

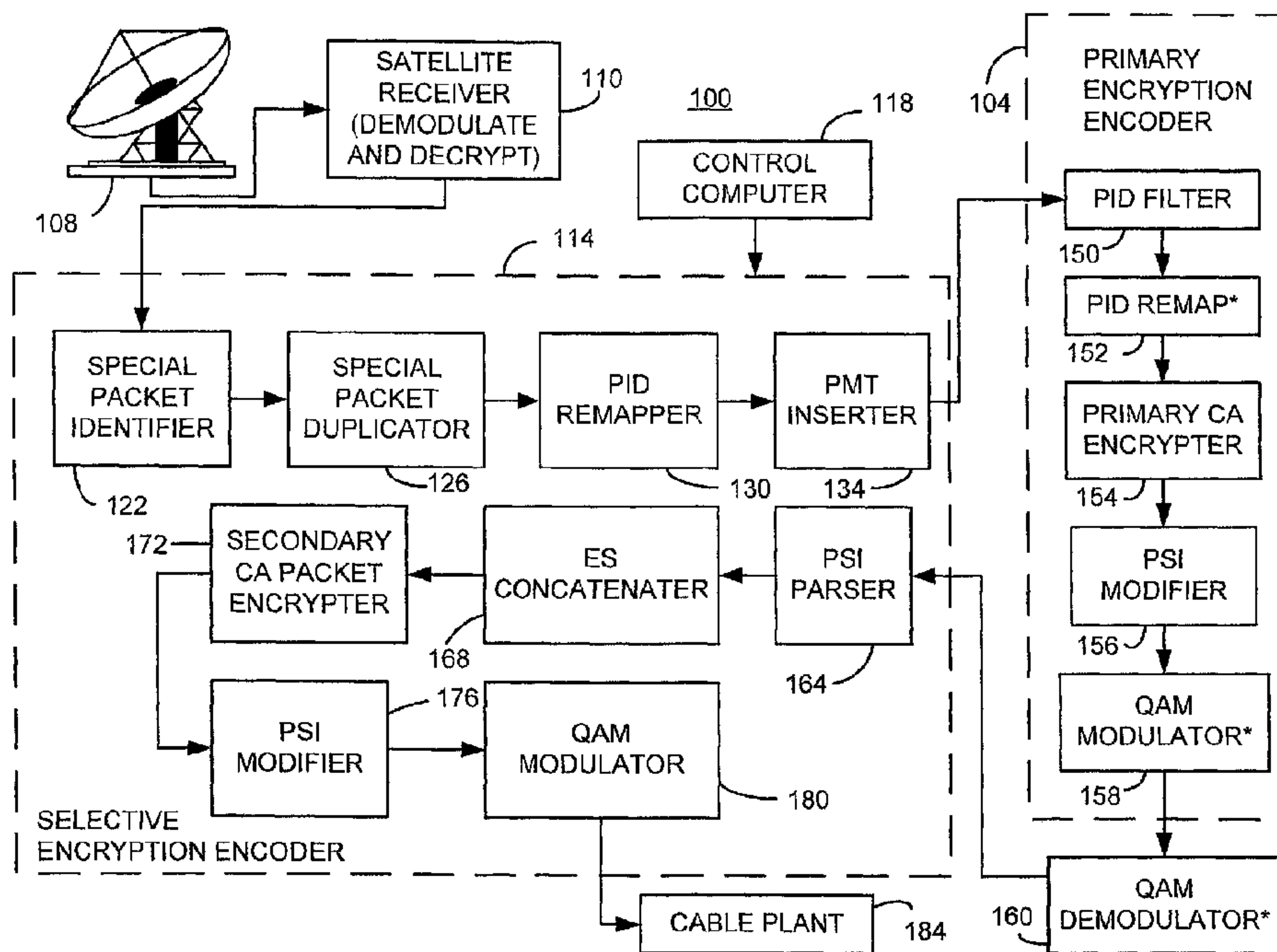


(22) Date de dépôt/Filing Date: 2002/12/10
 (41) Mise à la disp. pub./Open to Public Insp.: 2003/07/02
 (45) Date de délivrance/Issue Date: 2014/09/16
 (62) Demande originale/Original Application: 2 413 980
 (30) Priorités/Priorities: 2002/01/02 (US10/037,499);
 2002/01/02 (US10/037,498); 2002/01/02 (US10/038,217);
 2002/01/02 (US10/038,032); 2002/01/02 (US10/037,914);
 2002/01/24 (US60/351,828); 2002/02/08 (US60/355,326);
 2002/04/04 (US60/370,427); 2002/09/09 (US60/409,675);
 2002/10/18 (US10/273,905)

(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 : CRYPTAGE PARTIEL DOUBLE BASE SUR UNE TRANCHE DE VIDEO ET UNE REGION ACTIVE DE L'IMAGE

(54) Title: VIDEO SLICE AND ACTIVE REGION BASED DUAL PARTIAL ENCRYPTION



(57) Abrégé/Abstract:

A selective encryption encoder and method of dual selective encryption. The selective encryption encoder has a packet identifier that identifies packets of at least one specified packet type, the at least one specified packet type being any of a plurality of packet types including packets containing a video slice headers or packets carrying data appearing in an active area of the image. A packet duplicator duplicates the identified packets to produce first and second sets of the identified packets. The packets are sent to and from a primary encryption encoder to encrypt the first set of identified packets under a first encryption method. A secondary encrypter encrypts the second set of identified packets under a second encryption method.

ABSTRACT OF THE DISCLOSURE

1
2
3 A selective encryption encoder and method of dual selective encryption. The
4 selective encryption encoder has a packet identifier that identifies packets of at
5 least one specified packet type, the at least one specified packet type being any
6 of a plurality of packet types including packets containing a video slice headers or
7 packets carrying data appearing in an active area of the image. A packet duplicator
8 duplicates the identified packets to produce first and second sets of the identified
9 packets. The packets are sent to and from a primary encryption encoder to encrypt
10 the first set of identified packets under a first encryption method. A secondary
11 encrypter encrypts the second set of identified packets under a second encryption
12 method.
13
14

1
2
3 **VIDEO SLICE AND ACTIVE REGION BASED DUAL PARTIAL ENCRYPTION**
4
5
6

7 **COPYRIGHT NOTICE**

8 A portion of the disclosure of this patent document contains material which
9 is subject to copyright protection. The copyright owner has no objection to the
10 facsimile reproduction of the patent document or the patent disclosure, as it
11 appears in the Patent and Trademark Office patent file or records, but otherwise
12 reserves all copyright rights whatsoever.
13

14 **FIELD OF THE INVENTION**

15 This invention relates generally to the field of encryption. More particularly,
16 this invention relates to a dual encryption method and apparatus particularly useful
17 for encrypting packetized video content such as that provided by cable and satellite
18 television systems.
19

20 **BACKGROUND OF THE INVENTION**

21 The above-referenced patent document describe
22 inventions relating to various aspects of methods generally referred to herein as
23 partial encryption or selective encryption. More particularly, systems are described
24 therein wherein selected portions of a particular selection of digital content are
25 encrypted using two (or more) encryption techniques while other portions of the
26 content are left unencrypted. By properly selecting the portions to be encrypted, the
27 content can effectively be encrypted for use under multiple decryption systems
28 without the necessity of encryption of the entire selection of content. In some
29 embodiments, only a few percent of data overhead is needed to effectively encrypt

1 the content using multiple encryption systems. This results in a cable or satellite
2 system being able to utilize Set-top boxes or other implementations of conditional
3 access (CA) receivers from multiple manufacturers in a single system - thus freeing
4 the cable or satellite company to competitively shop for providers of Set-top boxes.
5

6 BRIEF DESCRIPTION OF THE DRAWINGS

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

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

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

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

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

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

23 **FIGURE 6** illustrates slice header encryption consistent with certain
24 embodiments of the present invention.

25 **FIGURE 7** illustrates slice header encryption in addition to encryption of the
26 first macroblock in each slice consistent with certain embodiments of the present
27 invention.

28 **FIGURE 8** illustrates active region encryption consistent with certain
29 embodiments of the present invention.

1 **FIGURE 9** illustrates packetized active region encryption consistent with
2 certain embodiments of the present invention.

3 **FIGURE 10** illustrates active slice encryption consistent with certain
4 embodiments of the present invention.

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

7 **FIGURE 12** is a flow chart broadly illustrating an encryption process
8 consistent with embodiments of the present invention.

9 10 **DETAILED DESCRIPTION OF THE INVENTION**

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

18 The terms "scramble" and "encrypt" and variations thereof are used
19 synonymously herein. Also, the term "television program" and similar terms can
20 be interpreted in the normal conversational sense, as well as a meaning wherein
21 the term means any segment of AV content that can be displayed on a television
22 set or similar monitor device. The term "video" is often used herein to embrace not
23 only true visual information, but also in the conversational sense (e.g., "video tape
24 recorder") to embrace not only video signals but associated audio and data. The
25 term "legacy" as used herein refers to existing technology used for existing cable
26 and satellite systems. The exemplary embodiments disclosed herein are decoded
27 by a television Set-Top Box (STB), but it is contemplated that such technology will
28 soon be incorporated within television receivers of all types whether housed in a
29 separate enclosure alone or in conjunction with recording and/or playback

1 equipment or Conditional Access (CA) decryption module or within a television set
2 itself. The present document generally uses the example of a "dual partial
3 encryption" embodiment, but those skilled in the art will recognize that the present
4 invention can be utilized to realize multiple partial encryption without departing from
5 the invention. Partial encryption and selective encryption are used synonymously
6 herein.

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

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

29 It is assumed, for purposes of the present embodiment of the invention, that
30 the data from satellite receiver 110 is supplied as MPEG (Moving Pictures Expert

1 Group) compliant packetized data. In the first stage of operation the data is passed
2 through a Special Packet Identifier (PID) 122. Special Packet Identifier 122
3 identifies specific programming that is to be dual partially encrypted according to
4 the present invention. The Special Packet Identifier 122 signals the Special Packet
5 Duplicator 126 to duplicate special packets. The Packet Identifier (PID) Remapper
6 130, under control of the computer 118, remaps the PIDs of the elementary
7 streams (ES) (i.e., audio, video, etc.) of the programming that shall remain clear
8 and the duplicated packets to new PID values. The payload of the elementary
9 stream packets are not altered in any way by Special Packet Identifier 122, Special
10 Packet Duplicator 126, or PID remapper 130. This is done so that the primary
11 encryption encoder 104 will not recognize the clear unencrypted content as content
12 that is to be encrypted.

13 The packets may be selected by the special packet identifier 122 according
14 to one of the selection criteria described in the above-referenced applications or
15 may use another selection criteria such as those which will be described later
16 herein. Once these packets are identified in the packet identifier 122, packet
17 duplicator 126 creates two copies of the packet. The first copy is identified with the
18 original PID so that the primary encryption encoder 104 will recognize that it is to
19 be encrypted. The second copy is identified with a new and unused PID, called
20 a "secondary PID" (or shadow PID) by the PID Remapper 130. This secondary PID
21 will be used later by the selective encryption encoder 114 to determine which
22 packets are to be encrypted according to the secondary encryption method.
23 **FIGURE 2** illustrates an exemplary set of transport PSI tables 136 after this
24 remapping with a PAT 138 defining two programs (10 and 20) with respective PID
25 values 0100 and 0200. A first PMT 140 defines a PID=0101 for the video
26 elementary stream and PIDs 0102 and 0103 for two audio streams for program 10.
27 Similarly, a second PMT 142 defines a PID=0201 for the video elementary stream
28 and PIDs 0202 and 0203 for two audio streams for program 20.

29 As previously noted, the two primary commercial providers of cable head
30 end encryption and modulation equipment are (at this writing) Motorola, Inc. and

1 Scientific-Atlanta, Inc. While similar in operation, there are significant differences
2 that should be discussed before proceeding since the present selective encryption
3 encoder 114 is desirably compatible with either system. In the case of Motorola
4 equipment, the Integrated Receiver Transcoder (IRT), an unmodulated output is
5 available and therefore there is no need to demodulate the output before returning
6 a signal to the selective encryption encoder 114, whereas no such unmodulated
7 output is available in a Scientific-Atlanta device. Also, in the case of current
8 Scientific-Atlanta equipment, the QAM, the primary encryption encoder carries out
9 a PID remapping function on received packets. Thus, provisions are made in the
10 selective encryption encoder 114 to address this remapping.

11 In addition to the above processing, the Program Specific Information (PSI)
12 is also modified to reflect this processing. The original, incoming Program
13 Association Table (PAT) is appended with additional Program Map Table (PMT)
14 entries at a PMT inserter 134. Each added PMT entry contains the new, additional
15 streams (remapped & shadow PIDs) created as part of the selective encryption
16 (SE) encoding process for a corresponding stream in a PMT of the incoming
17 transport. These new PMT entries will mirror their corresponding original PMTs.
18 The program numbers will be automatically assigned by the selective encryption
19 encoder 114 based upon open, available program numbers as observed from the
20 program number usage in the incoming stream. The selective encryption System
21 114 system displays the inserted program information (program numbers, etc) on
22 the configuration user interface of control computer 118 so that the Multiple System
23 Operator (MSO, e.g., the cable system operator) can add these extra programs into
24 the System Information (SI) control system and instruct the system to carry these
25 programs in the clear.

26 The modified transport PSI is illustrated as 144 in **FIGURE 3** with two
27 additional temporary PMTs 146 and 148 appended to the tables of transport PSI
28 136. The appended PMTs 146 and 148 are temporary. They are used for the
29 primary encryption process and are removed in the second pass of processing by
30 the secondary encryption encoder. In accordance with the MPEG standard, all

1 entries in the temporary PMTs are marked with stream type "user private" with an
 2 identifier of 0xF0. These PMTs describe the remapping of the PIDs for use in later
 3 recovery of the original mapping of the PIDs in the case of a PID remapping in the
 4 Scientific-Atlanta equipment. Of course, other identifiers could be used without
 5 departing from the present invention.

6 In order to assure that the Scientific-Atlanta PID remapping issue is
 7 addressed, if the selective encryption encoder 114 is configured to operate with a
 8 Scientific-Atlanta system, the encoder adds a user private data descriptor to each
 9 elementary stream found in the original PMTs in the incoming data transport
 10 stream (TS) per the format below (of course, other formats may also be suitable):
 11

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

12 The selective encryption encoder 114 of the current embodiment also adds
 13 a user private data descriptor to each elementary stream placed in the temporary
 14 PMTs created as described above per the format below:
 15

<u>Syntax</u>	<u>value</u>	<u># of bits</u>
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
}		
}		

1
2 The "????" in the tables above is the value of the "orig_pid" which is a variable
3 while the "??" is a "stream_type" value. The data field for "orig_pid" is a variable
4 that contains the original incoming PID or in the case of remap or shadow PIDs, the
5 original PID that this stream was associated with. The data field "stream_type" is
6 a variable that describes the purpose of the stream based upon the chart below:

<u>Stream Type</u>	<u>Value</u>
Legacy ES	0x00
Remapped ES	0x01
Shadow ES	0x02
Reserved	0x03 – 0xFF

7
8
9
10
11
12
13
14 These descriptors will be used later to re-associate the legacy elementary
15 streams, which are encrypted by the Scientific-Atlanta, Inc. primary encryption
16 encoder 104, with the corresponding shadow and remapped clear streams after
17 PID remapping in the Scientific-Atlanta, Inc. modulator prior to the second phase
18 of processing of the Selective Encryption Encoder. Those skilled in the art will
19 appreciate that the above specific values should be considered exemplary and
20 other specific values could be used without departing from the present invention.

21 In the case of a Motorola cable system being selected in the selective
22 encryption encoder configuration GUI, the original PAT and PMTs can remain

1 unmodified, providing the system does not remap PIDs within the primary
2 encryption encoder. The asterisks in **FIGURE 1** indicate functional blocks that are
3 not used in a Motorola cable system.

4 The data stream from selective encryption encoder 114 is passed along to
5 the input of the primary encryption encoder 104 which first carries out a PID filtering
6 process at 150 to identify packets that are to be encrypted. At 152, in the case of
7 a Scientific-Atlanta device, a PID remapping may be carried out. The data are then
8 passed along to an encrypter 154 that, based upon the PID of the packets encrypts
9 certain packets (in accord with the present invention, these packets are the special
10 packets which are mapped by the PID Remapper 130 to the original PID of the
11 incoming data stream for the current program). The remaining packets are
12 unencrypted. The data then passes through a PSI modifier 156 that modifies the
13 PSI data to reflect changes made at the PID remapper. The data stream is then
14 modulated by a quadrature amplitude modulation (QAM) modulator 158 (in the
15 case of the Scientific-Atlanta device) and passed to the output thereof. This
16 modulated signal is then demodulated by a QAM demodulator 160. The output of
17 the demodulator 160 is directed back to the selective encryption encoder 114 to a
18 PSI parser 164.

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

1 concatenator 168. The packets in the legacy streams are appended to the
 2 remapped content, which is again remapped back to the PID of the legacy streams,
 3 completing the partial, selective encryption of the original elementary streams.

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

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

<u>CA PID Definition</u>	<u>Secondary CA private data Value</u>
ECM PID	0x00
Replacement PID	0x01
Insertion PID	0x02
ECM PID	undefined (default)

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

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

14 The control processor 100 may be a personal computer based device that
15 is used to control the selective encryption encoder as described herein. An
16 exemplary personal computer based controller 100 is depicted in **FIGURE 4**.
17 Control processor 100 has a central processor unit (CPU) 210 with an associated
18 bus 214 used to connect the central processor unit 210 to Random Access Memory
19 218 and Non-Volatile Memory 222 in a known manner. An output mechanism at
20 226, such as a display and possibly printer, is provided in order to display and/or
21 print output for the computer user as well as to provide a user interface such as a
22 Graphical User Interface (GUI). Similarly, input devices such as keyboard and
23 mouse 230 may be provided for the input of information by the user at the MSO.
24 Computer 100 also may have disc storage 234 for storing large amounts of
25 information including, but not limited to, program files and data files. Computer
26 system 100 also has an interface 238 for connection to the selective encryption
27 encoder 114. Disc storage 234 can store any number of encryption methods that
28 can be downloaded as desired by the MSO to vary the encryption on a regular
29 basis to thwart hackers. Moreover, the encryption methods can be varied

1 according to other criteria such as availability of bandwidth and required level of
2 security.

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

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

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

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

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

1 SLICE HEADER ENCRYPTION

2 **FIGURE 6** illustrates a encryption of the slice headers for all of the slices of
3 the frame 254. In this illustration, the diagonal cross-hatching is intended to
4 represent encrypted information. By encryption of a slice header, the
5 corresponding slice cannot be properly displayed. Moreover, a relatively low
6 amount of bandwidth is required in a dual encryption scenario for encryption of
7 packets with secondary PIDs when the encrypted packets are those containing the
8 slice header. As a practical matter, encryption of a packet containing the slice
9 header likely involves encryption of additional information including at least a
10 portion of the first macroblock following each slice header, rendering the slice all
11 the more difficult to decode. Such a scheme involves encryption of less than about
12 2 percent of the data and is thus quite practical to implement with little impact on
13 bandwidth. However, since such a scheme leaves certain anchor data transmitted
14 in the clear, it is potentially subject to attack.

15

16 SLICE HEADER AND FIRST MACROBLOCK ENCRYPTION

17 Security can be further enhanced if in addition to the slice header, the first
18 macroblock is encrypted in each slice. This is depicted in **FIGURE 7** as frame 258,
19 again with the encrypted information shown with diagonal cross-hatch marks.
20 Since the first macroblock of each slice contains anchor data in the form of
21 absolute chrominance and luminance values, encryption of the first macroblock of
22 each slice reduces the amount of absolute data available to a hacker to work
23 backwards from in order to decypher the image. Using this technique adds little
24 to the overhead of encryption of slice headers alone and results in encryption of
25 only about 2 percent of the total data. Owing to the variable length of the
26 macroblocks, somewhat more data may be encrypted according to this scheme,
27 since a packet may carry portions of multiple macroblocks.

1 Those skilled in the art will also appreciate that the first macroblock of each
2 slice can also be encrypted without encryption of the slice headers to distort the
3 video. This is also a viable encryption scheme.
4

5 **ACTIVE REGION ENCRYPTION**

6 Another technique providing a suitable tradeoff between bandwidth and
7 encryption security involves encryption of selected portions of the frame which can
8 be deemed the "active region" of the image. This region is somewhat difficult to
9 define and is somewhat content dependent. But, generally speaking it is
10 approximately a central area of the frame. More commonly, it is approximately an
11 upper central portion of the frame of approximately half (say, one third to 3/4) of the
12 overall area of the frame centered at approximately the center of the frame
13 horizontally and approximately the tenth to fifteenth slice. According to its broadest
14 definition, the active region of the image is made up of the centralized portion of a
15 frame with at least one slice bounding the upper and lower region of the frame.
16 One embodiment of this region is depicted in frame 262 of **FIGURE 8**, as region
17 266.

18 Owing to the variable size of the macroblocks in each frame, encryption of
19 an active area as described suggests that a varying number of packets in each
20 slice might require encryption (assuming packetizing of the macroblocks) and a
21 scenario wherein more actual data than that illustrated in **FIGURE 8** will actually
22 undergo encryption. This is illustrated in **FIGURE 9** in which each slice of frame
23 270 is depicted as encompassing a varying number of packets such as packet 272.
24 Moreover, the actual starting and ending point of the packet varies due to the
25 variation in size of the macroblocks. Depending upon the actual definition of the
26 active region, the overhead required for dual encryption of frames such as those
27 described above, will also vary. (Note that for illustrative purposes, the packets are
28 depicted as variable in length and the macroblocks fixed in length, whereas, the
29 opposite is actually the case)

1 In this encryption technique, the active portion of the screen is deemed to be
2 the area of most interest to the viewer. Although some intelligible video information
3 is present, it is likely to at least be an annoyance to an unauthorized viewer. In
4 combination with other techniques, this can be a useful variation in the available
5 encryption techniques.

6 7 **ACTIVE SLICE ENCRYPTION**

8 **FIGURE 10** depicts a frame 274 that has all slices in an active region
9 encrypted. Under the broadest definition of "active region" above, this type of
10 encryption is a subcategory of the active region encryption method. In this
11 embodiment, slices 6 through 23 are encrypted, but other regions of slices could
12 equally well be defined as the central or active region and encrypted as shown.
13 Again, this technique, when used alone, will permit substantial information to be
14 transmitted in the clear and possibly provide clear images at the upper and lower
15 portions of a frame. Encryption of the active slices can be accomplished in any
16 number of ways including, but not limited to, encryption of the slice headers alone
17 or in combination with the first macroblocks of the active slices as well as full
18 encryption of all data in the active slices.

19 20 **ENCRYPTION OF ANCHOR DATA**

21 Anchor data appears in the data stream at various times to provide absolute
22 luminance and chrominance information. This is normally carried out in an MPEG
23 system using an I Frame. However, some encoders (e.g., those produced by
24 Motorola, Inc.) use P Frames to encode progressively refreshed intracoded slices.
25 Such systems often refresh three consecutive slices in a P Frame with the
26 following three slices refreshed in the next P Frame. Thus a full refresh takes 30
27 frames and requires about one second to accomplish. The most important motion
28 vectors to encrypt appear to be those that occur immediately after a refresh of
29 anchor data. Encryption of such anchor data (I Frames or P Frames in a

1 progressive refreshed system) will cause data that follows the anchor data to be
2 rendered useless since it contains no reference point from which to adjust the
3 picture.
4

5 **ENCRYPTION OF MOTION VECTORS AFTER ANCHOR DATA**

6 A number of theoretical attacks against proposed SE encryption schemes
7 recover information that may be encrypted by the intracoded slice headers. The
8 information encrypted could be the DC absolute values for luminance and/or
9 chrominance. For example, clear intracoded macroblocks sent in previous frames
10 or in adjoining slices might be used to recover the DC absolute values for the
11 macroblocks with that information encrypted (through some type of correlation).
12 Other methods use a minimum/maximum differential technique to derive the DC
13 absolute value without any need for clear intracoded macroblocks. An encryption
14 technique that might be more immune to this type of attack is described below.

15 As previously described, motion vectors are used to describe the movement
16 of blocks or macroblocks of information within the image. Motion compensation
17 displaces macroblocks from previous pictures. Macroblock predictions are formed
18 out of arbitrary 16x16 pixel (or 16x8 in MPEG-2) areas from previously reconstructed
19 pictures. There are no boundaries which limit the location of a macroblock
20 prediction within the previous picture. In accordance with certain embodiments
21 consistent with the present invention, consider encryption of the first macroblock
22 in non-intracoded slices (slices without all intracoded macroblocks).

23 The most critical motion vectors to encrypt appear to be those appearing
24 right after a "refresh" either with an I Frame or a P Frame. These motion vectors
25 most typically are sent in a B or P frame. Since B frames are not referenced by
26 other frames, a maximal destructive effect is achieved by encrypting the motion
27 vectors in the subsequent P frame after an I Frame or P Frame. There are two
28 types of refresh mechanisms currently employed by content encoders in the
29 content community. Traditional encoders use I frames, while Motorola encoders
30 use P frames with progressively refreshed intracoded slices.

1 It may be possible to skip encryption for some of the motion vectors, and still
 2 achieve a destructive effect. For example, the motion vectors after every other I
 3 frame could be encrypted and still affect the image to a large extent ... making it
 4 unwatchable. For HITS (Headend In The Sky) streams, every other P frame could
 5 be skipped. However, it would be beneficial to lap the encryption so that every slice
 6 is affected at least once approximately every two seconds. For HITS, it may be
 7 possible to encrypt two out of the three or one out of the three slices after a refresh
 8 swath.

9 Motion vectors are differentially coded from the previous macroblock except
 10 in the following instances:

- 11 1) Start of a slice;
- 12 2) An intra macroblock;
- 13 3) Non-intracoded macroblock which has motion_forward = 0; and
- 14 4) A macroblock is skipped.

15 Certain embodiments consistent with the present invention covers case 1)
 16 above at all times. In other embodiments, cases 2), 3) and 4) can be recognized
 17 by encrypting the macroblock that comes after the start of a slice (with absolute
 18 motion vectors).

20 **ENCRYPTION OF SLICES WITH INTRA_SLICE_FLAG OR INTRA_SLICE SET**

21 The slice header has syntax described by the table below:

23 Slice() {	No. of bits	Mnemonic
24 slice_start_code	32	bslbf
25 If (vertical_size>28000		
26 slice_vertical_position_extension	3	uimsbf
27 if(<sequence_scalable_extension () is present		
28 in bitstream>){		
29 if (scalable_mode === "data partitioning")		

1	priority_breakpoint	7	uimsbf
2	}		
3	quantizer_scale_code	5	uimsbf
4	if (nextbits() == '1'){		
5	intra_slice_flag	1	bslbf
6	intra_slice	1	uimsbf
7	reserved_bits	7	uimsbf
8	while (nextbits() == '1' {		
9	extra_bit_slice /* with value of '1' */	1	uimsbf
10	extra_slice_information	8	uimsbf
11	}		
12	}		
13	extra_bit_slice /* with value of '0' */		
14	do {		
15	macroblock()		
16	} while (nextbits() != '000 0000 0000 0000 0000		
17	0000')		
18	next_start_code()		
19	}		
20			

21 Slices with all intra-coded macroblocks have the intra_slice indicator set to 1. This
 22 flag may be used to signal slices with intra-coded macroblocks which would not
 23 only be sent with I Frames, but also with "progressive refresh" P Frames (where a
 24 certain number of slices are sent with all intra-coded macroblocks). The
 25 intra_slice_flag set to "1" may be used to flag slices with any portion of intra-coded
 26 macroblocks, and might be used to completely eliminate decoding of any
 27 intra-coded macroblocks.

28 For applications in cable television systems, there are primarily two types of

1 streams to consider, the Motorola DigiCipher™ streams and Divicom™ streams.
2 DigiCipher™ streams do not use I Frames and are of the progressive refresh P
3 Frame type. Divicom™ streams use conventional MPEG I Frames. In progressive
4 refresh streams, a selected number of slices (e.g., three out of thirty) are sent as
5 completely intra-coded macroblocks. In I Frames, all slices are sent completely
6 intra-coded macroblocks. In each case, these intra-coded macroblocks serve to
7 carry "anchor data" for motion compensation vectors and other compression
8 techniques which are signaled in other frames. If this anchor data are encrypted,
9 then all the data that references it is useless. In both cases, the intra_slice_flag
10 and the intra_slice indicator are set to "1". Thus, by encrypting packets containing
11 slice headers with set intra_slice_flags and/or intra_slice indicators, key anchor
12 data can be encrypted.

13 14 **ENCRYPTION OF INTRA-CODED MACROBLOCKS**

15 The previous technique provides one technique for detection of intra-coded
16 macroblocks. However, any technique that detects macroblocks containing intra-
17 coded data can be used as a selection criterion for selecting data or data packets
18 containing key anchor data for encryption.

19 20 **ENCRYPTION OF SLICES WITH MULTIPLE INTRA-CODED MACROBLOCKS**

21 If a slice contains multiple intra-coded macroblocks, this may be used in
22 another technique as the selection criterion for selection of information to be
23 encrypted. Slices which contain multiple intra-coded macroblocks are indicative
24 that the slice contains significant amounts of anchor data.

25 26 **COMBINED ENCRYPTION TECHNIQUES**

27 Multiple combinations of the above techniques are possible to produce
28 encryption that has varying bandwidth requirements, varying levels of security and
29 varying complexity. Several examples of these combinations, without limitation to

1 those specifically mentioned are:

- 2 • Packets containing slice headers, first macroblocks following slice headers
3 or intra_coded data appearing within a specifically defined active region of
4 the image.
- 5 • All packets containing either I Frame data or P Frame data following the I
6 Frame within the active region of the image.
- 7 • All packets containing either I Frame data or slice header data.
- 8 • All packets containing data in the active region of the image plus all packets
9 containing slice headers.

10
11 Numerous other combinations of the above encryption techniques as well
12 as those described in the above-referenced patent applications and other partial
13 encryption techniques can be combined to produce a rich palette of encryption
14 techniques from which to select. In accordance with certain embodiments of the
15 present invention, a selection of packets to encrypt can be made by the control
16 computer 118 in order to balance encryption security with bandwidth and in order
17 to shift the encryption technique from time to time to thwart hackers.

18 An authorized set-top box such as 300 illustrated in **FIGURE 11** operating
19 under the secondary CA system decrypts and decodes the incoming program by
20 recognizing both primary and secondary PIDs associated with a single program.
21 The multiplexed video data stream containing both PIDs is directed to a
22 demultiplexer 304. When a program is received that contains encrypted content
23 that was encrypted by any of the above techniques, the demultiplexer directs
24 encrypted packets containing encrypted content and secondary PIDS to a
25 secondary CA decrypter 308. These packets are then decrypted at 308 and passed
26 to a PID remapper 312. As illustrated, the PID remapper 312 receives packets that
27 are unencrypted and bear the primary PID as well as the decrypted packets having
28 the secondary PID. The PID remapper 312 combines the decrypted packets from
29 decrypter 308 with the unencrypted packets having the primary PID to produce an
30 unencrypted data stream representing the desired program. PID remapping is

1 used to change either the primary or secondary PID or both to a single PID. This
2 unencrypted data stream can then be decoded normally by decoder 316. Some or
3 all of the components depicted in **FIGURE 11** can be implemented and/or
4 controlled as program code running on a programmed processor, with the code
5 being stored on an electronic storage medium.

6 **FIGURE 12** is a flow chart 400 that broadly illustrates the encryption process
7 consistent with certain embodiments of the present invention starting at 404. At
8 408 the packet type that is to be encrypted is specified. In accordance with certain
9 embodiments consistent with the present invention, the selected packet type may
10 be any individual one or combination of the following: packets containing a video
11 slice header appearing in an active region of a video frame, any packet carrying
12 data representing an active region of a video frame, I Frame packets, packets
13 containing motion vectors in a first P frame following an I Frame, packets having
14 an intra_slice_flag indicator set, packets having an intra_slice indicator set, packets
15 containing an intra_coded macroblock, packets that carry data for a slice
16 containing an intra_coded macroblock, packets containing data from a first
17 macroblock following the video slice header, packets containing video slice
18 headers, packets containing anchor data, and P Frame packets for progressively
19 refreshed video data. Packets are then examined at 412 to identify packets of the
20 specified type. At 416, the identified packets are duplicated and at 420 one set of
21 these packets is encrypted under a first encryption method. The other set of
22 identified packets is encrypted at 424 under a second encryption method. The
23 originally identified packets are then replaced in the data stream with the two sets
24 of encrypted packets at 430 and the process ends at 436.

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

29 Those skilled in the art will recognize that the present invention has been

1 described in terms of exemplary embodiments based upon use of a programmed
2 processor (e.g., processor 118, processors implementing any or all of the elements
3 of 114 or implementing any or all of the elements of 300). However, the invention
4 should not be so limited, since the present invention could be implemented using
5 hardware component equivalents such as special purpose hardware and/or
6 dedicated processors which are equivalents to the invention as described and
7 claimed. Similarly, general purpose computers, microprocessor based computers,
8 micro-controllers, optical computers, analog computers, dedicated processors
9 and/or dedicated hard wired logic may be used to construct alternative equivalent
10 embodiments of the present invention.

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

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

1 Such variations are contemplated and considered equivalent.

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

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

What is claimed is:

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

a demultiplexer that receives packets of digital video, certain of the packets being unencrypted and certain of the packets being encrypted, wherein certain of the encrypted packets carry data representing an active region of a video frame;

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

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

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

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

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

a demultiplexer that receives packets of digital video, certain of the packets being unencrypted and certain of the packets being encrypted, wherein certain of the encrypted packets carry a video slice header;

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

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

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

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

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

a demultiplexer that receives packets of digital video, certain of the packets being unencrypted and certain of the packets being encrypted, wherein certain of the encrypted packets carry at least one of the following: packets containing a video slice header appearing in an active region of a video frame, any packet carrying data describing an active region of a video frame, I Frame packets, packets containing motion vectors in a first P frame following an I Frame, packets having an `intra_slice_flag` indicator set, packets having an `intra_slice` indicator set, packets containing an `intra_coded` macroblock, packets that carry data for a slice containing an `intra_coded` macroblock, packets containing data from a first macroblock following the video slice header, packets containing video slice headers, packets containing anchor data, and P Frame packets for progressively refreshed video data;

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

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

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

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

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

receiving packets of digital video, certain of the packets being unencrypted and certain of the packets being encrypted, wherein certain of the encrypted packets carry data describing an active region of a video frame;

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

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

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

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

5. A computer readable medium carrying instructions which, when executed on a programmed processor, carry out the method of decoding and decrypting a digital video signal according to claim 4.

6. The computer readable medium of claim 5, wherein the medium comprises an electronic storage medium.

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

receiving packets of digital video, certain of the packets being unencrypted and certain of the packets being encrypted, wherein certain of the encrypted packets carry a video slice header;

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

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

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

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

8. A computer readable medium carrying instructions which, when executed on a programmed processor, carry out the method of decoding and decrypting a digital video signal according to claim 7.

9. The computer readable medium of claim 8, wherein the medium comprises an electronic storage medium.

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

receiving packets of digital video, certain of the packets being unencrypted and certain of the packets being encrypted, wherein certain of the encrypted packets carry at least one of the following: packets containing a video slice header appearing in an active region of a video frame, any packet carrying data describing an active region of a video frame, I Frame packets, packets containing motion vectors in a first P frame following an I Frame, packets having an intra_slice_flag indicator set, packets having an intra_slice indicator set, packets containing an intra_coded macroblock, packets that carry data for a slice containing an intra_coded macroblock, packets containing data from a first macroblock following the video slice header, packets containing video slice headers, packets containing anchor data, and P Frame packets for progressively refreshed video data;

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

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

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

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

11. A computer readable medium carrying instructions which, when executed on a programmed processor, carry out the method of decoding and decrypting a digital video signal according to claim 10.
12. The computer readable medium of claim 11, wherein the medium comprises an electronic storage medium.
13. A computer readable medium that carries instructions that when executes on a programmed processor to facilitate operation of a video receiver device to decrypt and decode a selectively encoded digital video signal wherein the instructions comprise:
 - a code segment that controls a demultiplexer that receives packets of digital video, certain of the packets being unencrypted and certain of the packets being encrypted, wherein certain of the encrypted packets carry data describing an active region of a video frame, the unencrypted packets having a first packet identifier (PID) and the encrypted packets having a second packet identifier (PID);
 - a code segment that controls decryption of the encrypted packets to produce decrypted packets;
 - a code segment that controls remapping at least one of the first and second PIDs so that the unencrypted packets and the decrypted packets have the same PID; and
 - a code segment that controls decoding the unencrypted and decrypted packets to produce a decoded video signal.
14. The computer readable medium of claim 13, wherein the medium comprises an electronic storage medium.
15. A computer readable medium that carries instructions that when executes on a programmed processor to facilitate operation of a video receiver

device to decrypt and decode a selectively encoded digital video signal wherein the instructions comprise:

a code segment that controls a demultiplexer that receives packets of digital video, certain of the packets being unencrypted and certain of the packets being encrypted, wherein certain of the encrypted packets carry a video slice header, the unencrypted packets having a first packet identifier (PID) and the encrypted packets having a second packet identifier (PID);

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

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

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

16. The computer readable medium of claim 15, wherein the medium comprises an electronic storage medium.

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

a code segment that controls a demultiplexer that receives packets of digital video, certain of the packets being unencrypted and certain of the packets being encrypted, wherein certain of the encrypted packets carry at least one of the following: packets containing a video slice header appearing in an active region of a video frame, any packet carrying data describing an active region of a video frame, I Frame packets, packets containing motion vectors in a first P frame following an I Frame, packets having an `intra_slice_flag` indicator set, packets having an `intra_slice` indicator set, packets containing an `intra_coded` macroblock, packets that carry data for a slice containing an `intra_coded`

macroblock, packets containing data from a first macroblock following the video slice header, packets containing video slice headers, packets containing anchor data, and P Frame packets for progressively refreshed video data;

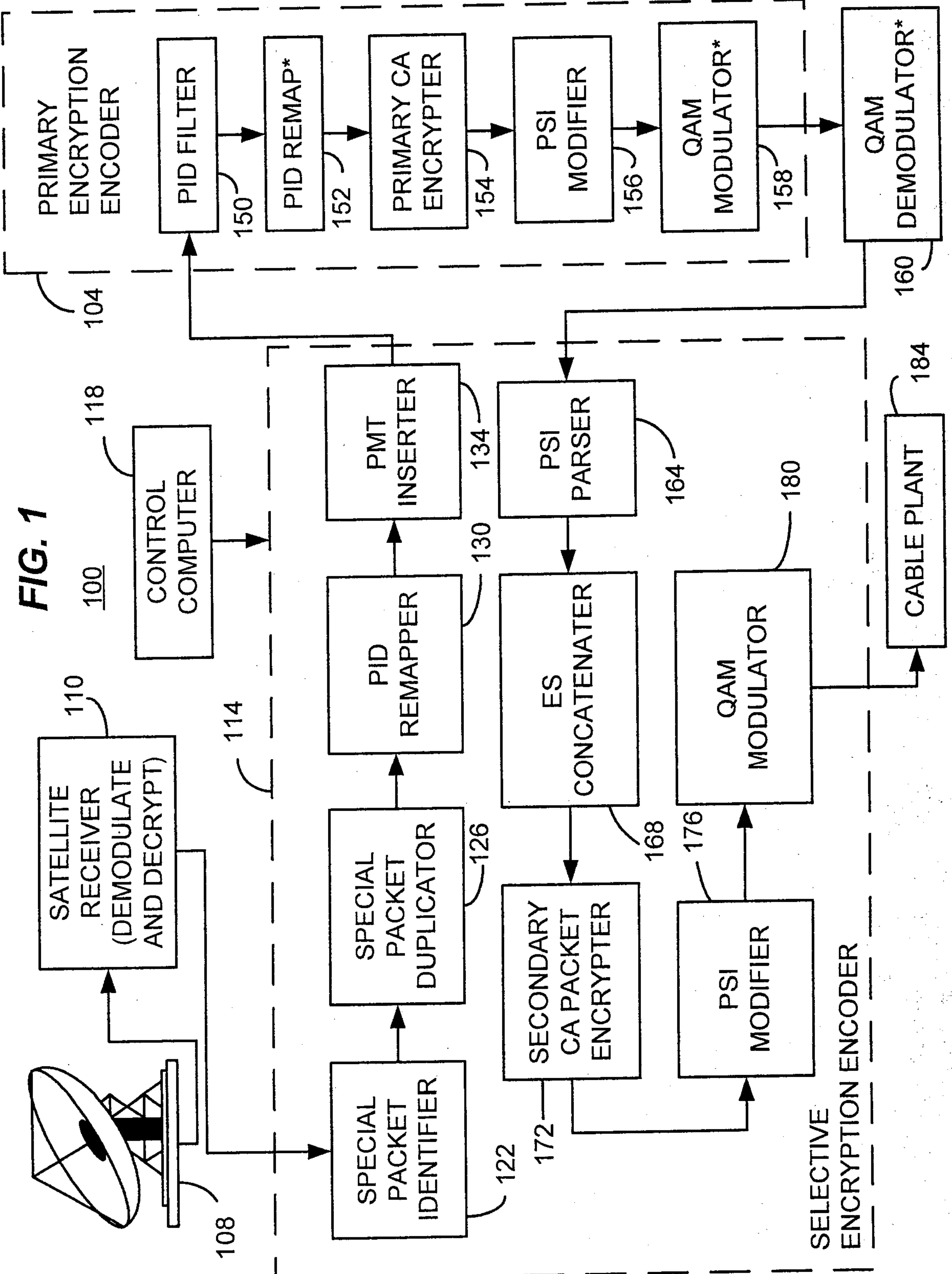
the unencrypted packets having a first packet identifier (PID) and the encrypted packets having a second packet identifier (PID);

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

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

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

18. The computer readable medium of claim 17, wherein the medium comprises an electronic storage medium.



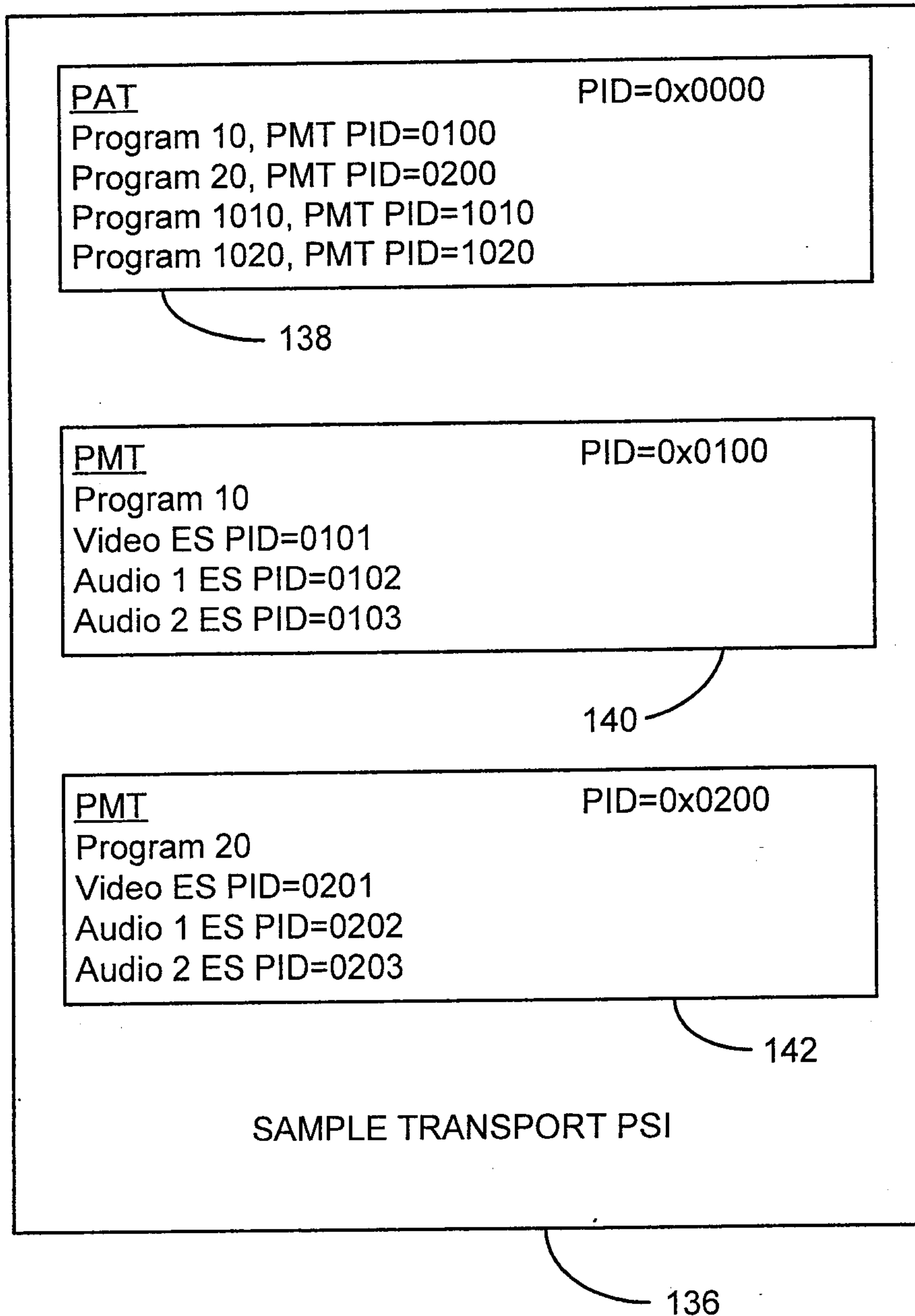


FIG. 2

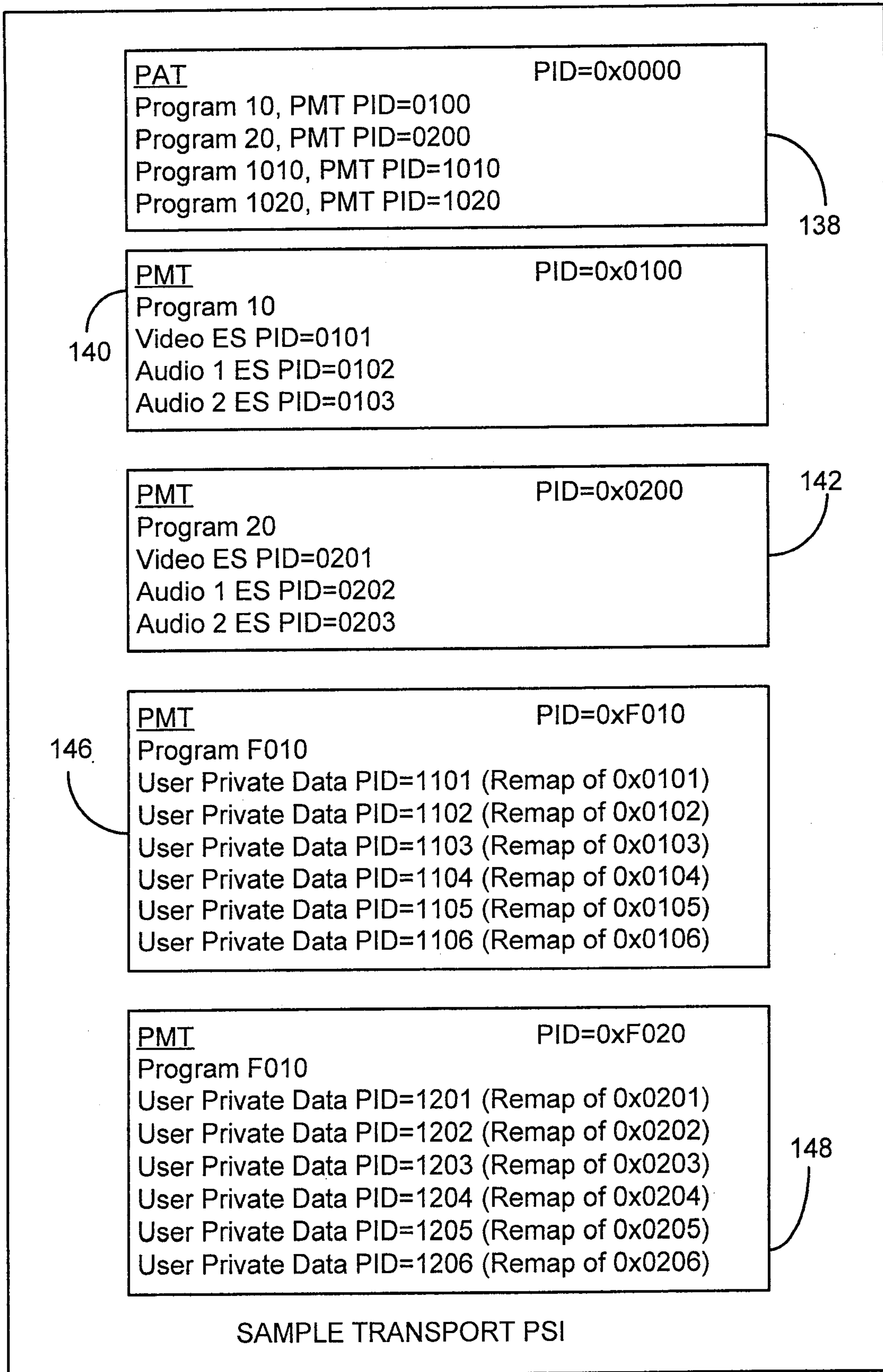


FIG. 3

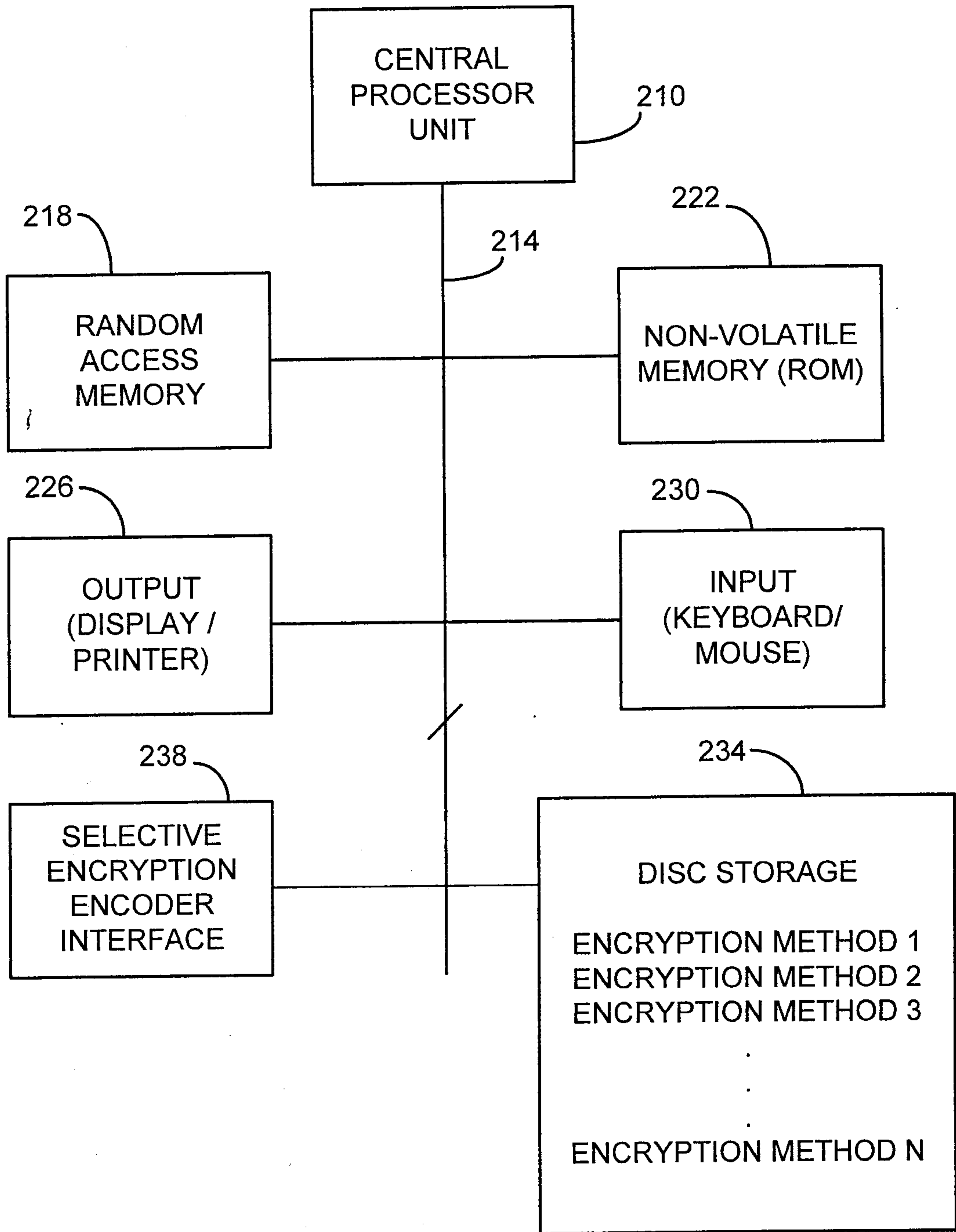


FIG. 4

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

FIG. 6

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

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

FIG. 8

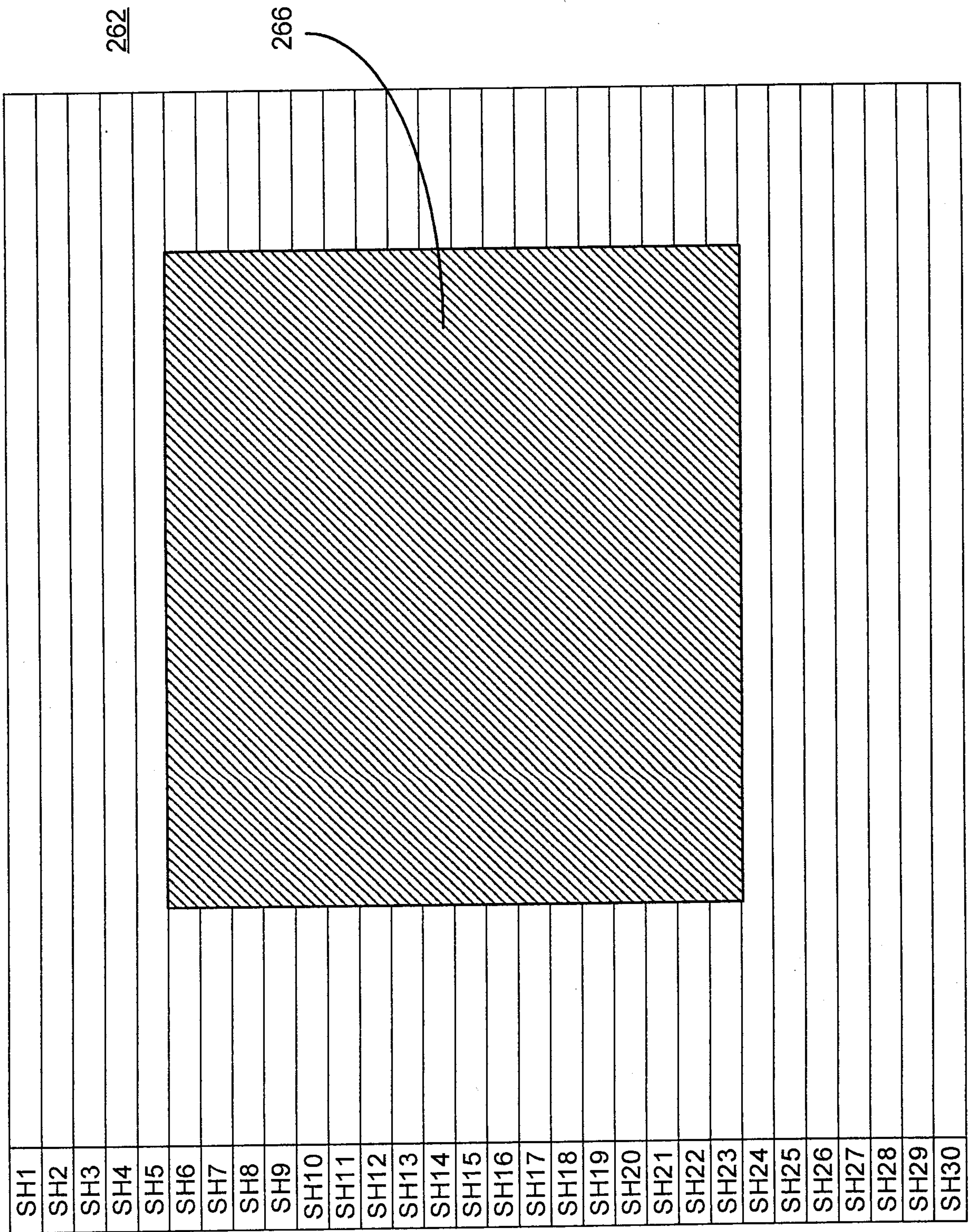
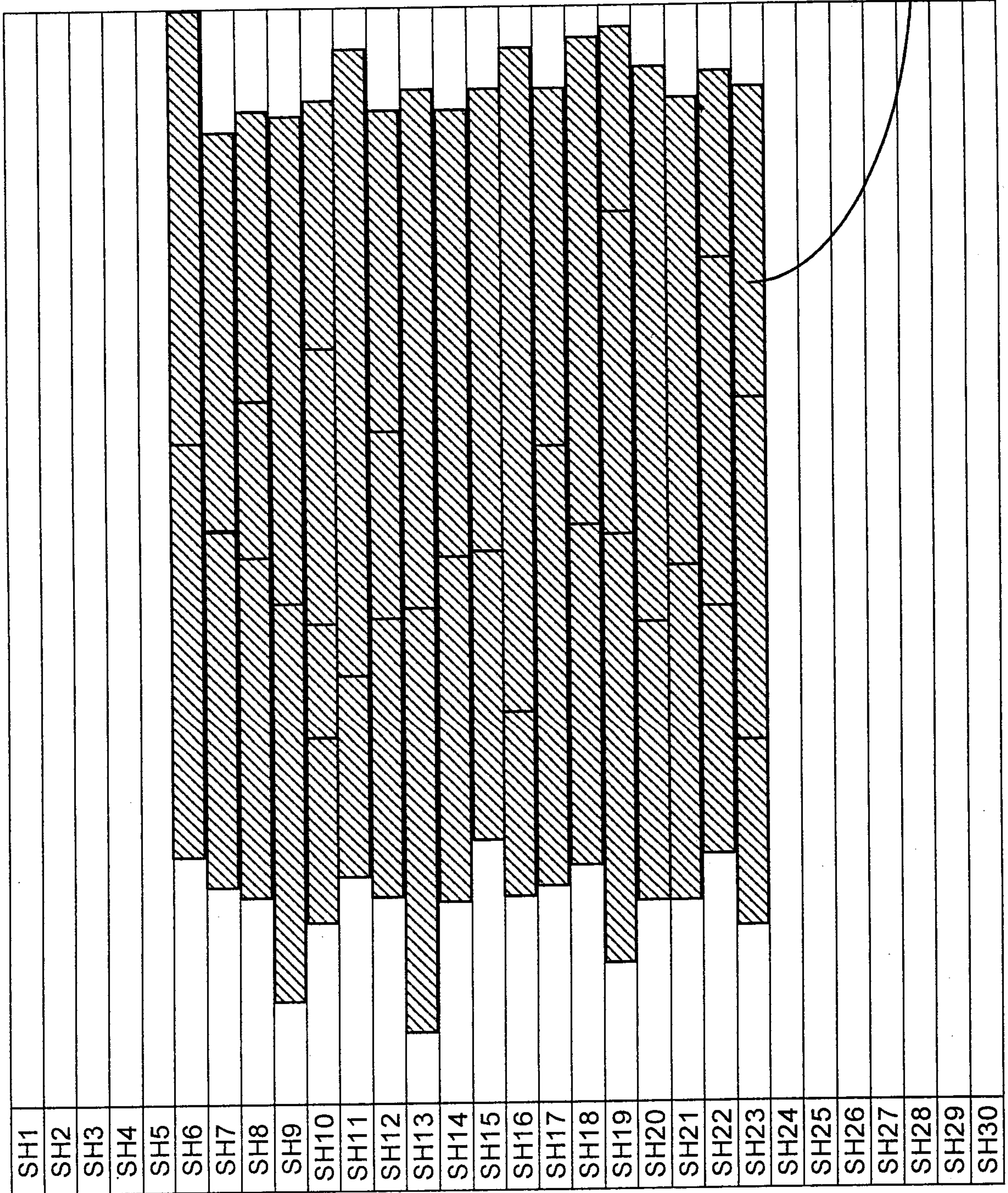


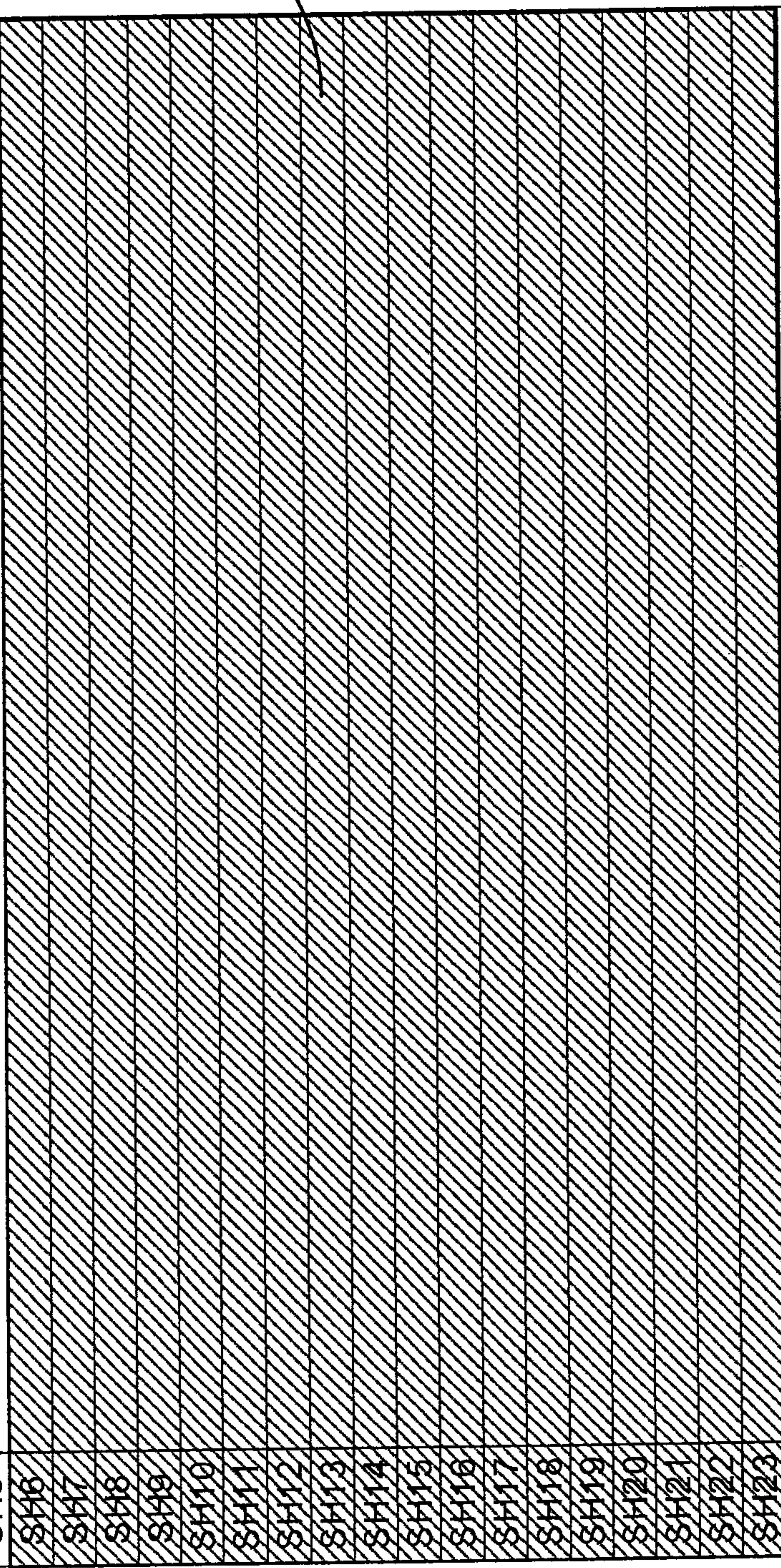
FIG. 9

270



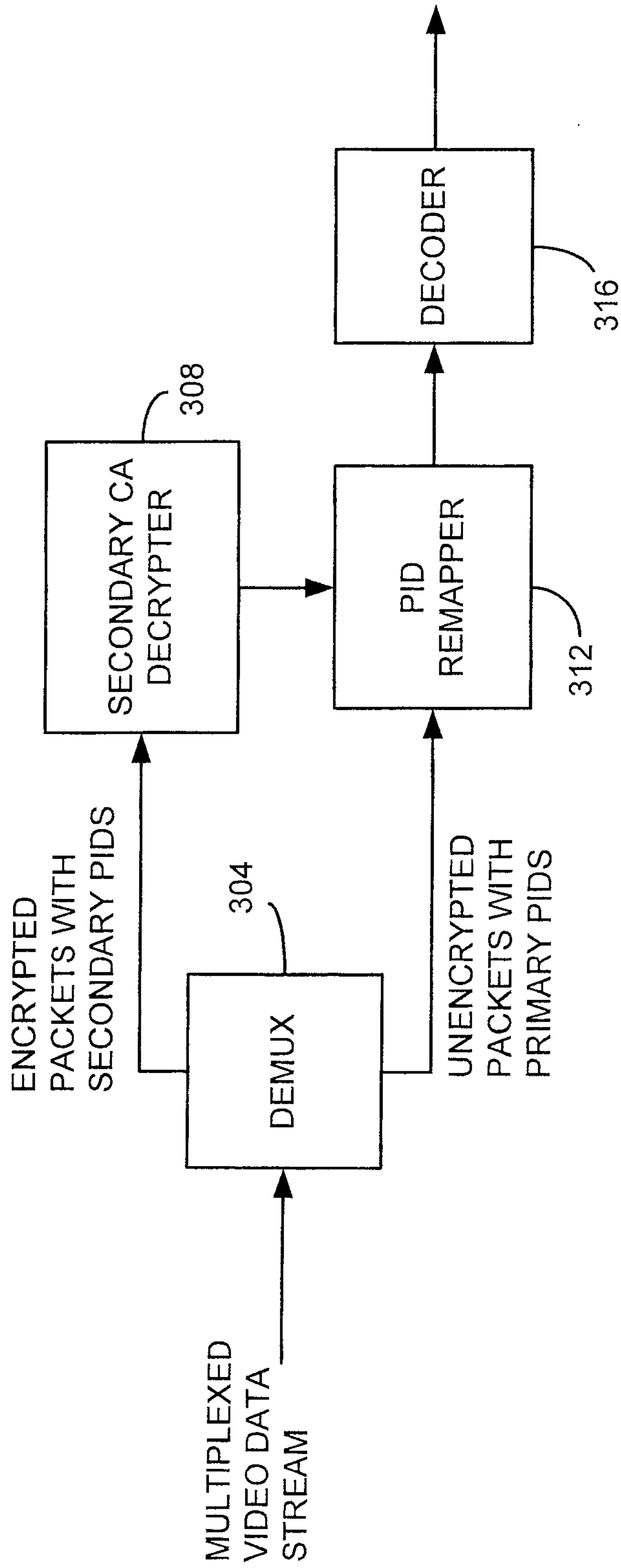
272

FIG. 10

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

274

278



300

FIG. 11

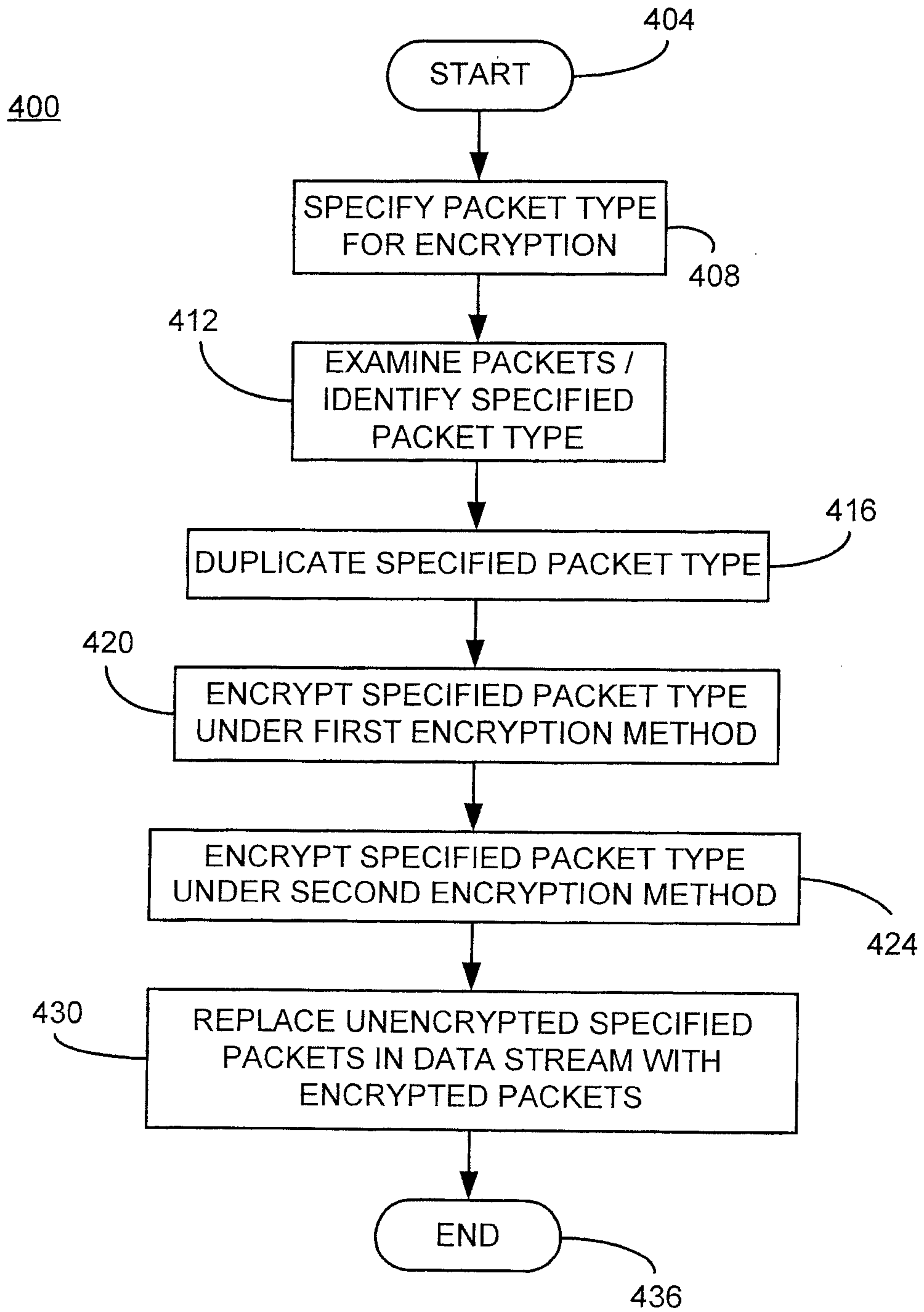


FIG. 12

