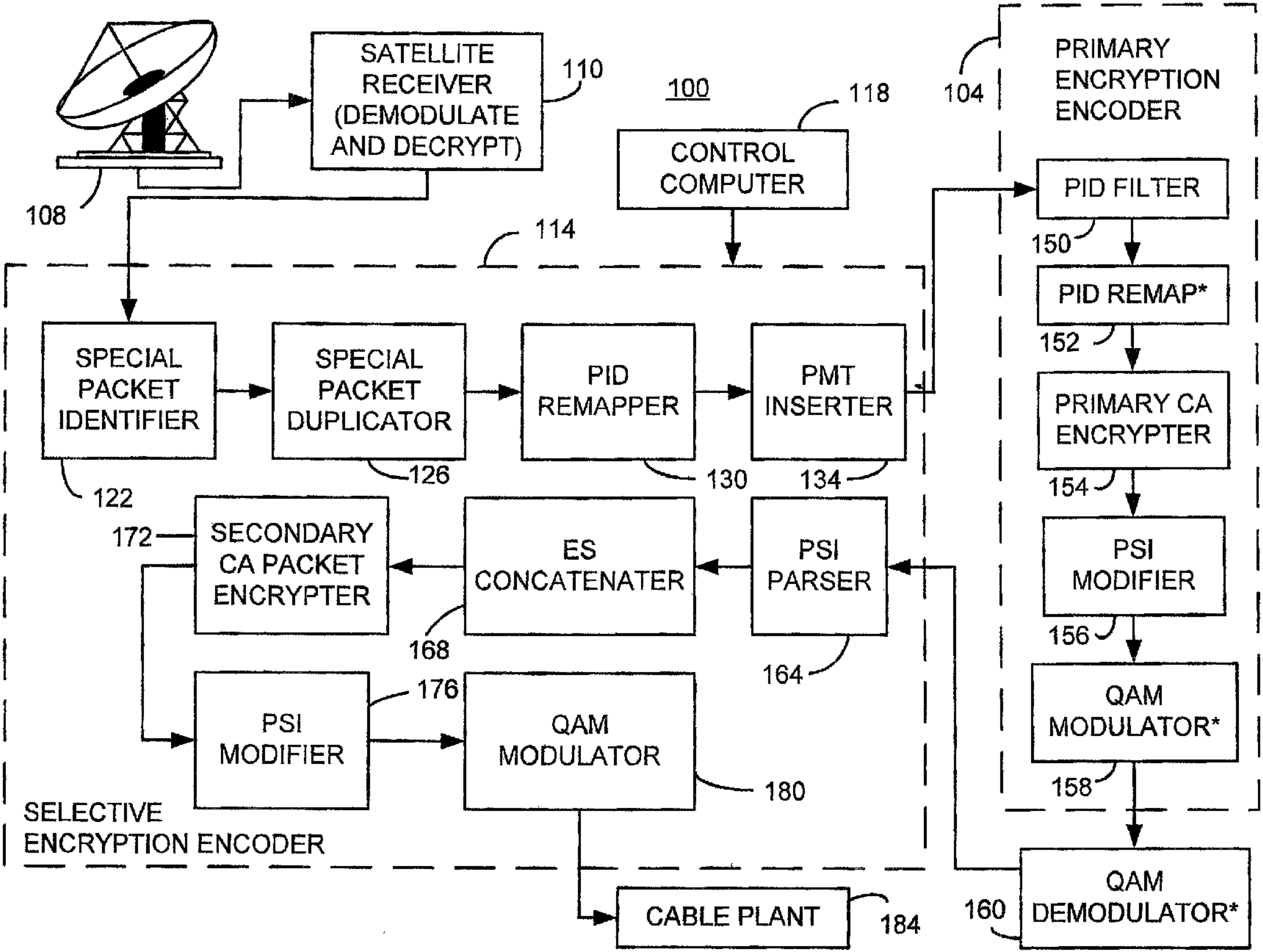

400
404
START
SPECIFY PACKET TYPE FOR ENCRYPTION
408
412
EXAMINE PACKETS / IDENTIFY SPECIFIED PACKET TYPE
416
DUPLICATE SPECIFIED PACKET TYPE
420
ENCRYPT SPECIFIED PACKET TYPE UNDER FIRST ENCRYPTION METHOD
ENCRYPT SPECIFIED PACKET TYPE UNDER SECOND ENCRYPTION METHOD
424
430
REPLACE UNENCRYPTED SPECIFIED PACKETS IN DATA STREAM WITH ENCRYPTED PACKETS
END
436

FIG. 8


SATELLITE RECEIVER (DEMODULATE AND DECRYPT)
110
100
118
104
PRIMARY ENCRYPTION ENCODER
CONTROL COMPUTER
PID FILTER
108
114
150
PID REMAP*
152
SPECIAL PACKET IDENTIFIER
SPECIAL PACKET DUPLICATOR
PID REMAPPER
PMT INSERTER
PRIMARY CA ENCRYPTER
126
130
134
154
122
172
SECONDARY CA PACKET ENCRYPTER
ES CONCATENATER
PSI PARSER
PSI MODIFIER
156
168
164
176
PSI MODIFIER
QAM MODULATOR
QAM MODULATOR*
180
158
SELECTIVE ENCRYPTION ENCODER
QAM DEMODULATOR*
CABLE PLANT
184
160