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

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2413880 A1 2003/07/02

(21) 2 413 880

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) Date de dépôt/Filing Date: 2002/12/10

(41) Mise à la disp. pub./Open to Public Insp.: 2003/07/02

(30) Priorités/Priorities: 2002/01/02 (10/038,217) US; 2002/01/02 (10/038,032) US; 2002/01/02 (10/037,914) US; 2002/01/02 (10/037,499) US; 2002/01/02 (10/037,498) US; 2002/02/08 (60/355,326) US; 2002/04/05 (60/370,274) US; 2002/10/18 (10/273,875) US

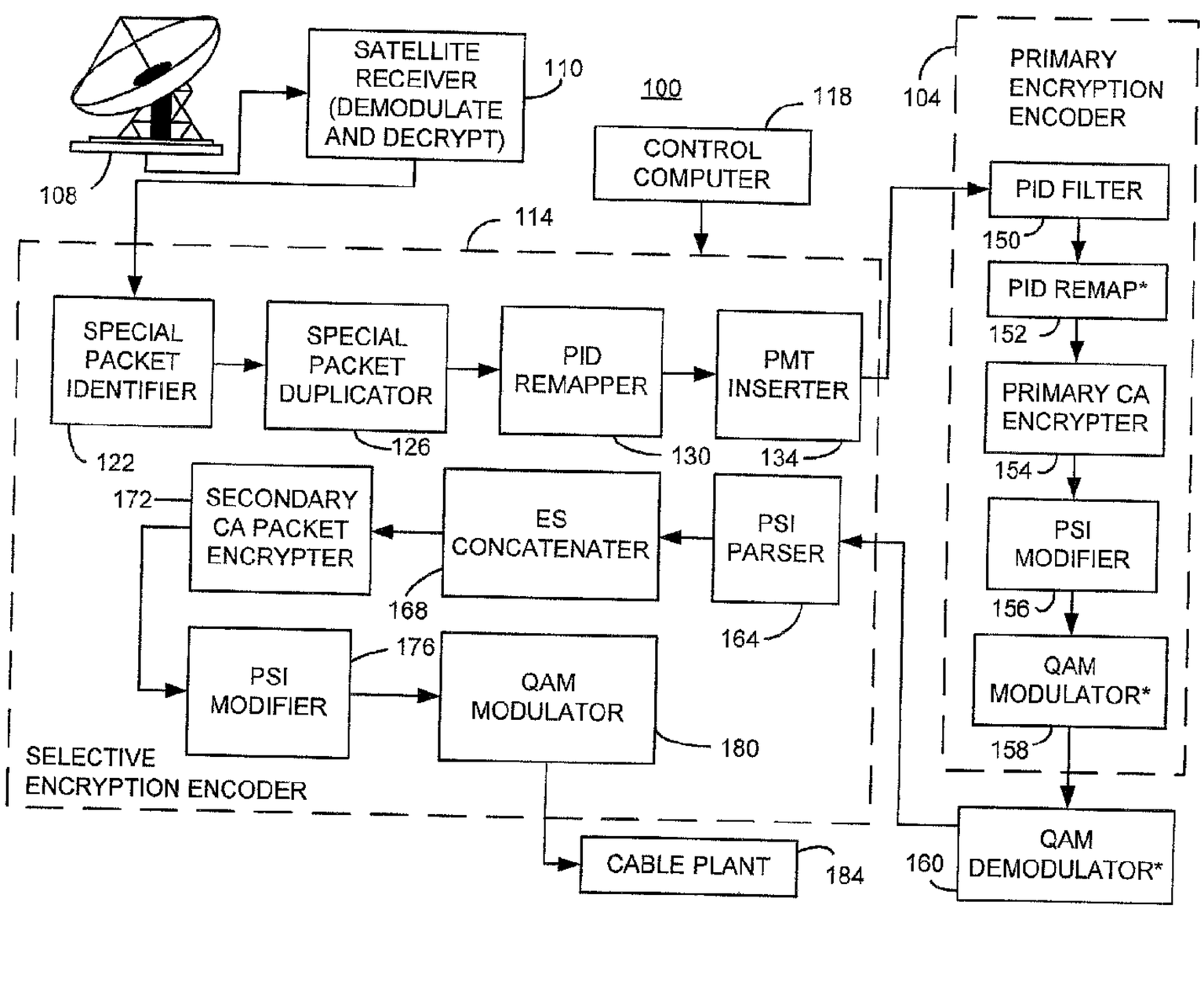
(51) Cl.Int.^{7}/Int.Cl.^{7} H04N 7/167, H04L 9/14

(71) Demandeur/Applicant:
SONY ELECTRONICS INC., US

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

(74) Agent: GOWLING LAFLEUR HENDERSON LLP

(54) Titre : CRYPTAGE ET COMMANDE DU CONTENU DANS UN SYSTEME DE RADIODIFFUSION NUMERIQUE
(54) Title: ENCRYPTION AND CONTENT CONTROL IN A DIGITAL BRAODCAST SYSTEM



(57) Abrégé/Abstract:
A selective encryption encoder has a packet identifier that identifies packets of a specified packet type forming a part of a program. A packet duplicator duplicates the identified packets to produce first and second sets of the identified packets. A PMT (program map table) inserter generates temporary identifying information that identifies the first and second sets of identified packets inserts the temporary identifying information as user private data in a program map table (PMT) forming a part of the transport program specific information (PSI). The data are then sent to and received 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. The PSI is then modified at a PSI modifier to remove the temporary identifying information and to correctly associate the first and second sets of identified packets and the unencrypted packets with the program.

ABSTRACT OF THE DISCLOSURE

A selective encryption encoder has a packet identifier that identifies packets of a specified packet type forming a part of a program. A packet duplicator duplicates the identified packets to produce first and second sets of the identified packets. A PMT (program map table) inserter generates temporary identifying information that identifies the first and second sets of identified packets inserts the temporary identifying information as user private data in a program map table (PMT) forming a part of the transport program specific information (PSI). The data are then sent to and received 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. The PSI is then modified at a PSI modifier to remove the temporary identifying information and to correctly associate the first and second sets of identified packets and the unencrypted packets with the program.

ENCRYPTION AND CONTENT CONTROL IN A DIGITAL BROADCAST SYSTEM

CROSS REFERENCE TO RELATED DOCUMENTS

This application is a continuation in part of patent applications docket number SNY-R4646.01 entitled "Critical Packet Partial Encryption" to Unger et al., serial number 10/038,217; patent applications docket number SNY-R4646.02 entitled "Time Division Partial Encryption" to Candelore et al., serial number 10/038,032; docket number SNY-R4646.03 entitled "Elementary Stream Partial Encryption" to Candelore , serial number 10/037,914; docket number SNY-R4646.04 entitled "Partial Encryption and PID Mapping" to Unger et al., serial number 10/037,499; and docket number SNY-R4646.05 entitled "Decoding and Decrypting of Partially Encrypted Information" to Unger et al., serial number 10/037,498 all of which were filed on January 2, 2002 and are hereby incorporated by reference herein.

This application is also related to and claims priority benefit of U.S. Provisional patent application serial number 60/355,326 filed February 8, 2002 docket number 50R4900, entitled "Analysis of Content Selection Methods", to Candelore and to U.S. Provisional patent application serial number 60/370,274 filed April 5, 2002, docket number 50R4903 entitled " Method of Control of Encryption and Content in a Digital Broadcast System" to Pedlow, Jr., et al. These applications are also hereby incorporated by reference herein.

COPYRIGHT NOTICE

FIELD OF THE INVENTION

This invention relates generally to the field of encryption. More particularly, this invention relates to a method of control of content and encryption in a digital broadcast system.

BACKGROUND OF THE INVENTION

The above-referenced commonly owned patent applications 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.

In order to provide appropriate tracking of clear packets and packets encrypted under multiple encryption systems, a system of multiple packet identifiers (PIDs) has been devised as described in the above-referenced patent

applications. However, in head-end equipment provided by certain manufacturers, the PIDs can be remapped within the encryption encoder. This can result in the system losing track of the clear and encrypted packets.

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 is a flow chart generally describing the overall operation of the selective encryption encoder 114.

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 operational process 250 of the selective encryption encoder 114 of **FIGURE 1** is described generally by the flow chart of **FIGURE 5** starting at 254. Incoming packets from the satellite receiver 110 are first optionally remapped at 122. In accordance with the specified dual encryption process, packets to be encrypted are identified at 258 and these packets are duplicated and mapped to specific PIDs at 262. The original unencrypted packets that are to be encrypted are replaced with these duplicated packets at 262. Temporary identifying information is inserted as PMT tables of the PSI, with the identifying information being coded as user private data at 270. This will permit reassociation of the proper packets with appropriate PIDs after processing (and possible PID remapping) by the primary encryption encoder. The data stream with the PSI, unencrypted and duplicated packets is then sent to the primary encryption encoder at 274 where it is processed by encryption of one set of the duplicated packets. As previously mentioned, for

Scientific Atlanta encoders (or any other encoder operating in a similar manner), the PIDs may be remapped inside the encoder.

The data stream is then returned from the primary encryption encoder at 278. The data stream is then processed by parsing the PSI information to recover information describing any PID remapping that has taken place in the primary encryption encoder at 282. PID remapping can be addressed at this point in either of at least two ways. In one embodiment, the PIDs can be remapped back to the mapping as originally sent to the primary encryption encoder. This, of course, requires that each packet be examined and potentially remapped. A simpler technique is to simply accept any remapping that the primary encryption encoder has done.

The selective encryption processor encrypts the other of the pair of duplicated packets at 286. The PIDs can then either be remapped as described above or the PSI can simply be modified to correct for any PID remapping at 290. Also at 290, the temporary identifying information added to the PSI at 270 can be removed. The resultant data stream can then be modulated and transmitted to the end user at 294 and the process ends at 298.

The partial encryption process described above utilizes any suitable conditional access encryption method at encrypters 154 and 174. Any suitable selective encryption process (e.g., such as those described in the above-referenced applications or any other suitable selective encryption technique). For example, in one such technique, only slice headers are encrypted at encrypters 154 and 174. Other encryption techniques are also possible. 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. Additionally, multiple combinations of the above techniques are possible to produce encryption that has varying bandwidth requirements, varying levels of

security and varying complexity. Control computer 118 can be used to selectively choose an encryption technique from a plurality of available techniques. 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.

Many modifications will occur to those skilled in the art which fall within the scope of the present invention. For example, in certain embodiments, it is not necessary to map the duplicated content to two new PID packets. In this embodiment, only one of the packets is remapped to get the legacy equipment to encrypt it. The other can stay "disguised" with the content that is to remain "clear". The PSI can be correspondingly simpler in such an embodiment.

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). 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 method, comprising:

examining unencrypted packets of data in the digital video signal to identify a specified packet type;

duplicating the packets of the specified packet type to produce duplicate packets;

identifying the duplicate packets by a first packet identifier (PID);

identifying remaining unencrypted packets by a second packet identifier (PID);

replacing the packets of the specified packet type with the first duplicate packets;

generating identifying information that identifies the first duplicate packets, and the unencrypted packets;

storing the identifying information as transport program specific information (PSI);

creating a data stream comprising the PSI, the first duplicate packets, and the unencrypted packets into the data stream; and

sending the data stream to a primary encryption encoder.

2. The method according to claim 1, wherein the identifying information is stored as user private data a program map table (PMT) in the transport PSI.

3. The method according to claim 1, further comprising:

receiving a data stream back from the primary encryption encoder;

reading a program map table (PMT), a program association tables (PAT) and the identifying information from the transport PSI; and

mapping the PIDs associated with at least one of the first duplicate packets and the unencrypted packets to values stored in the identifying information.

4. The method according to claim 3, further comprising deleting the identifying information from the PSI.

5. The method according to claim 1, further comprising:

receiving a data stream back from the primary encryption encoder;

reading a program map table (PMT), a program association tables (PAT) and the identifying information from the transport PSI; and

modifying the PSI to reflect any remapping the PIDs in the primary encryption encoder.

6. The method according to claim 1, further comprising deleting the identifying information from the PSI.

7. A computer readable medium storing instructions which, when executed on a programmed processor, carry out the selective encryption method according to claim 1.

8. The computer readable medium of claim 7, wherein the medium comprises one of an electronic storage medium and a carrier wave.

9. An electronic transmission medium carrying a digital video signal encrypted by the method according to claim 1.

10. A selective encryption method, comprising:

examining unencrypted packets of data in the digital video signal to identify a specified packet type;

duplicating the packets of the specified packet type to produce first and second duplicate packets;

identifying the first duplicate packets by a first packet identifier (PID);

identifying the second duplicate packets by a second packet identifier (PID);

identifying unencrypted packets by a third packet identifier (PID);

replacing the packets of the specified packet type with the first duplicate packets and the second duplicate packets;

generating identifying information that identifies the first duplicate packets, the second duplicate packets and the unencrypted packets;

storing the identifying information as transport program specific information (PSI);

creating a data stream comprising the PSI, the first duplicate packets, the second duplicate packets and the unencrypted packets into the data stream; and

sending the data stream to a primary encryption encoder.

11. The method according to claim 10, wherein the identifying information is stored as user private data a program map table (PMT) in the transport PSI.

12. The method according to claim 10, further comprising:

receiving a data stream back from the primary encryption encoder;

reading a program map table (PMT), a program association tables (PAT) and the identifying information from the transport PSI; and

mapping the PIDs associated with at least one of the first duplicate packets, the second duplicate packets and the unencrypted packets to values stored in the identifying information.

13. The method according to claim 12, further comprising deleting the identifying information from the PSI.

14. The method according to claim 10, further comprising:

receiving a data stream back from the primary encryption encoder;

reading a program map table (PMT), a program association tables (PAT) and the identifying information from the transport PSI; and

modifying the PSI to reflect any remapping the PIDs in the primary encryption encoder.

15. The method according to claim 10, further comprising deleting the identifying information from the PSI.

16. A computer readable medium storing instructions which, when executed on a programmed processor, carry out the selective encryption method according to claim 10.

17. The computer readable medium of claim 16, wherein the medium comprises one of an electronic storage medium and a carrier wave.

18. An electronic transmission medium carrying a digital video signal encrypted by the method according to claim 10.

19. A selective encryption encoder, comprising:

a packet identifier that identifies packets of a specified packet type forming a part of a program;

a packet duplicator, receiving an output from the packet identifier, that duplicates the identified packets to produce first and second sets of the identified packets;

means for generating temporary identifying information that identifies the first and second sets of identified packets and for inserting the temporary identifying information as transport program specific information (PSI); and

means for sending and receiving packets to and from a primary encryption encoder to encrypt the first set of identified packets under a first encryption method.

20. The selective encryption encoder of claim 19, wherein the temporary identifying information is stored as user private data in a program map table.

21. The selective encryption encoder of claim 19, further comprising:

a secondary encrypter for encrypting the second set of identified packets under a second encryption method; and

means for modifying the PSI to remove the temporary identifying information and to correctly associate the first and second sets of identified packets with the program.

22. The selective encryption encoder of claim 21, wherein the means for modifying the PSI further modifies the PSI to correctly associated unencrypted packets with the program.

23. The selective encryption encoder of claim 19, further comprising:

a secondary encrypter for encrypting the second set of identified packets under a second encryption method;

means for modifying the PSI to remove the temporary identifying information; and

a PID remapper that remaps the PIDs associated with the first and second identified packets to correctly associate the first and second sets of identified packets with the program.

24. The selective encryption encoder of claim 23, wherein the PID remapper further remaps PIDs associated with unencrypted packets to correctly associate the unencrypted packets with the program.

25. A selective encryption encoder, comprising:

means for receiving a demodulated clear data stream of unencrypted packets carrying a program;

a PID remapper that remaps packet identifiers (PIDs) associated with the program;

a packet identifier, receiving an output from the PID remapper, that identifies packets of a specified packet type forming a part of the program;

a packet duplicator, receiving an output of the packet identifier, that duplicates the identified packets to produce first and second sets of the identified packets;

means for generating temporary identifying information that identifies the first and second sets of identified packets and for inserting the temporary identifying information as user private data in a program map table (PMT) forming a part of transport program specific information (PSI);

means for sending and receiving packets comprising the PSI, the first and second sets of identified packets and the unencrypted packets to and from a primary encryption encoder to encrypt the first set of identified packets under a first encryption method;

a secondary encrypter for encrypting the second set of identified packets under a second encryption method;

means for modifying the PSI to remove the temporary identifying information and to correctly associate the first and second sets of identified packets and unencrypted packets with the program; and

a quadrature amplitude modulation (QAM) modulator that QAM modulates a data stream associated with the program and comprising PSI, first and second identified packets and the unencrypted packets.

26. A computer readable medium that carries instructions that when executes on a programmed processor to facilitate operation of a selective encryption encoder wherein the instructions comprise:

a code segment that examines unencrypted packets of data in the digital video signal to identify a specified packet type;

a code segment that duplicates the packets of the specified packet type to produce first and second duplicate packets;

a code segment that identifies the first duplicate packets by a first packet identifier (PID);

a code segment that identifies the second duplicate packets by a second packet identifier (PID);

a code segment that identifies unencrypted packets by a third packet identifier (PID);

a code segment that replaces the packets of the specified packet type with the first duplicate packets and the second duplicate packets;

a code segment that generates identifying information that identifies the first duplicate packets, the second duplicate packets and the unencrypted packets;

a code segment that stores the identifying information as transport program specific information (PSI); and

a code segment that creates a data stream comprising the PSI, the first duplicate packets, the second duplicate packets and the unencrypted packets into the data stream.

27. The computer readable medium of claim 26, wherein the medium comprises one of an electronic storage medium and a carrier wave.

28. A computer readable medium carrying instructions that, when executed, carry out a selective encryption method, comprising:

examining unencrypted packets of data in the digital video signal to identify a specified packet type;

duplicating the packets of the specified packet type to produce first and second duplicate packets;

identifying the first duplicate packets by a first packet identifier (PID);

identifying the second duplicate packets by a second packet identifier (PID);

identifying unencrypted packets by a third packet identifier (PID);

replacing the packets of the specified packet type with the first duplicate packets and the second duplicate packets;

generating identifying information that identifies the first duplicate packets, the second duplicate packets and the unencrypted packets;

storing the identifying information as transport program specific information (PSI); and

creating a data stream comprising the PSI, the first duplicate packets, the second duplicate packets and the unencrypted packets into the data stream.

29. The computer readable medium of claim 28, wherein the medium comprises one of an electronic storage medium and a carrier wave.

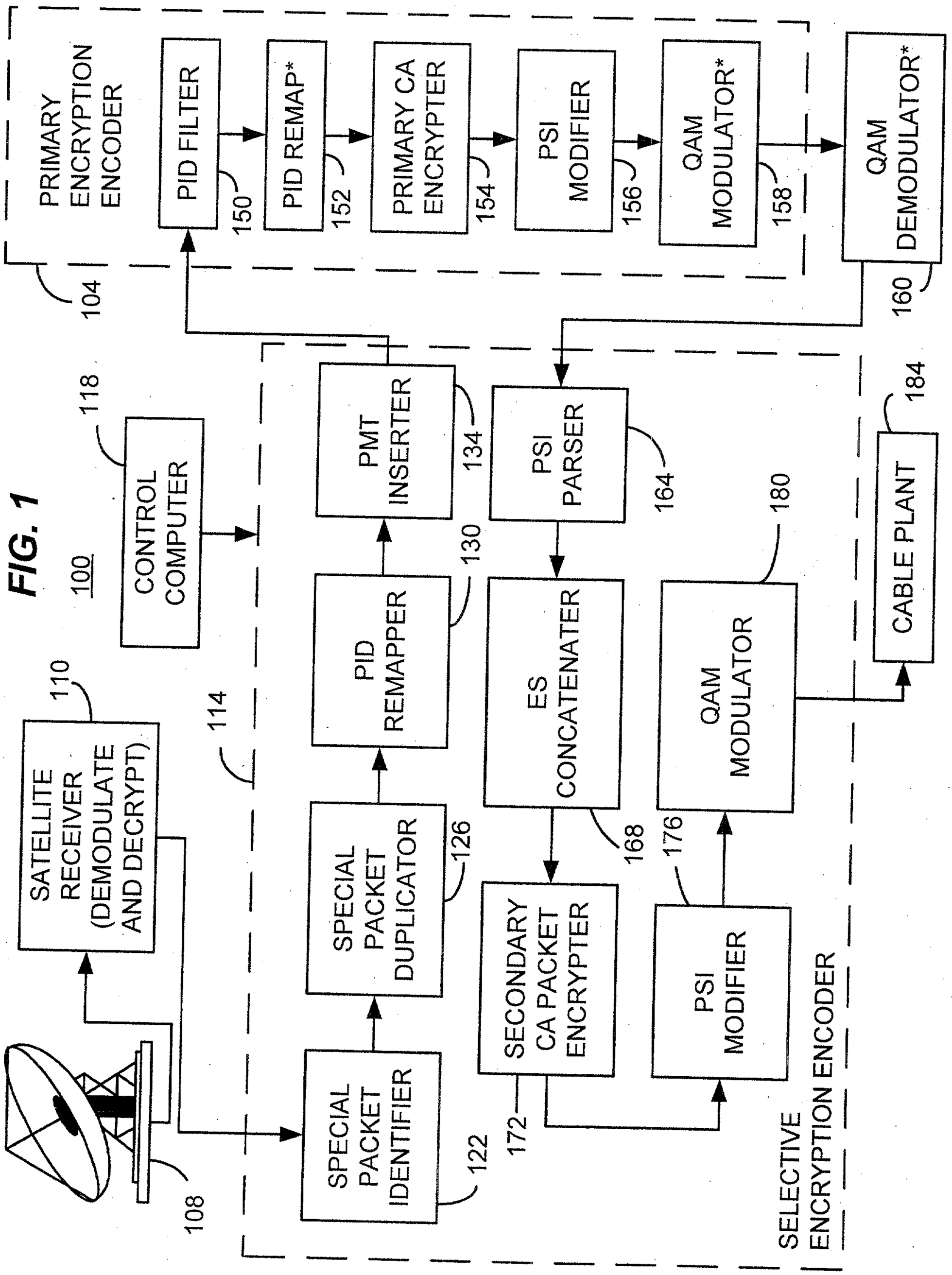


FIG. 1
100
SATELLITE RECEIVER (DEMODULATE AND DECRYPT)
110
108
CONTROL COMPUTER
118
114
PRIMARY ENCRYPTION ENCODER
104
PID FILTER
150
PID REMAP*
152
PRIMARY CA ENCRYPTER
154
PSI MODIFIER
156
QAM MODULATOR*
158
QAM DEMODULATOR*
160
SPECIAL PACKET IDENTIFIER
122
SPECIAL PACKET DUPLICATOR
126
PID REMAPPER
130
PMT INSERTER
134
PSI PARSER
164
ES CONCATENATER
168
SECONDARY CA PACKET ENCRYPTER
172
PSI MODIFIER
176
QAM MODULATOR
180
CABLE PLANT
184
SELECTIVE ENCRYPTION ENCODER

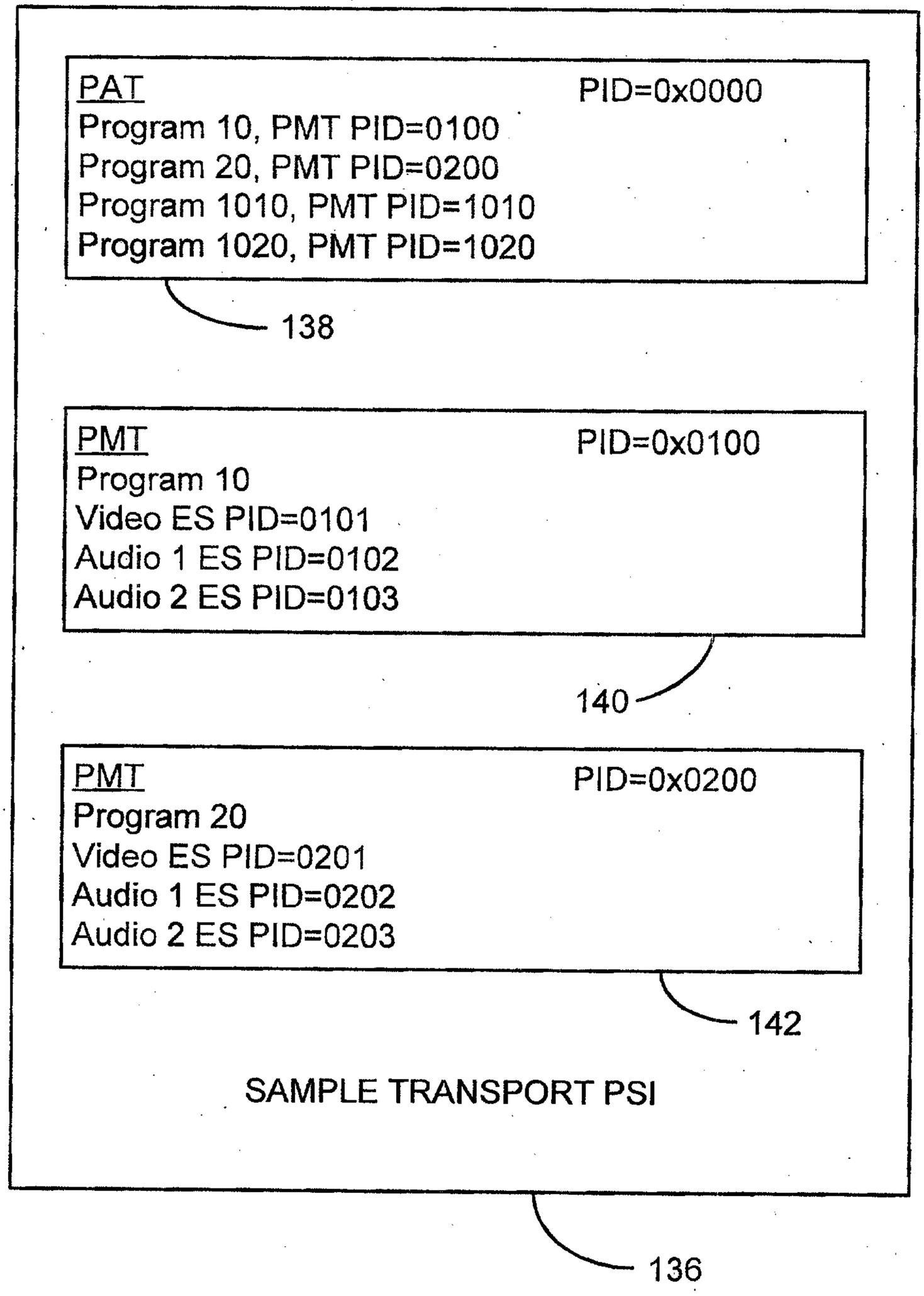

PAT
PID=0x0000
Program 10, PMT PID=0100
Program 20, PMT PID=0200
Program 1010, PMT PID=1010
Program 1020, PMT PID=1020
138
PMT
PID=0x0100
Program 10
Video ES PID=0101
Audio 1 ES PID=0102
Audio 2 ES PID=0103
140
PMT
PID=0x0200
Program 20
Video ES PID=0201
Audio 1 ES PID=0202
Audio 2 ES PID=0203
142
SAMPLE TRANSPORT PSI
136

FIG. 2

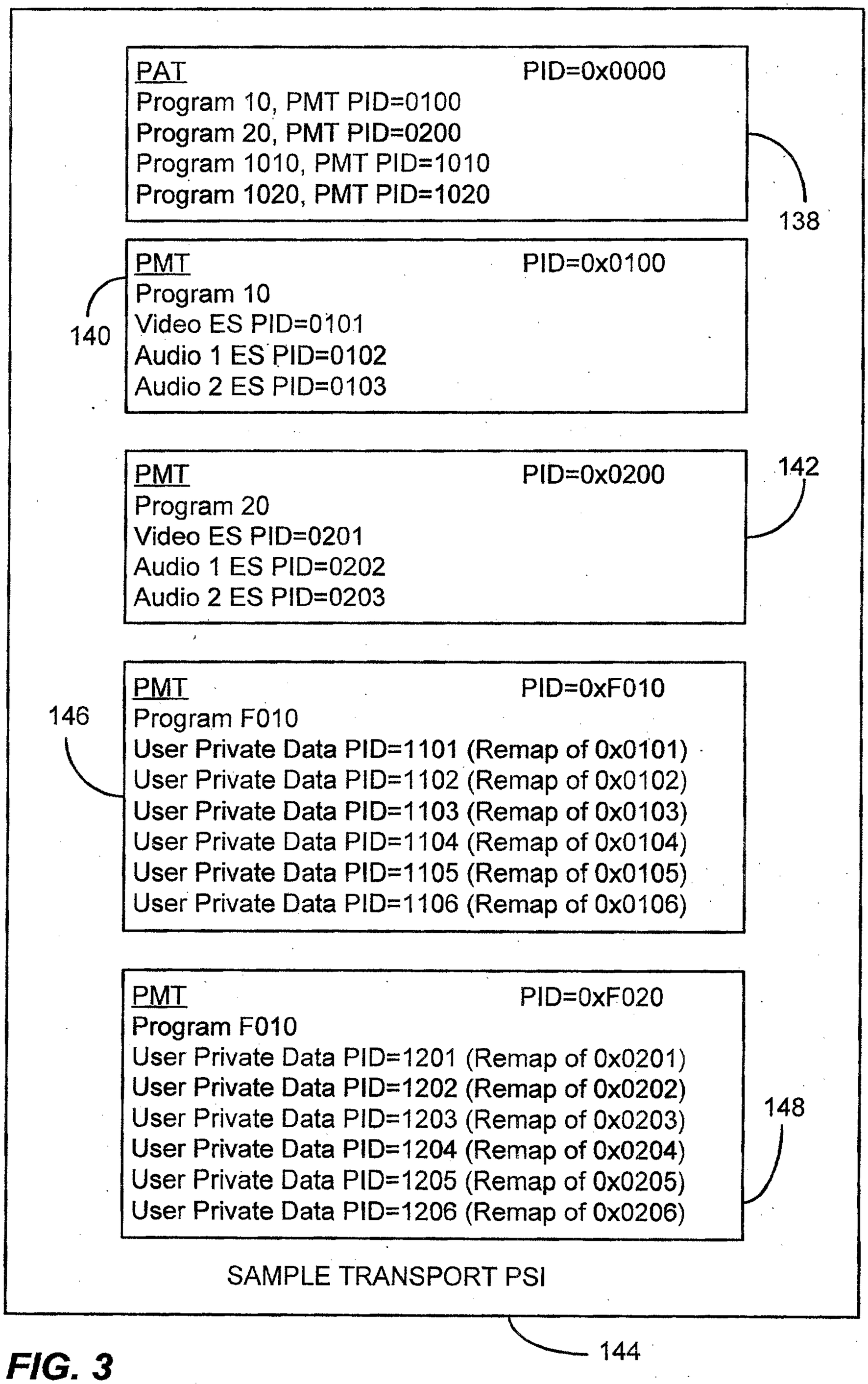

PAT
PID=0x0000
Program 10, PMT PID=0100
Program 20, PMT PID=0200
Program 1010, PMT PID=1010
Program 1020, PMT PID=1020
138
PMT
PID=0x0100
Program 10
Video ES PID=0101
Audio 1 ES PID=0102
Audio 2 ES PID=0103
140
PMT
PID=0x0200
Program 20
Video ES PID=0201
Audio 1 ES PID=0202
Audio 2 ES PID=0203
142
PMT
PID=0xF010
146
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)
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

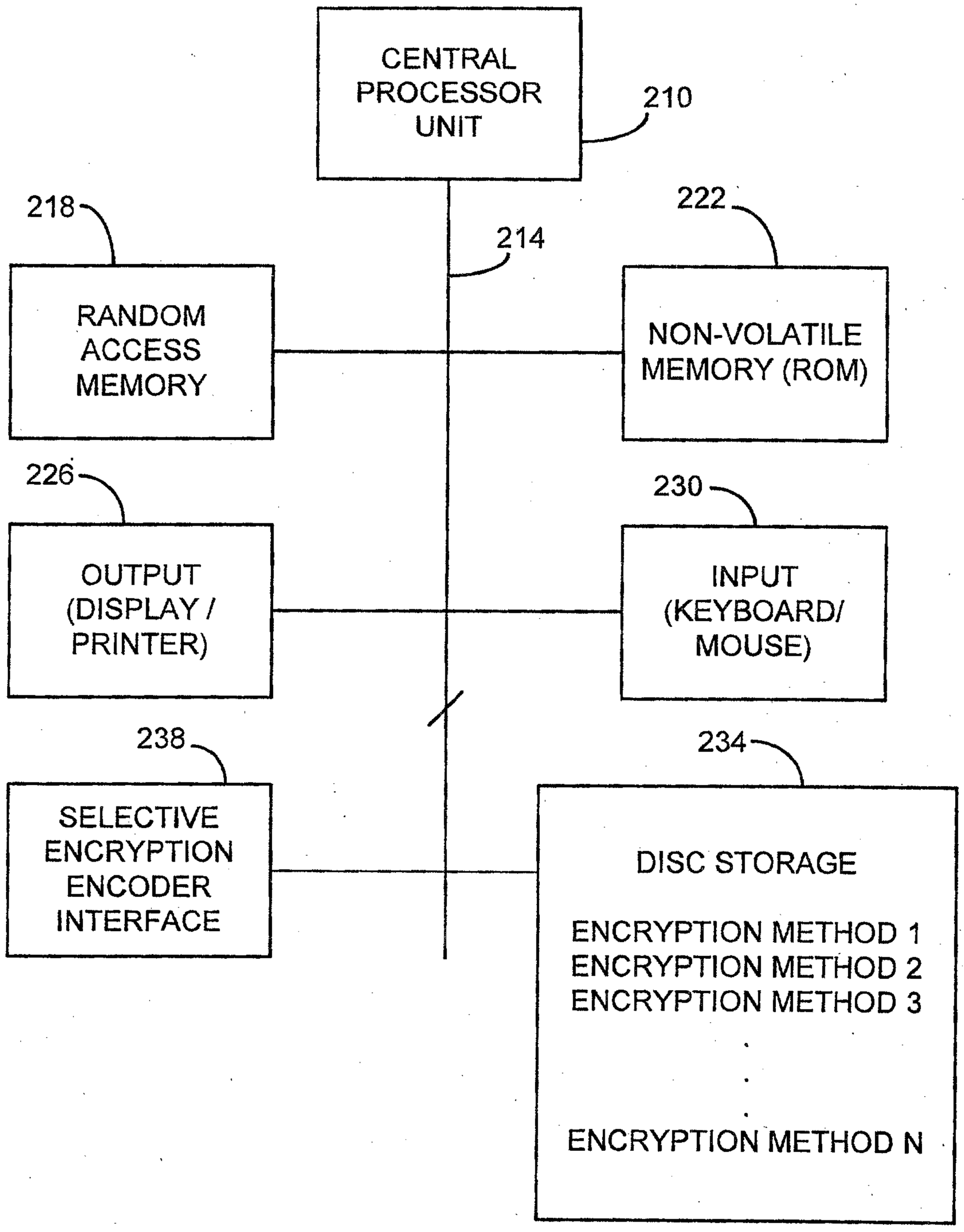

CENTRAL PROCESSOR UNIT
210
214
218
RANDOM ACCESS MEMORY
222
NON-VOLATILE MEMORY (ROM)
226
OUTPUT (DISPLAY / PRINTER)
230
INPUT (KEYBOARD/ MOUSE)
238
SELECTIVE ENCRYPTION ENCODER INTERFACE
234
DISC STORAGE
ENCRYPTION METHOD 1
ENCRYPTION METHOD 2
ENCRYPTION METHOD 3
ENCRYPTION METHOD N
100

FIG. 4

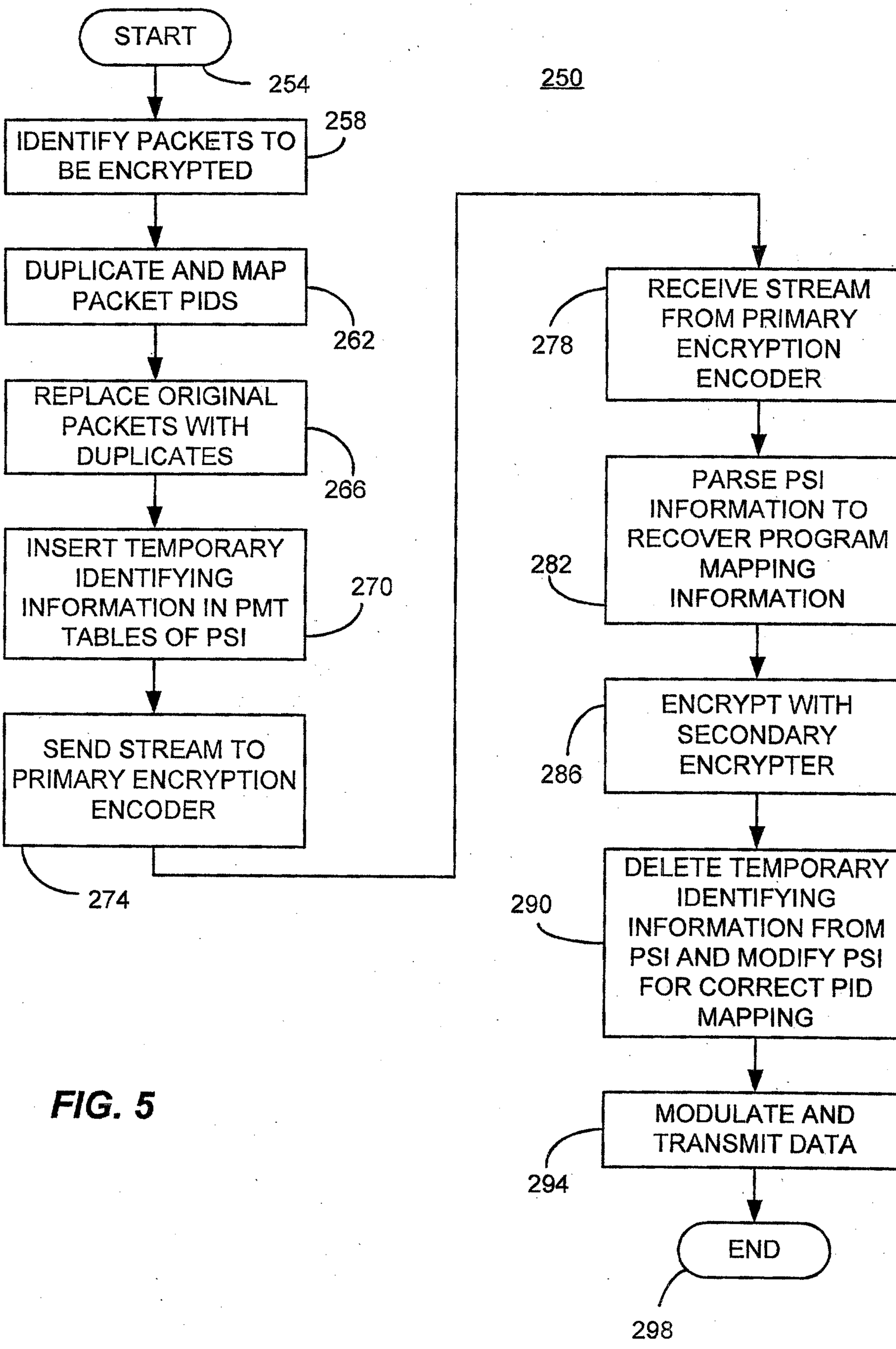
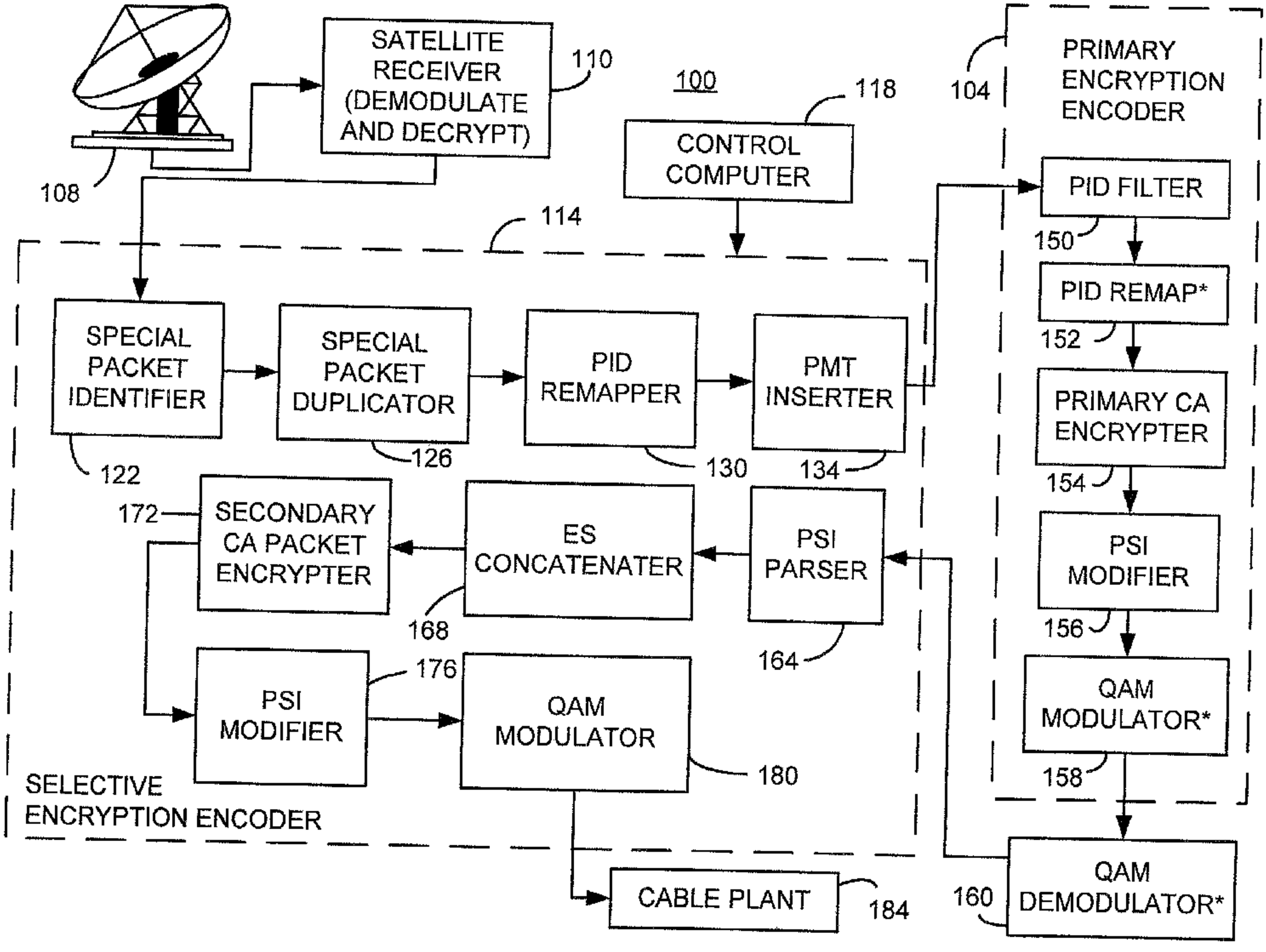


FIG. 5

Gowling Lafleur Henderson LLP


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