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

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2748539 C 2014/12/09

(11)(21) **2 748 539**

(12) BREVET CANADIEN / CANADIAN PATENT

(13) **C**

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

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

(45) **Date de délivrance/Issue Date:** 2014/12/09

(62) **Demande originale/Original Application:** 2 413 955

(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); 2002/04/16 (US60/372,855); 2002/09/09 (US60/409,675); 2002/10/18 (US10/274,084)

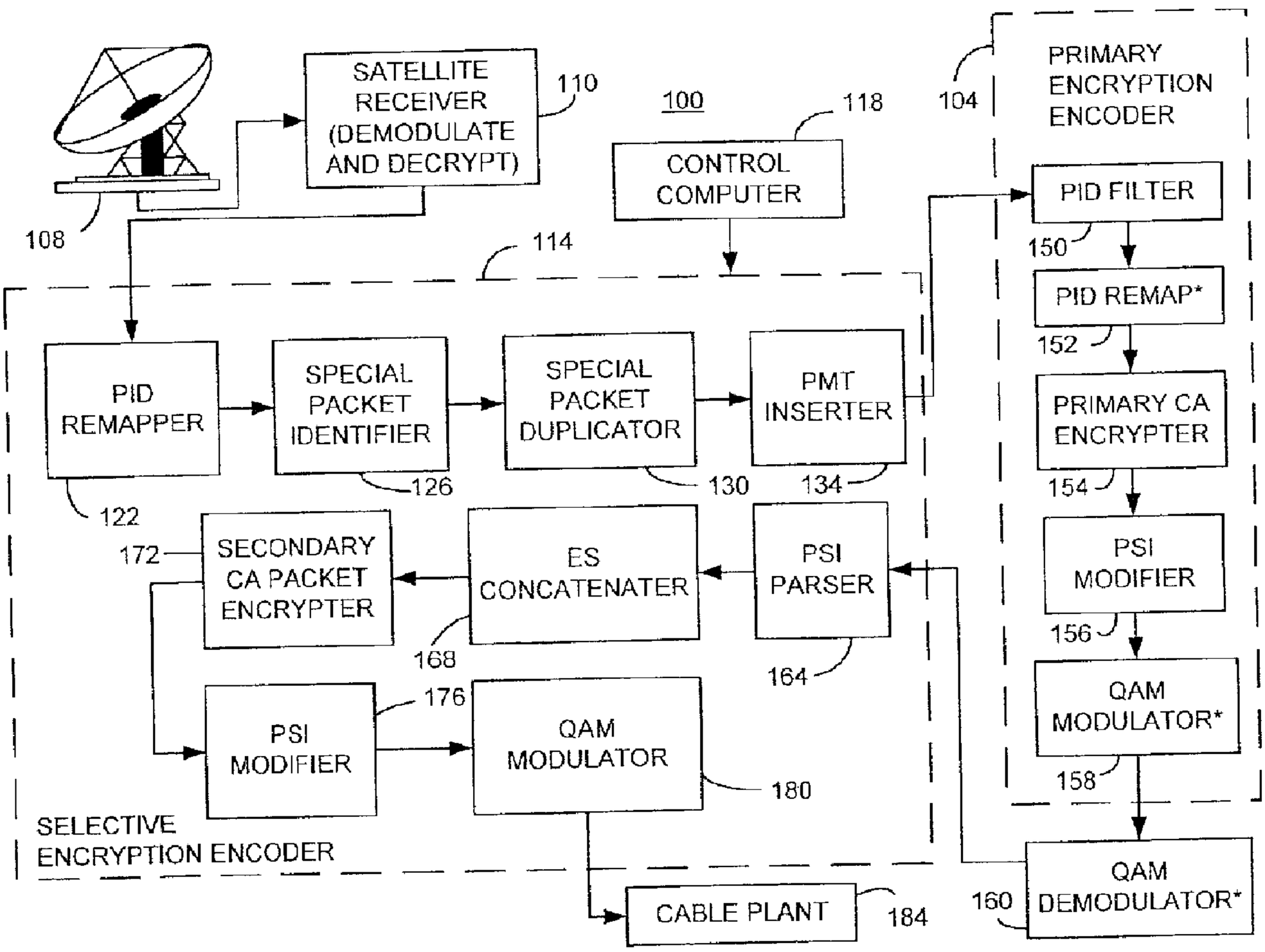
(51) **Cl.Int./Int.Cl.** ***H04N 21/4405*** (2011.01)

(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 : EMBROUILLAGE PARTIEL DE PROFIL MOAT A MASQUAGE DE TRANCHES**
(54) **Title: SLICE MASK AND MOAT PATTERN PARTIAL ENCRYPTION**



(57) **Abrégé/Abstract:**
A selective encryption encoder consistent with certain embodiments of the invention has vertical and/or horizontal stripes encrypted. In one embodiment, packets are examined in the digital video signal to identify a specified packet type, the specified

CA 2748539 C 2014/12/09

(11)(21) **2 748 539**

(13) **C**

(57) **Abrégé(suite)/Abstract(continued):**
packet type being both packets carrying intra-coded data representing a pattern of horizontal stripes across an image and packets carrying intra- coded data representing a pattern of vertical stripes across an image. The packets identified as being of the specified packet type are encrypted using a first encryption method to produce first encrypted packets. These first encrypted packets are then used to replace the unencrypted packets in the digital video signal to produce a partially encrypted video signal. The packets of the specified type can also be multiple encrypted and replaced in the data stream to produce a multiple encrypted video data stream.

ABSTRACT OF THE DISCLOSURE

A selective encryption encoder consistent with certain embodiments of the invention has vertical and/or horizontal stripes encrypted. In one embodiment, packets are examined in the digital video signal to identify a specified packet type, the specified packet type being both packets carrying intra-coded data representing a pattern of horizontal stripes across an image and packets carrying intra-coded data representing a pattern of vertical stripes across an image. The packets identified as being of the specified packet type are encrypted using a first encryption method to produce first encrypted packets. These first encrypted packets are then used to replace the unencrypted packets in the digital video signal to produce a partially encrypted video signal. The packets of the specified type can also be multiple encrypted and replaced in the data stream to produce a multiple encrypted video data stream.

SLICE MASK AND MOAT PATTERN PARTIAL ENCRYPTION

COPYRIGHT NOTICE

FIELD OF THE INVENTION

This invention relates generally to the field of encryption. More particularly, this invention relates to a 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 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.

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 video frame with encryption of odd numbered slices consistent with certain embodiments of the present invention.

FIGURE 7 illustrates a video frame with encryption of even numbered slices consistent with certain embodiments of the present invention.

FIGURE 8 illustrates a sequence of slice masks used to produce alternating odd and even numbered encrypted slices in a manner consistent with certain embodiments of the present invention.

FIGURE 9 illustrates a sequence of slice masks used to produce random encryption of frame slices in a manner consistent with certain embodiments of the present invention.

FIGURE 10 illustrates a pattern of horizontal moats and vertical motes forming a checkerboard pattern representing encrypted portions of video.

FIGURE 11 illustrates a television Set-top box that decrypts and decodes in a manner consistent with certain embodiments of the present invention.

FIGURE 12 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.

In accordance with certain embodiments of the present invention, a method of dual encrypting a digital video signal involves examining unencrypted packets of data in the digital video signal to identify at least one specified packet type, the specified packet type comprising packets of data as will be described hereinafter; encrypting packets identified as being of the specified packet type using a first encryption method to produce first encrypted packets; encrypting the packets identified as being of the specified packet type using a second encryption method to produce second encrypted packets; and replacing the unencrypted packets of the specified packet type with the first encrypted packets and the second encrypted packets in the digital video signal to produce a partially dual encrypted video signal.

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, for standard resolution, 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 standard definition 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).

Several techniques are described below for encryption of the selected data. In each case, for the current embodiment, it will be understood that selection of a particular type of information implies that the payload of a packet carrying such data is encrypted. However, in other environments, the data itself can be directly encrypted. Those skilled in the art will appreciate that such variations as well as others are possible without departing from the present invention. Moreover, those skilled in the art will appreciate that many variations and combinations of the encryption techniques described hereinafter can be devised and used singularly or in combination without departing from the present invention.

SLICE MASK ENCRYPTION

In accordance with one embodiment consistent with the invention referred to herein as "slice mask encryption", a different set of slice headers are encrypted from frame to frame. When a slice header is encrypted, the content for that slice is "frozen" on the screen, while content on adjoining slices is updated. This has the effect of breaking up the image on the screen. In certain embodiments, certain

slices can be encrypted more often than others to thus deny the decoder the ability to update the content in those slices.

One embodiment of slice mask encryption is illustrated in **FIGURE 6** and **FIGURE 7**. In **FIGURE 6**, a frame of video 270 is illustrated as 30 slices with each slice having a slice header and 33 macroblocks with alternating odd numbered slices being encrypted. In certain embodiments, the entire slice can be encrypted while in others, only key information in the slice is encrypted (e.g., the slice header, or slice header and first macroblock, or slice header and all intra-coded macroblocks in the slice). Frame 280 of **FIGURE 7**, by contrast, has all even numbered slices encrypted . As with frame 270, in certain embodiments, the entire slice can be encrypted while in others, only key information in the slice is encrypted (e.g., the slice header, or slice header and first macroblock, or slice header and all intra-coded macroblocks in the slice). In one embodiment, odd slice encryption as in frame 270 can be alternated with even slice encryption as in frame 280. In connection with the present embodiment, alternating video frames can be encrypted with odd or even slice encryption, with alternating video frames meaning every other frame or every other I, P or B frame.

The slice that is to be encrypted can be coded or represented using a slice mask as shown in **FIGURE 8**. The slice masks of **FIGURE 8** are simply binary one dimensional arrays that contain a 1 to indicate that a slice is to be encrypted and a 0 to indicate that the slice is to be unencrypted (or similar code designation). Thus, for example, slice masks 282, 284 and 286 represent odd slice encryption while slice masks 292 and 294 represent even slice encryption. Such arrays can be stored or generated, in one embodiment, for use in determining which slice is to be encrypted. These masks may be applied to I frames, I frames and P frames, or just P frames. Moreover, different masks may be used for I frames than P frames. In this illustrative example, fifteen packets/frame can be encrypted to encrypt the slice headers of the slices corresponding to 1 in the slice mask. This

results in a low percentage of the actual data in a video frame actually being encrypted.

The encryption of a slice can depend on any of the following:

- The location of the slice in the frame (with higher density towards the "active" part of the screen)
- Whether found in an I, P or B frame (higher to lower priority)
- # of patterns or masks used before they are repeated

Encrypting I frame slices eliminates anchor chrominance/luminance data used by the other types of frames. Encrypting P frame slices eliminates both anchor chrominance/luminance as well as motion vector data. Anchor chrominance/luminance can come in the form of scene changes, and if the content is Motorola encoded, then "progressive" I slices. The effect of Frame Mask encryption can be very effective. Experiments have shown that for a Motorola encoded program, encrypting only 3% of the packets can make it difficult to identify any objects in an image.

In variations of the embodiment described above, slice masks can be varied according to any suitable algorithm. For example, **FIGURE 9** illustrates random variation in the slice masks from frame to frame. Each of the slice masks 302, 304, 306, 308 and 310 is randomly (or equivalently, pseudo-randomly) generated so that a random array of slices is encrypted (e.g., by encryption of the payload of a packet containing the slice header) at each frame.

In another variation, it is noted that selected portions of the frame 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 a central area of the frame. More commonly, it is approximately an upper central portion of the frame of approximately half (say, one third to 3/4) of the overall area of the frame centered at approximately the center of the frame horizontally and approximately the tenth to fifteenth slice. In accordance with this variation, random or pseudo-random slices are encrypted (e.g., by encryption of packets containing the slice header) with a weighting function applied to cause the active region of the

image to be encrypted with greater frequency than other portions of the image. By way of example, and not limitation, assume that the center of the image is the active region. In this case, for example, a linear or a bell shaped weighting function can be applied to the random selection of slices to encrypt so that slices near the center are more frequently encrypted than those at the top or bottom of the image. In another example, assume that slices 8-22 of a 30 slice frame are deemed to bound the active region. Slices can then be randomly selected in each frame for encryption with a multiplication factor used to increase the likelihood that slices 8-22 will be encrypted. For example, those slices can be made twice or three times as likely to be encrypted as other slices. Equivalently, slices 1-7 and 23-30 can be made less likely to be encrypted. Any suitable pattern of macroblocks within a slice can be encrypted in order to encrypt the slice. Other variations will occur to those skilled in the art upon consideration of the present teachings.

MOAT PATTERN ENCRYPTION

The above slice mask encryption technique can be viewed as creating horizontal "moats" of encrypted information in the video frame, with each moat corresponding to a single slice in width. The moat width can be varied by encrypting multiple adjacent slices. In a similar manner, vertical "moats" can be generated by selecting macroblocks of data to be encrypted in a particular frame of data. This is depicted in **FIGURE 10** by an array of binary data that represents encryption of slices 1-5,11-15 and 21-25 to create three horizontal moats 322, 324 and 326 respectively (each being 5 slices in width) in a video frame. This array may be referred to as a horizontal moat mask or slice mask. In a similar manner, an array of binary data 330 represents a vertical moat mask for encryption of macroblocks numbered 1-3, 7-9, 13-15, 19-21, 24-27 and 31-33 to create six vertical moats 332, 334, 336, 338, 340 and 342 respectively (each being three macroblocks in width). Of course, other patterns of horizontal moats can also be generated, for example, with greater or lesser density, greater or lesser moat width,

greater emphasis on an active portion of the image or randomly generated moats, without departing from the present invention.

To create the moats in accordance with preferred embodiments, intra-coded macroblocks in the vertical and horizontal stripes through the image are encrypted. By encrypting the intra-coded macroblocks, inter-coded macroblocks are left without reference data and become meaningless, thus effectively scrambling the video image. In other embodiments, the horizontal stripes can be encrypted by any suitable technique including, but not limited to, encryption of the slice header, encryption of the slice header plus the first macroblock, encryption of all macroblocks in the slice or any other suitable technique. Similarly, the vertical stripes can be encrypted by encryption of intra-coded macroblocks or all macroblocks in the stripe without departing from the invention.

It should be noted that to encrypt certain macroblocks generally suggests that the payload of a packet carrying the macroblock is encrypted. This further implies that, in fact, more data on one side, the other or both of the target macroblock will also be encrypted. This results in even greater amounts of data being encrypted and thus greater encryption security.

In one embodiment of this encryption mode, it is assumed that the first macroblock with absolute DC luminance and chrominance information is encrypted. Each macroblock after that is encrypted differentially from the macroblock to the left to produce the horizontal stripes.

By breaking up the image up into a checker board pattern as illustrated, the vertical moats prevent the direct calculation of all the macroblocks on a slice with one good known value anywhere on the slice. Although a known value may be obtained by correlation of macroblocks from previous frames of the same slice or clear intracoded macroblocks from another part of the slice, this is generally inadequate to provide an effective hack to the encryption method. By use of the checkerboard pattern of encryption, the correlated macroblock would only "fix" the macroblocks in the particular checkerboard square in which that macroblock is located ... not the entire slice. Thus, the vertical moat creates a discontinuity which

increases distortion in the image.

Likewise for horizontal encrypted moats. This encryption technique prevents intracoded macroblocks from slices below or above the encrypted slice from being used to correct information in macroblocks above or below. The horizontal stripe or moat creates a discontinuity that disrupts a hacker's ability to obtain enough reference data to effectively decrypt the image. This checker board pattern produces a bandwidth savings in a dual or multiple encryption scenario which is substantially reduced compared with 100% encryption of the slice.

Multiple combinations of the encryption techniques are possible to produce encryption that has varying bandwidth requirements, varying levels of security and varying complexity. Such encryption techniques can be selected by control computer 118 in accordance with the needs of the MSO. The above-described encryption techniques can provide several additional choices to enrich a pallette of encryption techniques that can thus be selected by control computer 118 to vary the encryption making hacking more difficult.

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 11** 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 11** can be implemented and/or controlled as program code running on a programmed processor, with the code being stored on an electronic storage medium.

FIGURE 12 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 containing data representing vertical and/or horizontal stripes in a 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 television set-top box, comprising:

a receiver receiving a digital television signal comprising:

a plurality of unencrypted packets; and

a plurality of encrypted packets, wherein certain of the encrypted packets represent at least one of a pattern of horizontal stripes across an image and a pattern of vertical stripes across the image;

a decrypter that decrypts the encrypted packets; and

a decoder that decodes the unencrypted packets and the decrypted packets to produce a signal suitable for play on a television set.

2. A television set-top box, comprising:

a receiver receiving a digital television signal comprising:

a plurality of unencrypted packets;

a plurality of encrypted packets, wherein certain of the encrypted packets represent at least one of a pattern of horizontal stripes across an image and a pattern of vertical stripes across the image; and wherein the plurality of encrypted packets comprise a plurality of pairs of redundant packets containing redundant information encrypted, where one of each pair is encrypted under a first encryption method and the other of the pair is encrypted using a second encryption method:

a decrypter that decrypts the encrypted packets encrypted under the first encryption method; and

a decoder that decodes the unencrypted packets and the decrypted packets to produce a signal suitable for play on a television set.

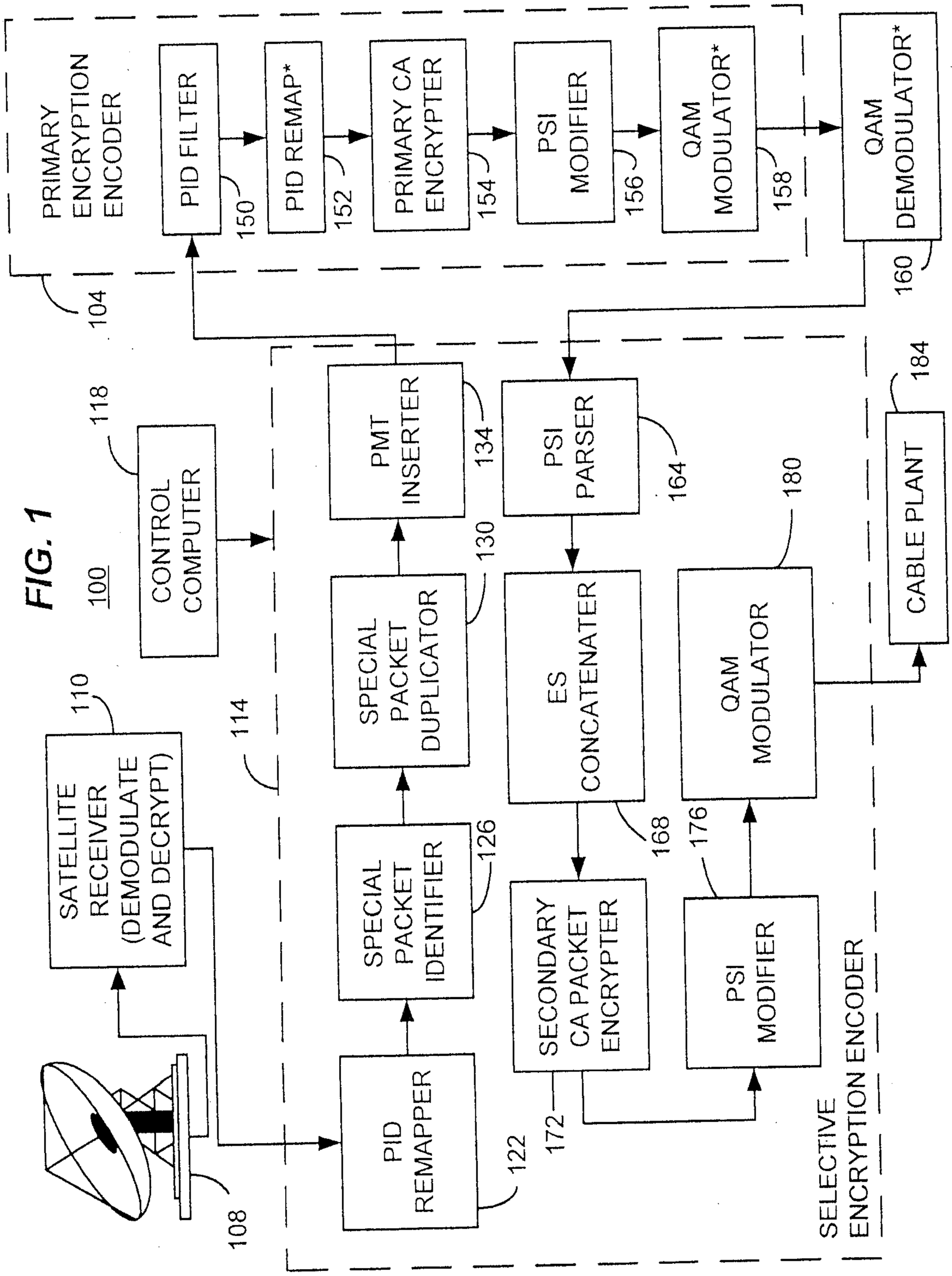


FIG. 1
100
SATELLITE RECEIVER (DEMODULATE AND DECRYPT)
110
CONTROL COMPUTER
118
PRIMARY ENCRYPTION ENCODER
104
PID FILTER
150
PID REMAP*
152
PRIMARY CA ENCRYPTER
154
PSI MODIFIER
156
QAM MODULATOR*
158
QAM DEMODULATOR*
160
CABLE PLANT
184
PMT INSERTER
134
PSI PARSER
164
180
SPECIAL PACKET DUPLICATOR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

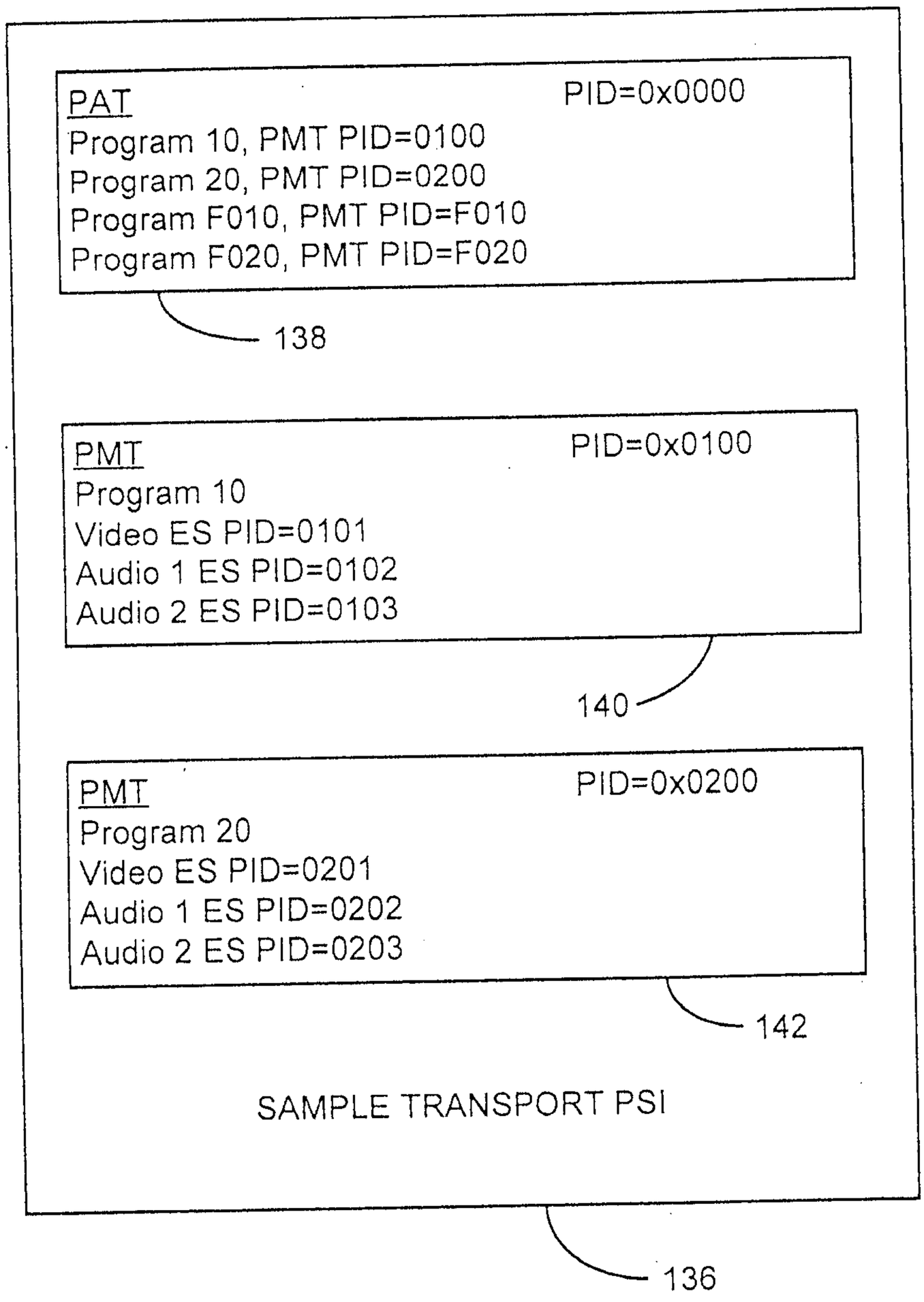

PAT
PID=0x0000
Program 10, PMT PID=0100
Program 20, PMT PID=0200
Program F010, PMT PID=F010
Program F020, PMT PID=F020
138
PMT
PID=0x0100
Program 10
Video ES PID=0101
Audio 1 ES PID=0102
Audio 2 ES PID=0103
140
PMT
PID=0x0200
Program 20
Video ES PID=0201
Audio 1 ES PID=0202
Audio 2 ES PID=0203
142
SAMPLE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

FIG. 2

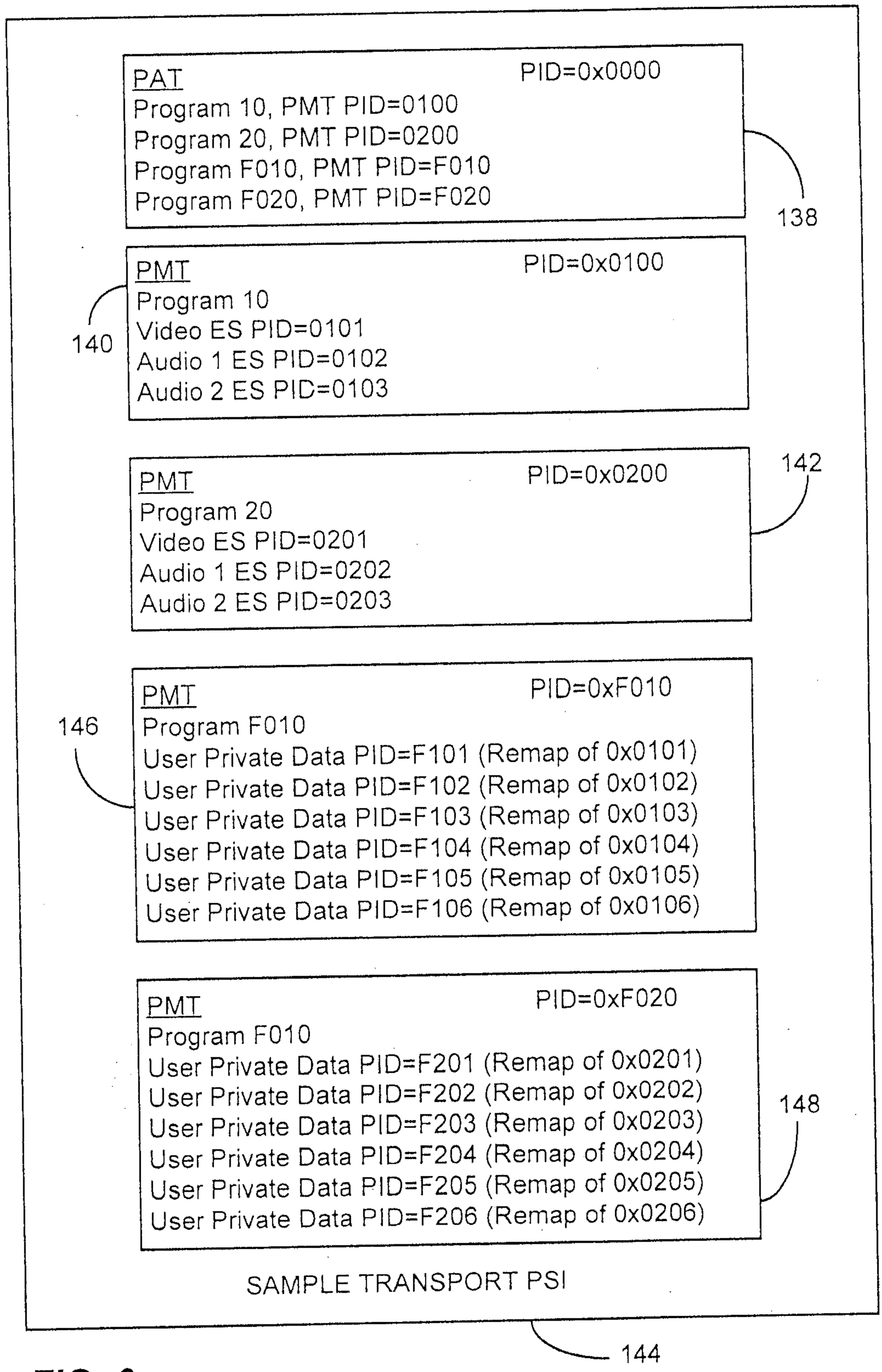

PAT
PID=0x0000
Program 10, PMT PID=0100
Program 20, PMT PID=0200
Program F010, PMT PID=F010
Program F020, PMT PID=F020
138
PMT
PID=0x0100
Program 10
Video ES PID=0101
Audio 1 ES PID=0102
Audio 2 ES PID=0103
140
PMT
PID=0x0200
Program 20
Video ES PID=0201
Audio 1 ES PID=0202
Audio 2 ES PID=0203
142
PMT
PID=0xF010
Program F010
User Private Data PID=F101 (Remap of 0x0101)
User Private Data PID=F102 (Remap of 0x0102)
User Private Data PID=F103 (Remap of 0x0103)
User Private Data PID=F104 (Remap of 0x0104)
User Private Data PID=F105 (Remap of 0x0105)
User Private Data PID=F106 (Remap of 0x0106)
146
PMT
PID=0xF020
Program F010
User Private Data PID=F201 (Remap of 0x0201)
User Private Data PID=F202 (Remap of 0x0202)
User Private Data PID=F203 (Remap of 0x0203)
User Private Data PID=F204 (Remap of 0x0204)
User Private Data PID=F205 (Remap of 0x0205)
User Private Data PID=F206 (Remap of 0x0206)
148
SAMPLE TRANSPORT PSI
144

FIG. 3

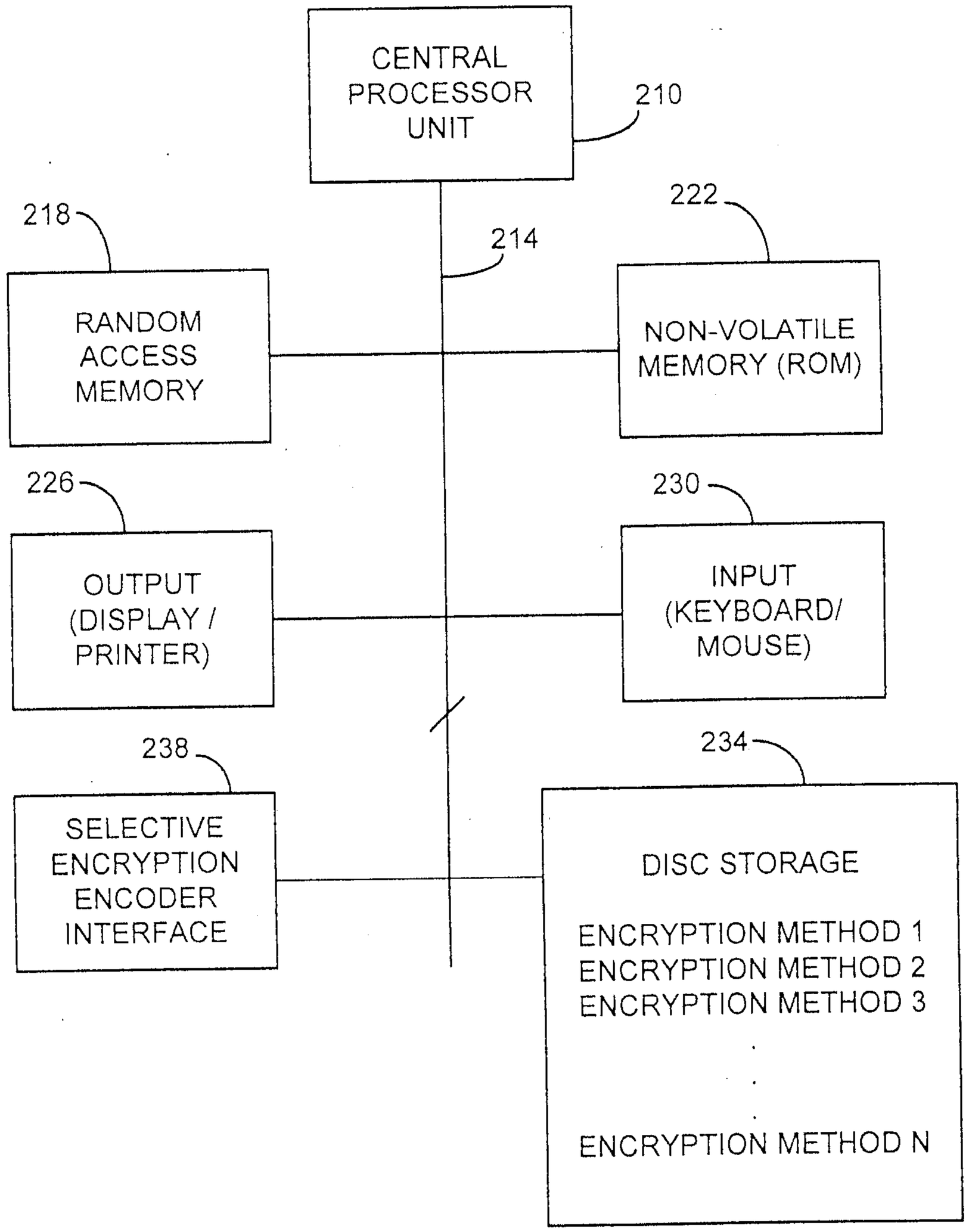

CENTRAL PROCESSOR UNIT
210
214
218
RANDOM ACCESS MEMORY
222
NON-VOLATILE MEMORY (ROM)
226
OUTPUT (DISPLAY / PRINTER)
230
INPUT (KEYBOARD/ MOUSE)
238
SELECTIVE ENCRYPTION ENCODER INTERFACE
234
DISC STORAGE
ENCRYPTION METHOD 1
ENCRYPTION METHOD 2
ENCRYPTION METHOD 3
ENCRYPTION METHOD N
100

FIG. 4

250

FIG. 5

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

CA 02748539 2011-08-04

FIG. 6

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

270

FIG. 7

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

280

FIG. 8

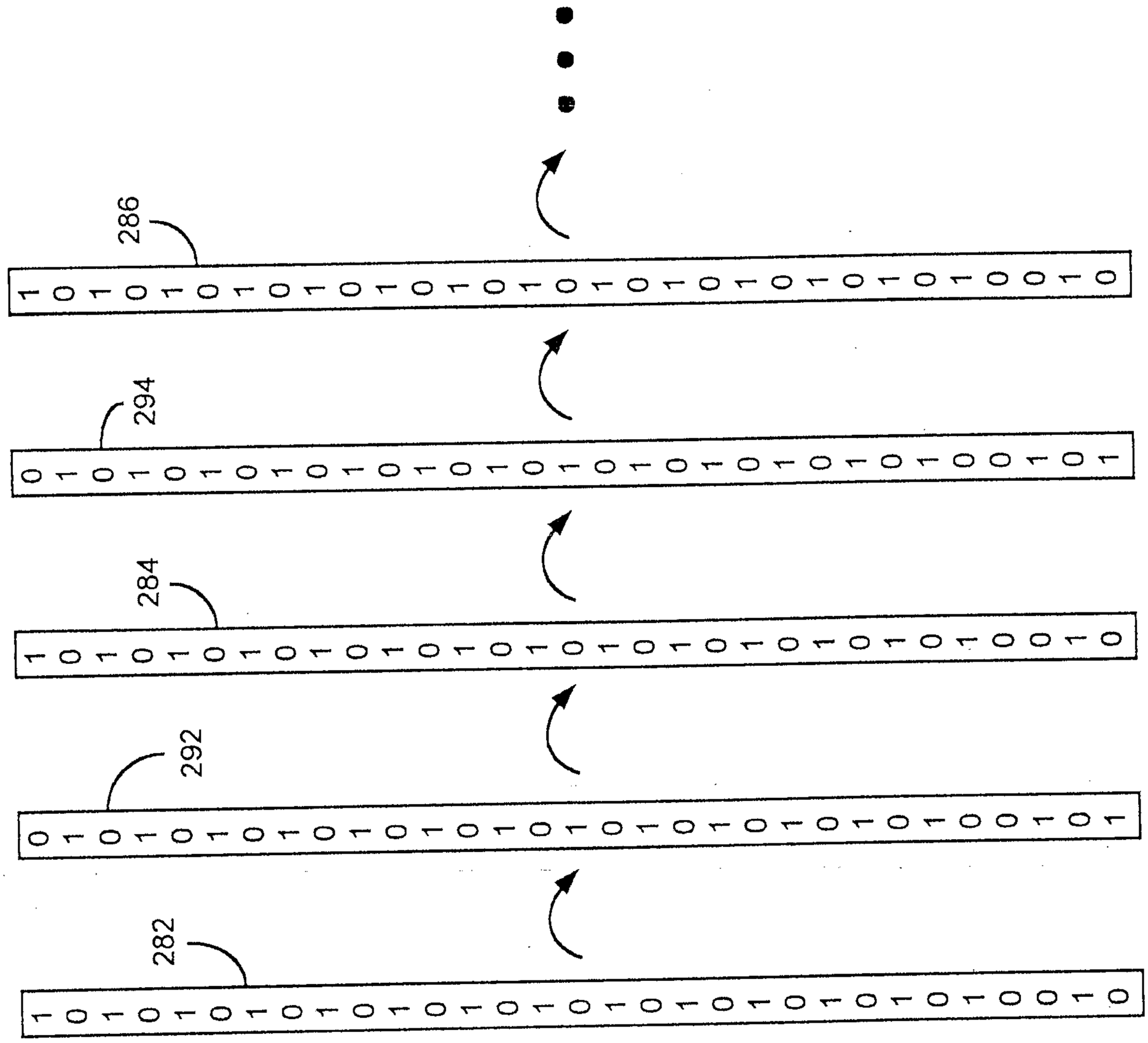


FIG. 9

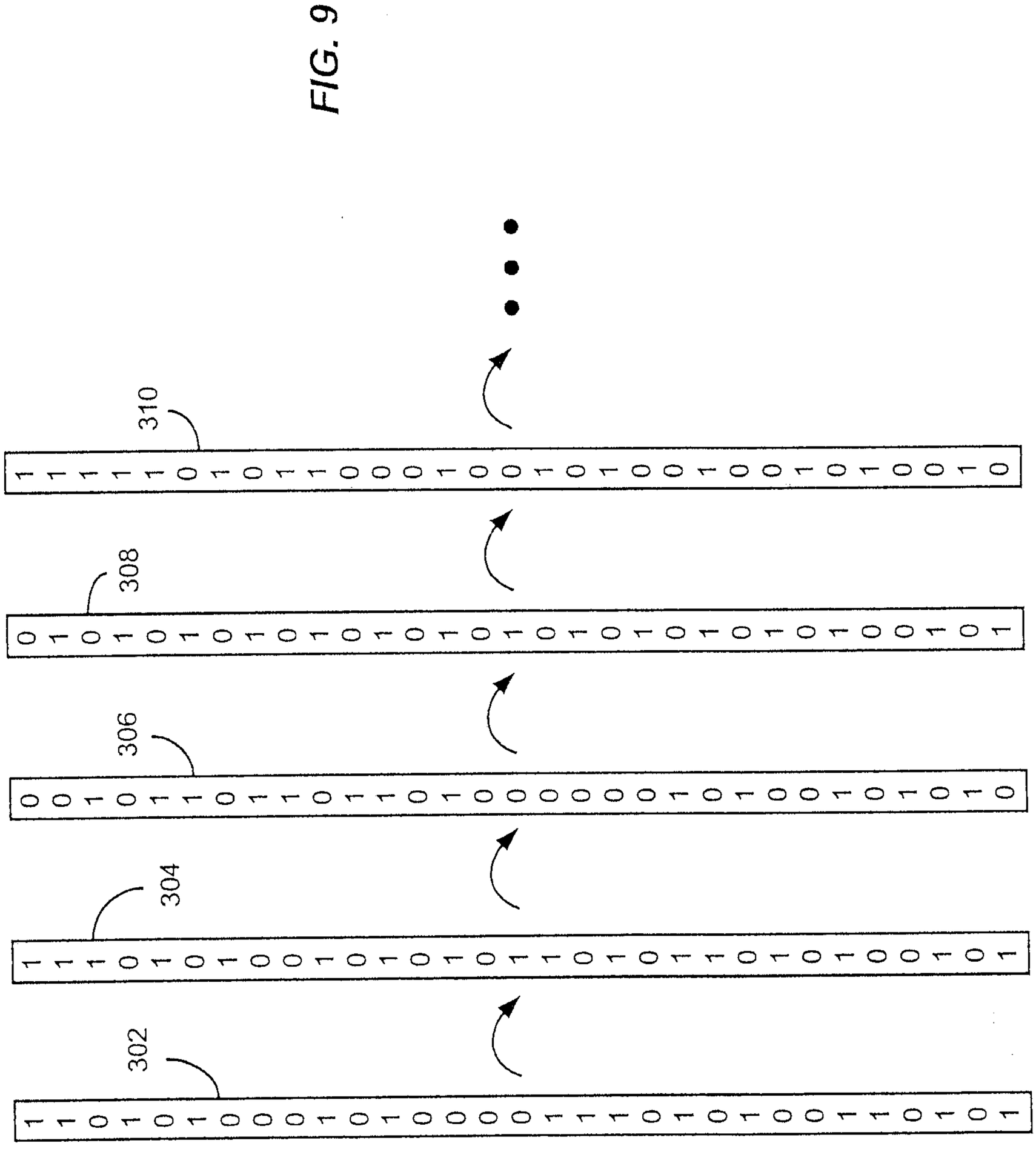
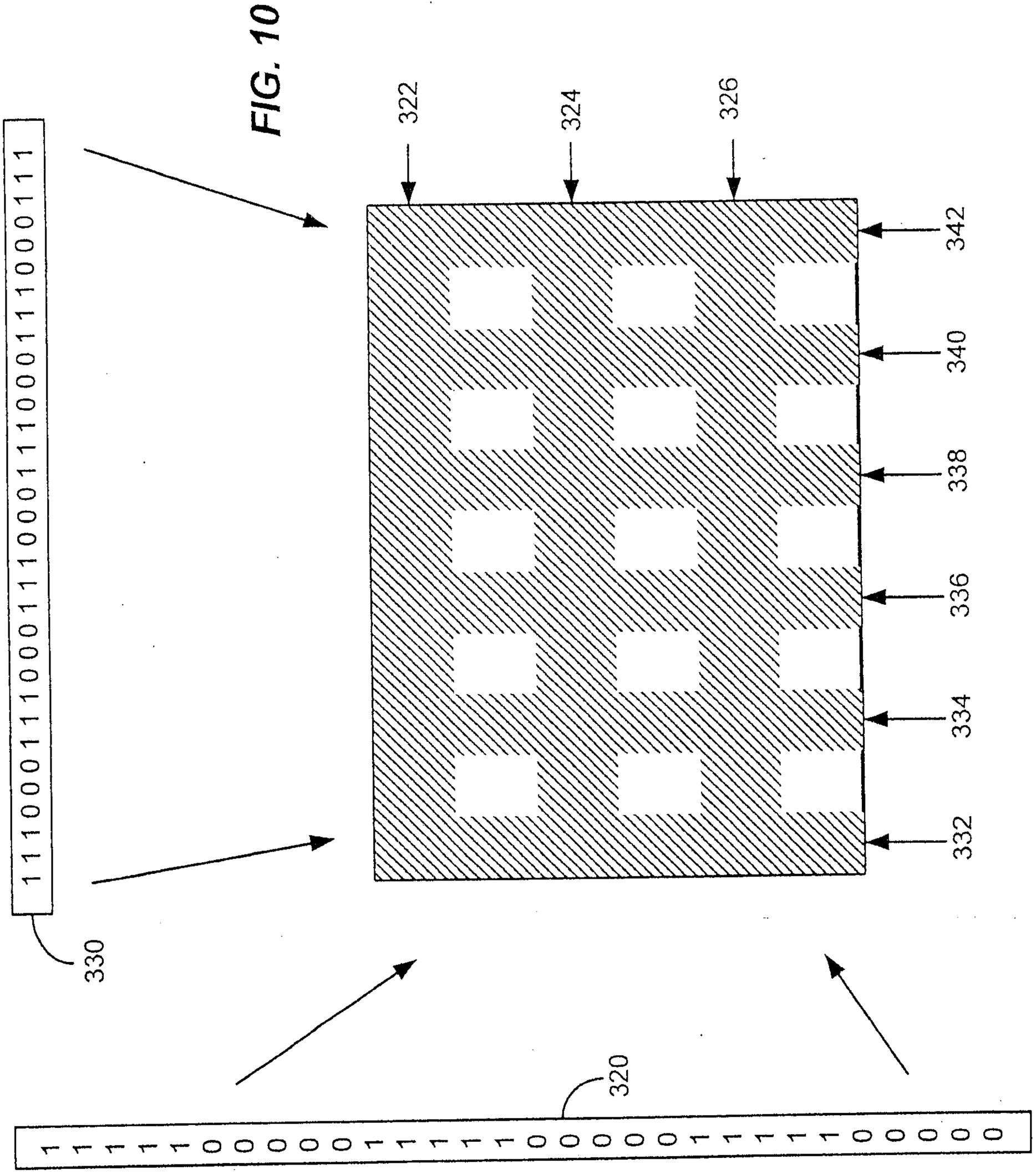


FIG. 1


322
324
326
342
340
338
336
334
332
1110001110001110001111
330
320
111111000001111100000

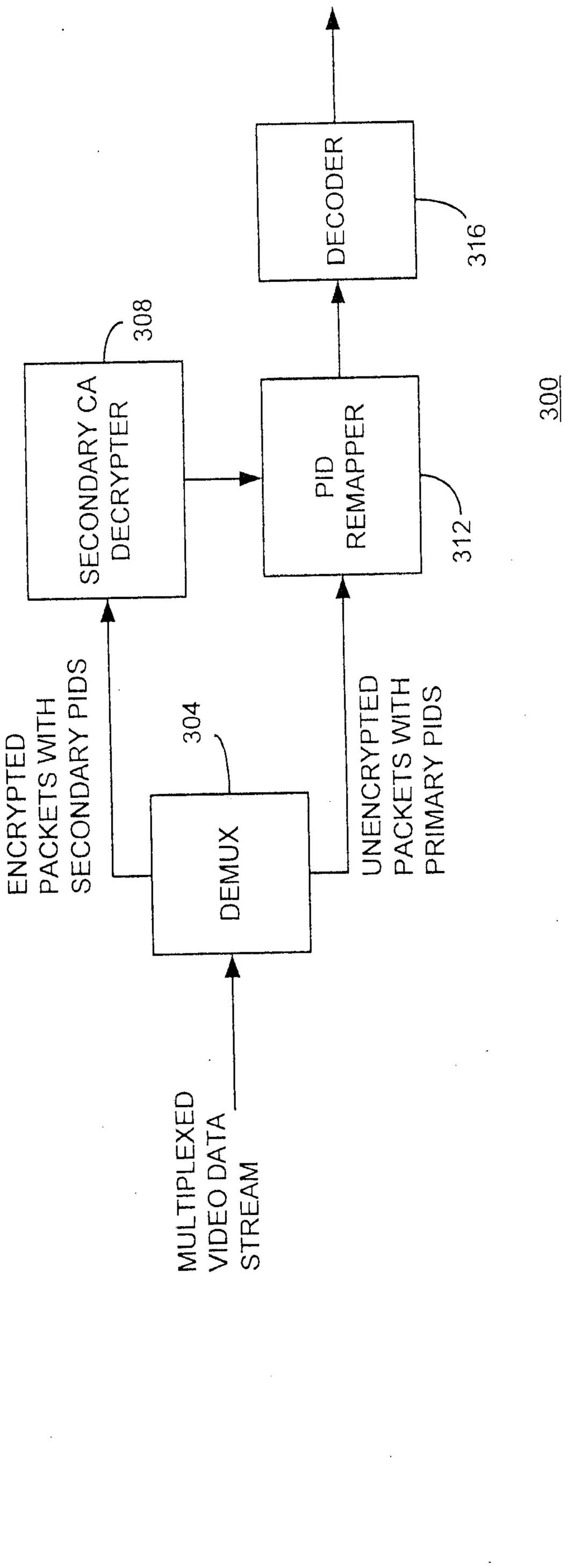

MULTIPLEXED
VIDEO DATA
STREAM
304
DEMUX
ENCRYPTED
PACKETS WITH
SECONDARY PIDS
UNENCRYPTED
PACKETS WITH
PRIMARY PIDS
SECONDARY CA
DECRYPTER
308
PID
REMAPPER
312
DECODER
316
300

FIG. 11

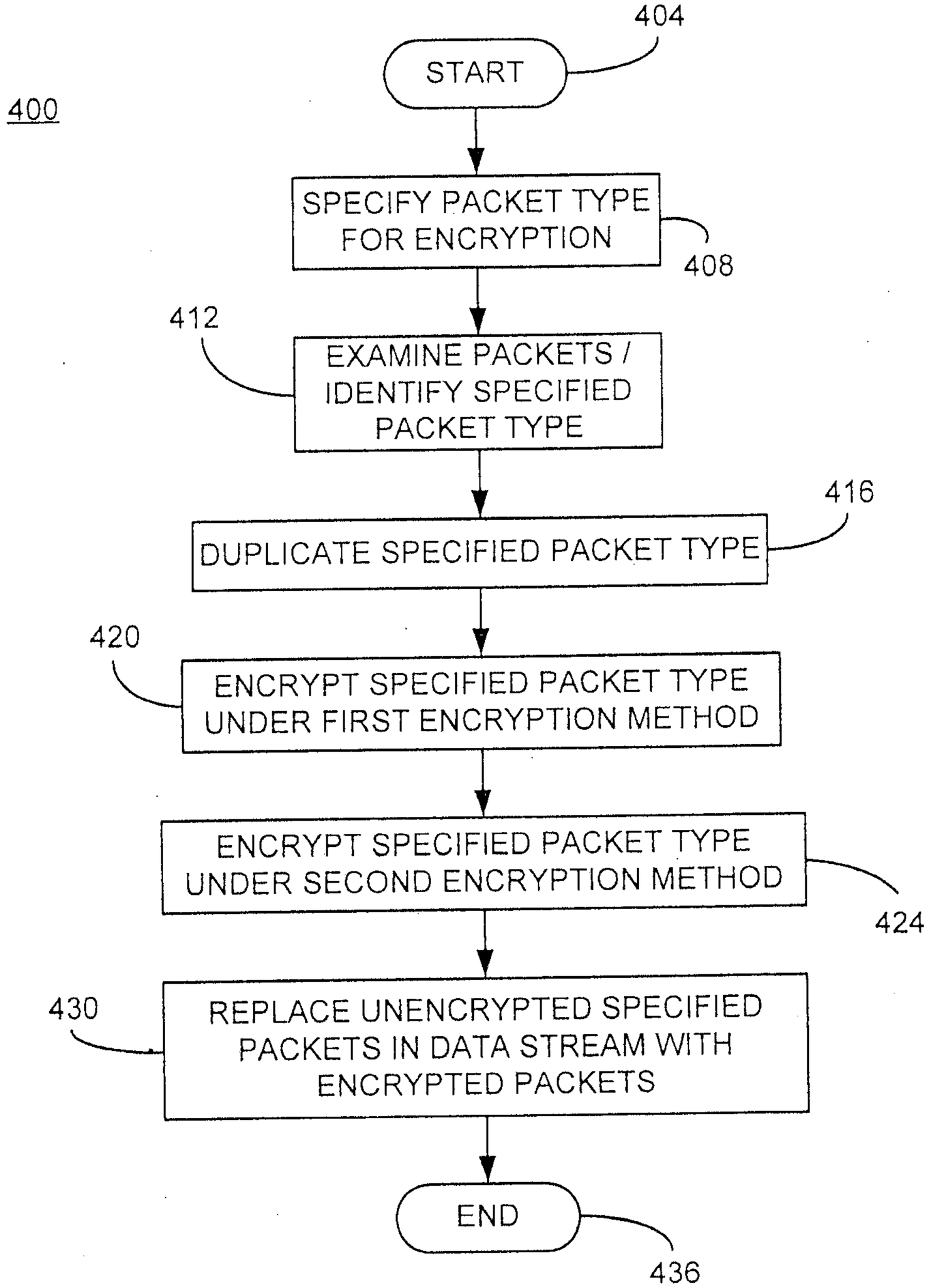
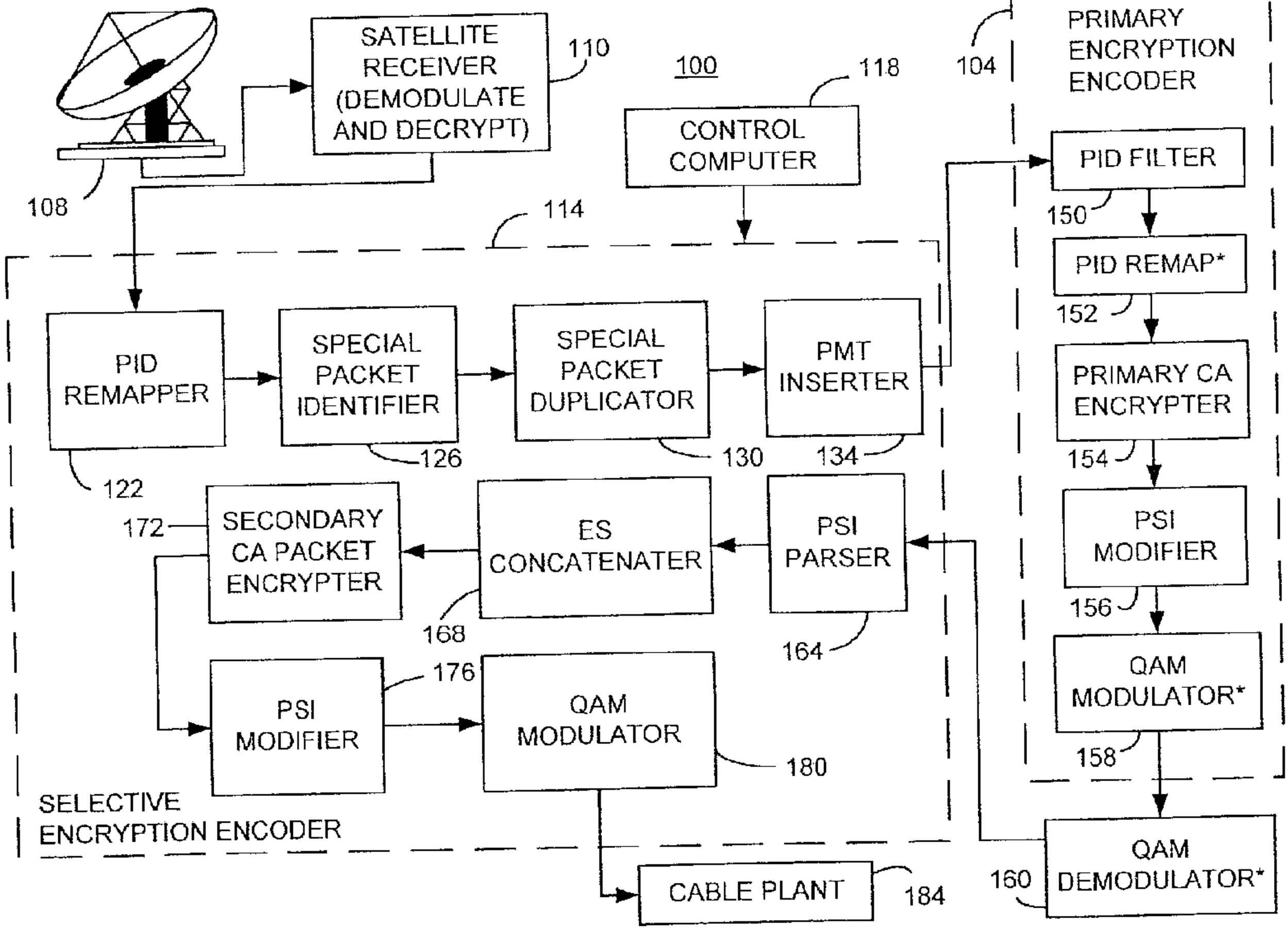

404
400
START
SPECIFY PACKET TYPE FOR ENCRYPTION
408
412
EXAMINE PACKETS / IDENTIFY SPECIFIED PACKET TYPE
416
DUPLICATE SPECIFIED PACKET TYPE
420
ENCRYPT SPECIFIED PACKET TYPE UNDER FIRST ENCRYPTION METHOD
ENCRYPT SPECIFIED PACKET TYPE UNDER SECOND ENCRYPTION METHOD
424
430
REPLACE UNENCRYPTED SPECIFIED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

FIG. 12


SATELLITE RECEIVER (DEMODULATE AND DECRYPT)
110
100
CONTROL COMPUTER
118
PRIMARY ENCRYPTION ENCODER
104
108
114
PID FILTER
150
PID REMAP*
152
PID REMAPPER
SPECIAL PACKET IDENTIFIER
SPECIAL PACKET DUPLICATOR
PMT INSERTER
PRIMARY CA ENCRYPTER
154
126
130
134
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
CABLE PLANT
184
160
QAM DEMODULATOR*