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

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2437014 A1 2004/03/09

(21) 2 437 014

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) Date de dépôt/Filing Date: 2003/08/12

(41) Mise à la disp. pub./Open to Public Insp.: 2004/03/09

(30) Priorités/Priorities: 2002/09/09 (60/409,675) US;
2002/11/13 (10/293,761) US

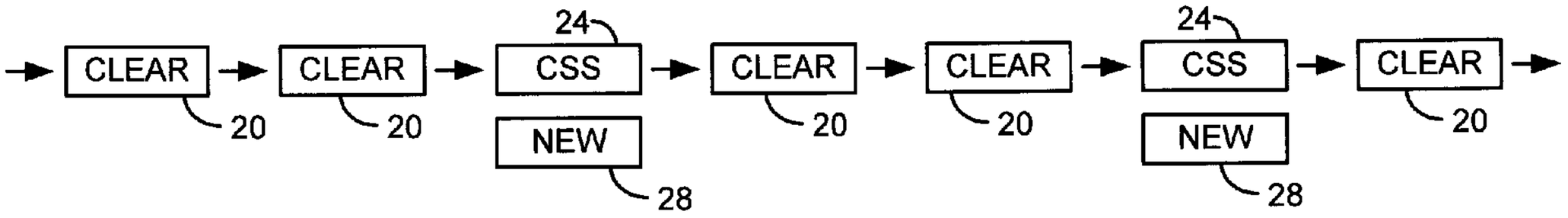
(51) Cl.Int.^{7}/Int.Cl.^{7} H04N 7/167, H04L 9/00

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

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

(74) Agent: GOWLING LAFLEUR HENDERSON LLP

(54) Titre : MISE A NIVEAU DU CRYPTAGE
(54) Title: UPGRADING OF ENCRYPTION



(57) Abrégé/Abstract:
A method of upgrading an encryption process for encryption of video information from an old encryption process to a new encryption process, consistent with certain embodiments involves selecting a portion of video content for selective encryption. The selected portion is duplicated to produce first and second copies of the selected portion. The first copy is encrypted using the old encryption process and the second copy is encrypted using the new encryption process to produce a dual partially encrypted segment of video information that can either be broadcast over a cable or satellite system or stored in a package medium as two program chains.

ABSTRACT OF THE DISCLOSURE

A method of upgrading an encryption process for encryption of video information from an old encryption process to a new encryption process, consistent with certain embodiments involves selecting a portion of video content for selective encryption. The selected portion is duplicated to produce first and second copies of the selected portion. The first copy is encrypted using the old encryption process and the second copy is encrypted using the new encryption process to produce a dual partially encrypted segment of video information that can either be broadcast over a cable or satellite system or stored in a package medium as two program chains.

UPGRADING OF ENCRYPTION

CROSS REFERENCE TO RELATED DOCUMENTS

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

This application is also related to U.S. patent applications serial number 10/273,905, filed October 18, 2002 to Candelore et al. entitled "Video Slice and Active Region Based Dual Partial Encryption", docket number SNY-R4854.01, which is hereby incorporated by reference; serial number 10/273,903, filed October 18, 2002 to Candelore et al. entitled "Star Pattern Partial Encryption", docket number SNY-S5064.01; serial number 10/274,084, filed October 18, 2002 to Candelore et al. entitled "Slice Mask and Moat Pattern Partial Encryption", and

docket number SNY-S5065.01; serial number 10/274,019, filed October 18, 2002 to Candelore et al. entitled "Video Scene Change Detection", docket number SNY-S5162.01.

This application is also related to and claims priority benefit of U.S. Provisional patent application serial number 60/409,675, filed September 9, 2002, docket number 50S5152, entitled "Generic PID Remapping for Content Replacement", to Candelore. These applications are also hereby incorporated by reference herein.

COPYRIGHT NOTICE

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

FIELD OF THE INVENTION

This invention relates generally to the field of digital video and encryption thereof. More particularly, this invention relates to an encryption method and apparatus particularly useful for encrypting 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 (e.g., a television program) 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 (STBs) 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 illustrates a chain of video object units as used in a Digital Versatile Disc (DVD).

FIGURE 2 illustrates a dual partially encrypted DVD with a video chain using standard encryption consistent with certain embodiments of the present invention.

FIGURE 3 illustrates a dual partially encrypted DVD with a video chain using a new encryption consistent with certain embodiments of the present invention.

FIGURE 4 illustrates a partially encrypted DVD with a video chain using a new encryption consistent with certain embodiments of the present invention.

FIGURE 5 illustrates a product transition cycle consistent with certain embodiments of the present invention.

FIGURE 6 illustrates a product transition cycle consistent with certain embodiments of the present invention.

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

FIGURE 8 is a flow chart depicting an encryption process consistent with certain 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 package medium and broadcast, cable and satellite systems such as existing encryption technology used at the launch of such a system. The exemplary embodiments disclosed in the above applications and consistent with certain embodiments of the present invention 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. The term "package medium" and similar terms as used herein are intended to embrace a recording medium such as a Digital Versatile Disc (DVD), Compact Disc (CD) or other magnetic, optical or other recorded medium that is generally merchandised as a package that contains the electronic storage medium and is sold as a retail commodity, as contrasted to an electronically downloadable data stream.

In order to provide content control and protection for both broadcast content (whether by satellite, cable, pay-per-view or otherwise) as well as for packaged media such as Digital Versatile Discs (DVDs), various types of encryption are often utilized. Either the entire content is encrypted under a given encryption system using a particular encryption technique, or the content is partially encrypted using a particular encryption technique.

Unfortunately, as computing power grows, a single encryption technique or a given encryption key may be rendered ineffective in thwarting those who would attempt to pirate the protected content. This problem has been recognized in the satellite and cable industry where it is common to make changes to encryption keys on a regular basis. For example, it is common for such systems to change keys on a monthly basis. Moreover, although less frequent, it is occasionally advisable to upgrade the encryption process itself. By way of example, DES (Data Encryption Standard) encryption can be upgraded from 40 bit encryption to 56 bit encryption to 128 bit encryption, etc. to enhance the security of the encryption. Unfortunately, even with these key sizes, with today's desktop computing power, it is feasible to hack an encryption key by brute force. In another example, DES encryption can be upgraded to a more sophisticated encryption algorithm such as Triple DES, Advanced Encryption Standard (AES) or Common Scrambling Algorithm (CSA). When this happens, upgrading of the software within a television

STB or equivalent device may require a software download or even a change in hardware.

Similarly, encryption techniques used in packaged media may be subject to being cracked by hackers and thus the security of the content compromised. Such is the case for the encryption algorithm originally released with the introduction of DVDs, which has been cracked and the decryption technique posted on the Internet. While the problem is substantial in the case of a content distributor such as a cable system operator, in the case of package media such as DVDs, the problem may even more complex since any encryption used in the packaged medium should be compatible with playback equipment from any of dozens of vendors (whereas, the cable or satellite system may be a closed environment with only one or a small limited number of approved vendors). Thus, until a generational change in encryption standards for the package medium can be made, the content may be compromised. Moreover, the user's existing content may become obsolete by any radical change in encryption introduced to prevent piracy. This may make it extremely difficult for equipment manufacturers to phase out equipment in favor of new equipment, since such changes might be rejected by the consumer. Thus, a transitional mechanism would be beneficial in order to make a transition to a new encryption standard which preserves the current encryption standard for a while, yet facilitates transition to a new standard.

In the above-referenced patent applications, a technique called dual partial encryption or dual selective encryption is described. In this technique, selective portions of video and/or audio content are encrypted while other portions are transmitted unencrypted (clear). By appropriate selection of the content to be encrypted, a very high level of security of the content can be maintained at the sacrifice of minimal amounts of overhead. Since the amount of encrypted content is a small percentage of the overall program content, that small portion can be duplicated and encrypted under several encryption schemes. This makes it possible to decode the program on multiple decoders using multiple decryption schemes. The various encrypted portions in the above applications are

distinguished by use of multiple program identifiers (PIDs). The present invention extends this concept to use in upgrading of encryption techniques for both broadcast content and packaged media.

First consider the example of packaged media, and in particular for purposes of this example (but without limitation) DVDs. DVDs are currently partially encrypted with up to 25% of the overall content being encrypted and up to 50% of any one sector being encrypted. However, the selected VOBU (video object units - a packet definition for packets of 2048 bytes used in DVDs) which are currently encrypted are not necessarily optimally selected. As the above-referenced patent applications have illustrated, by optimal selection of the content to be encrypted, a much lower percentage of packets can be encrypted to still effectively render the content well protected. The selection of content to be encrypted can be any of the selections identified in the above-referenced patent applications, such as, for example without limitation, packets containing a video slice header, packets containing a video slice header appearing in an active region of a video frame, any packet carrying data representing 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, packets occurring in a star pattern approximately situated at approximately a center of an image, packets carrying data representing a pattern of horizontal stripes across an image, packets carrying data representing a pattern of vertical stripes across an image, packets carrying information that is needed to decode the content, packets carrying a payload that comprises a packetized elementary stream (PES) header, samples of the video content taken at prescribed sampling intervals, packets containing a specified elementary stream, and any other suitable packet selection criterion.

Once a collection of VOBUs (packets) are selected for encryption, the content is dual partial encrypted so that it has a clear portion, a portion encrypted using the old encryption process and a portion encrypted using the new encryption process. The dual partial encrypted video content is then stored on the DVD so that a first program chain references the clear portion and the portion encrypted using the old encryption process, and so that a second program chain references the clear portion and the portion encrypted using the new encryption process. Such alternative program chains are currently used in some DVDs to provide additional program content such as director cuts, different viewing angles, alternate plots and endings, and to provide parental control and alternative audio tracks. The majority of DVDs currently in production have only a single linear program chain.

A dual partially encrypted DVD (or other package medium such as a CD) can thus be used as a transitional medium to facilitate conversion to the new encryption format. Consider, **FIGURES 1-4** to understand the principles of the transition to a new encryption algorithm. **FIGURE 1** depicts a DVD which is partially encrypted using the current standard CSS (Content Scrambling System) encryption system. In this figure, a selection of content contains a sequence of VOBUs (packets) having clear VOBUs 20 and encrypted VOBUs 24. The chain of clear VOBUs 20 and encrypted VOBUs 24 together form a content selection that can be played back through a standard DVD player that understands and decrypts CSS encrypted VOBUs.

FIGURES 2 and **3** depict a dual partially encrypted DVD consistent with certain embodiments of the present invention. In these figures, the DVD contains the same chain of partially encrypted content made up of VOBUs 20 and 24 as shown in **FIGURE 1**. Thus, a standard DVD player that decrypts CSS encrypted VOBUs can play back the DVD depicted in **FIGURE 2** by simply following the program chain shown. A new DVD player can be introduced that also can play back the DVD by following the program chain shown in **FIGURE 3**. The new DVD

player need not be able to decode CSS encryption as long as it can decode a new encryption scheme (shown as NEW).

In this arrangement of **FIGURE 3**, the new DVD player utilizes a program chain defined at the time of the manufacture of the DVD that bypasses VOBUs 24 in favor of VOBUs 28 that utilize the new encryption system. Such new DVD players could be programmed to only recognize the program chain associated with the new encryption system, yet the same DVD could be backward compatible with CSS encryption as well as being compatible with the new system. The process used to distinguish between the two encryption systems is similar to that used for parental control or separate viewing angles available on some currently available DVDs.

As applied to DVDs certain embodiments of the present invention would select Video Object Unit packets which are important to the decoding of the rest of the content. The Units chosen for encryption would be duplicated and scrambled with CSS and a new improved algorithm. A new type of program chain called "security" can be created that only the new players will understand and respond to. These would be similar to how parental rating program chains are managed. Older players will simply take the program chain containing CSS scrambled packets. New players would take the security program chain with the new algorithm packets.

The use of CSS encrypted packets in one program chain assures that new DVDs work in old DVD players. The duplicated and non-CSS scrambled packets will not interfere with the old players. The duplicated packets using the new encryption algorithm can be encoded as alternate track or program chain (PGC). Thus, new players can be "forced" to take the program chain with the new encryption algorithm automatically. Like camera angle branches, branches for encryption would be tightly interleaved together. These would likely use Interleaved Blocks (ILVB). So, in the case of the arrangements depicted in **FIGURE 2-3**, the

branches used for multiple encryption as depicted herein, are preferably tightly interleaved and preferably use Interleaved Blocks.

Once the marketplace has matured somewhat and the new encryption system is standard, DVD manufacturers can begin phasing out dual encrypted DVDs as shown in **FIGURE 2-3** in favor of the format depicted in **FIGURE 4**. When the market is mature enough, the new DVDs will only be compatible with new DVD players and only the new encryption system is needed. Alternatively, the new DVDs can be dual partially encrypted with the next generation of encryption technology in the same manner as shown in **FIGURE 2-3**.

Therefore, in accordance with certain embodiments consistent with the present invention, multiple replacement encryption algorithms can be used to produce packaged media such as DVDs so that each DVD contains multiple partially encrypted content. This will allow new players to actually phase out support for the older encryption algorithms since the older DVDs would already have the new algorithm encoded into them (even prior to marketing new players).

Thus, as described, method of providing an upgrade for encryption used to encrypt video content stored in a Digital Versatile Disc (DVD) from an old encryption process to a new encryption process, consistent with certain embodiments of the invention, involves selecting a portion of video content for dual partial encryption; dual partial encrypting the video content so that the video content has a clear portion, a portion encrypted using the old encryption process and a portion encrypted using the new encryption process; storing the dual partial encrypted video content on the DVD so that a first program chain references the clear portion and the portion encrypted using the old encryption process, and so that a second program chain references the clear portion and the portion encrypted using the new encryption process.

Similarly, a method of providing an upgrade for encryption used for encryption of video content stored in package medium from an old encryption process to a new encryption process, consistent with certain embodiments of the

invention, involves selecting a portion of video content for selective encryption; duplicating the selected portion of content to produce first and second copies of the selected portion; encrypting the first copy of the selected portion using the old encryption process; encrypting the second copy of the selected portion using the new encryption process; storing the portion of the video content which is not selected as clear content on the package medium; storing the encrypted first copy and the encrypted second copy of the selected portion on the package medium.

Thus, the transition path to a newer and more secure encryption method is depicted in **FIGURE 5** where initially, at 40, manufacturers of DVDs and DVD players manufacture the players and media using the technique illustrated in **FIGURE 1** where only a single encryption process is used. During a transitional stage, the package media is dual partially encrypted to carry data encrypted by both the old encryption process and the new process at 44. Finally, at 48, the transition can be completed by phasing out the use of the original encryption process entirely. During the interim, at 44, players may be compatible with either encryption system or both and can still decode and play back the medium.

Consider now the application of dual partial encryption to the broadcast content industry. In the US cable and satellite markets, the Data Encryption Standard (DES) is primarily in use. DES is quickly becoming obsolete. The current standard version of DES as used by the cable and satellite industry generally uses a 56-bit key. With the rapidly increasing processing capabilities of PCs, decoding by a brute force trial of all possible keys with one or more computers, is rapidly becoming more feasible.

One of the most difficult things for a service provider to do is to upgrade the low level scrambling of a content delivery network. This is because of the installed base of decoders that perform decryption only based on the old encryption process and have no provision for upgrading the encryption. It is difficult for an operator to upgrade all the units in the field. This could potentially cost many millions of dollars. One possible solution is the use of Point of Deployment (POD) modules.

When they are deployed, POD modules will provide one method of changing the low level scrambling used in a network. This is accomplished by wholesale replacement of all PODs in the network. However, even replacing POD modules can be costly, and this avenue is not available for decoders that do not support PODs. As of this date, PODs have only been deployed in limited numbers in the US cable market. Using current technology, new scrambling cannot be used until all the units or modules doing the old encryption are removed from the field. This is a logistical and financial problem as mentioned earlier. The invention allows new Set-top boxes and other decoding devices to be introduced without the need to make legacy STBs and other decoders obsolete. As an impetus to replace older units, the service operator may withhold new services to these devices, an thus compel the users to get new units (performing the new algorithm) to get the new services.

Accordingly, the progression for transition to a new encryption algorithm for cable and satellite operators (and similar content providers) is similar to that depicted in **FIGURE 5** and is illustrated more explicitly in **FIGURE 6**. In this figure, the current encryption algorithm is depicted at 60 with a transitional phase at 64 being used to transition from an old encryption algorithm to a newer algorithm as new STBs or PODs are introduced. When a large installed base of newer STBs is achieved, the new encryption algorithm may be used exclusively at 68.

Thus, in accordance with certain embodiments of the present invention, a method of upgrading an encryption process for encryption of video information from an old encryption process to a new encryption process involves selecting a portion of video content for selective encryption; duplicating the selected portion of content to produce first and second copies of the selected portion; encrypting the first copy of the selected portion using the old encryption process; and encrypting the second copy of the selected portion using the new encryption process.

In order to achieve the desired dual partial encryption according to the present invention for making a transition between two encryption algorithms, a newly deployed decoder (e.g., a STB) is provided with a mechanism to distinguish

the encrypted portions of the program material. This is accomplished in the manner described in the above-referenced patent applications. In one preferred method, the dual encrypted packets are distinguished by use of separate Program Identifiers (PIDs). That is, clear packets are identified by a first packet identifier. Dual encrypted packets are identified by a pair of PIDs that distinguish the new encryption system from the old. For example, PID 101 can be associated with clear packets as well as packets encrypted under the old encryption system. PID 102 can be used to identify packets encrypted under the new encryption system and is referred to as a secondary PID or shadow PID. The new STB is provided with the PIDs associated with the program and then decodes the program by ignoring encrypted packets with PID 101 in favor of encrypted packets with PID 102. This process is described in detail in the above-referenced patent applications.

In accordance with certain embodiments consistent with the present invention, a selectively encrypted digital video signal can be embodied in a carrier wave, that has a stream of packets of video data, wherein the stream of packets when not encrypted represent a segment of video content; certain of the packets being unencrypted and certain of the packets being encrypted under a legacy encryption method and certain of the packets being encrypted under a replacement encryption method; a first segment of code that identifies the unencrypted packets by a first packet identifier (PID); and a second segment of code that identifies the encrypted packets by a second packet identifier (PID).

An authorized Set-top box such as 100 illustrated in **FIGURE 7** operating under the new encryption 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 104. When a program is received that contains encrypted content that was encrypted by any of the selective encryption techniques described in the above-referenced patent applications, the demultiplexer directs encrypted packets containing content encrypted under the new encryption algorithm and secondary

PIDS to a decrypter 108 that decrypts the packets encrypted under the new encryption system. After these packets are decrypted at 108, they are passed to a PID remapper 112. As illustrated, the PID remapper 112 receives packets that are unencrypted and bear the primary PID as well as the decrypted packets having the secondary PID. The PID remapper 112 combines the decrypted packets from decrypter 108 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 116. Some or all of the components depicted in **FIGURE 7** can be implemented as program code running on a programmed processor running code stored on an electronic storage medium.

In one embodiment of the case of package media consistent with the present invention, the decoder or player used to decode the content encrypted under the new encryption algorithm may be functionally identical to a conventional decoder or player except for the substitution of a different decrypter or different decryption algorithm. In other exemplary embodiments, the decoder or player can be designed to recognize newly encrypted program chains while ignoring program chains associated with the old encryption algorithm.

In other embodiments consistent with the present invention, a method of playback of content stored on a recording medium involves reading a portion of the recording medium to determine that the recording medium contains content containing portions encrypted under multiple encryption techniques; selecting content having portions encrypted under one of the multiple encryption techniques; and playing the content, wherein the playing comprises decrypting the encrypted portion of the content.

FIGURE 8 is a flow chart 150 that broadly illustrates the encryption process consistent with certain embodiments of the present invention starting at 154. At 158 the VOBU or other 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 any of the packets described above that generally contain data that makes it difficult to decode the content. Packets are then examined at 162 to identify packets of the specified type. At 166, the identified packets are duplicated and at 170 one set of these packets is encrypted under a the old "legacy" encryption method. The other set of identified packets is encrypted at 174 under a the new encryption method that is designed to replace the legacy encryption method. The originally identified packets are then replaced in the data with the two sets of encrypted packets at 180 and the process ends at 186. In certain embodiments, other steps are taken such as indexing the two program chains in the package medium, etc.

Thus, a method of upgrading an encryption process for encryption of video information from an old encryption process to a new encryption process, consistent with certain embodiments involves selecting a portion of video content for selective encryption. The selected portion is duplicated to produce first and second copies of the selected portion. The first copy is encrypted using the old encryption process and the second copy is encrypted using the new encryption process to produce a dual partially encrypted segment of video information that can either be broadcast over a cable or satellite system or stored in a package medium, for example, as two program chains.

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. 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.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method of providing an upgrade for encryption used to encrypt video content stored in a Digital Versatile Disc (DVD) from an old encryption process to a new encryption process, comprising:

selecting a portion of video content for dual partial encryption;

dual partial encrypting the video content so that the video content has a clear portion, a portion encrypted using the old encryption process and a portion encrypted using the new encryption process;

storing the dual partial encrypted video content on the DVD so that a first program chain references the clear portion and the portion encrypted using the old encryption process, and so that a second program chain references the clear portion and the portion encrypted using the new encryption process.

2. The method according to claim 1, wherein the selected portion comprises a collection of video object units.

3. The method according to claim 1, wherein the portion encrypted using the old encryption process and the portion encoded using the new encryption process are stored on the DVD using interleaved blocks.

4. The method according to claim 1, wherein the old encryption process comprises a process that uses the Content Scrambling Algorithm (CSS).

5. A method of providing an upgrade for encryption used for encryption of video content stored in package medium from an old encryption process to a new encryption process, comprising:

selecting a portion of video content for selective encryption;

duplicating the selected portion of content to produce first and second copies of the selected portion;

encrypting the first copy of the selected portion using the old encryption process;

encrypting the second copy of the selected portion using the new encryption process;

storing the portion of the video content which is not selected as clear content on the package medium;

storing the encrypted first copy and the encrypted second copy of the selected portion on the package medium.

6. The method according to claim 5, wherein the package medium comprises a DVD.

7. The method according to claim 5, wherein the old encryption process comprises a process that uses the Content Scrambling Algorithm (CSS).

8. The method according to claim 5, wherein the clear content and the encrypted first copy are stored as a first program chain and wherein the clear content and the encrypted second copy are stored as a second program chain.

9. A method of playback of content stored on a recording medium, comprising:

reading a portion of the recording medium to determine that the recording medium contains content containing portions encrypted under multiple encryption techniques;

selecting content having portions encrypted under one of the multiple encryption techniques; and

playing the content, wherein the playing comprises decrypting the encrypted portion of the content.

10. The method according to claim 9, wherein the multiple encryption techniques comprise a legacy encryption technique and an encryption technique to be used as a replacement for the legacy encryption technique.

11. The method according to claim 10, wherein the selected content has portions encrypted under the replacement for the legacy encryption technique.

12. The method according to claim 11, wherein the selecting comprises selecting a program chain containing the portions encrypted under the replacement for the legacy encryption technique.

13. The method according to claim 10, wherein the selected content has portions encrypted under the legacy encryption technique.

14. The method according to claim 13, wherein the selecting comprises selecting a program chain containing the portions encrypted under the legacy encryption technique.

15. A selectively encrypted digital video signal embodied in an electronic recording medium, comprising:

a sequence of packets of video data, wherein the sequence of packets when not encrypted represent a segment of video content;

wherein certain of the packets are dual encrypted using a legacy encryption method and a replacement encryption method; and

a segment of code that identifies the packets encrypted using the legacy encryption method and the packets encrypted using the replacement encryption method as separate program chains.

16. The selectively encrypted digital video signal according to claim 15, wherein the packets comprise video object units.

17. A method of providing an upgrade for encryption used for encryption of video content for electronic distribution by a content provider from an old encryption process to a new encryption process, comprising:

selecting a portion of video content for dual partial encryption;

dual partial encrypting the video content so that the video content has a clear portion, a portion encrypted using the old encryption process and a portion encrypted using the new encryption process;

transmitting the dual partial encrypted video content over a broadcast medium.

18. The method according to claim 17, wherein the broadcast medium comprises one of a cable and a satellite network.

19. The method according to claim 17, further comprising assigning program identifiers (PIDs) to distinguish between the portions encrypted using the old encryption process and the portion encrypted under the new encryption process.

20. The method according to claim 17, wherein the old encryption process comprises a data encryption standard (DES) encryption process.

21. The method according to claim 17, wherein the new encryption process comprises one of Triple DES, Advanced Encryption Standard (AES) and Common Scrambling Algorithm (CSA)

22. A method of decoding a stream of packets containing electronically distributed video content from a content provider, wherein the content is dual partially encrypted using an old encryption process and a new encryption process, comprising:

receiving the stream of dual partially encrypted video content;

discarding packets encrypted by the old encryption process;

decrypting packets encrypted by the new encryption process; and

combining the decrypted packets with unencrypted packets to create a clear stream of packets for decoding.

23. The method according to claim 22, wherein the stream of dual partially encrypted video content is received over one of a cable network and a satellite network.

24. The method according to claim 22, wherein program identifiers (PIDs) are used to distinguish between the portions encrypted using the old encryption process and the portion encrypted under the new encryption process, and wherein the discarding comprises discarding packets identified by the PID associated with the old encryption process.

25. The method according to claim 22, wherein the old encryption process comprises a data encryption standard (DES) encryption process.

26. The method according to claim 22, wherein the new encryption process comprises one of Triple DES, Advanced Encryption Standard (AES) and Common Scrambling Algorithm (CSA)

27. A selectively encrypted digital video signal embodied in a carrier wave, comprising:

a stream of packets of video data, wherein the stream of packets when not encrypted represent a segment of video content;

certain of the packets being unencrypted and certain of the packets being encrypted under a legacy encryption method and certain of the packets being encrypted under a replacement encryption method;

a first segment of code that identifies the unencrypted packets by a first packet identifier (PID); and

a second segment of code that identifies the encrypted packets by a second packet identifier (PID).

28. The method according to claim 27, wherein the carrier wave is broadcast using one of a cable network and a satellite network.

29. The method according to claim 27, wherein the legacy encryption process comprises a data encryption standard (DES) encryption process.

30. The method according to claim 27, wherein the replacement encryption process comprises one of Triple DES, Advanced Encryption Standard (AES) and Common Scrambling Algorithm (CSA).

31. A method of upgrading an encryption process for encryption of video information from an old encryption process to a new encryption process, comprising:

selecting a portion of video content for selective encryption;

duplicating the selected portion of content to produce first and second copies of the selected portion;

encrypting the first copy of the selected portion using the old encryption process; and

encrypting the second copy of the selected portion using the new encryption process.

32. The method according to claim 31, further comprising transmitting the encrypted first copy and encrypted second copy along with unselected portions of the video content over one of a cable network and a satellite network.

33. The method according to claim 31, further comprising distinguishing between the portions encrypted using the old encryption process and the portion encrypted under the new encryption process by assigning distinctive program identifiers (PIDs) to each.

34. The method according to claim 31, wherein the old encryption process comprises a data encryption standard (DES) encryption process.

35. The method according to claim 31, wherein the new encryption process comprises one of Triple DES, Advanced Encryption Standard (AES) and Common Scrambling Algorithm (CSA).

36. The method according to claim 31, further comprising storing the encrypted first copy and encrypted second copy along with unselected portions of the video content a digital versatile disc DVD.

37. The method according to claim 36, wherein the old encryption process comprises a process that uses the Content Scrambling Algorithm (CSS).

38. The method according to claim 36, wherein the unselected portion and the encrypted first copy are stored as a first program chain and wherein the unselected portion and the encrypted second copy are stored as a second program chain.

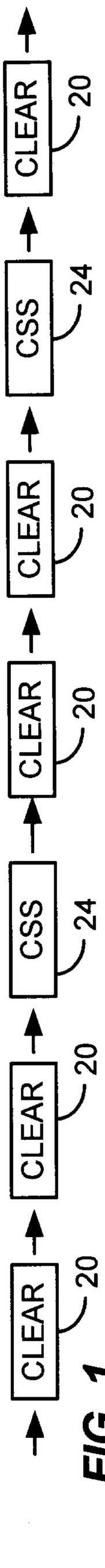


FIG. 1



FIG. 2

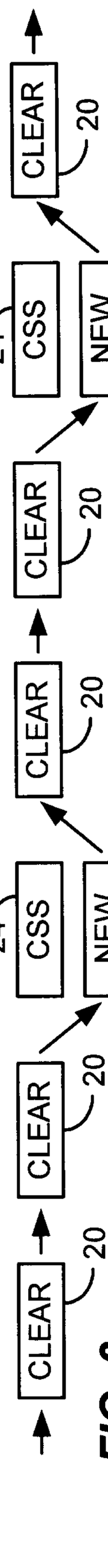


FIG. 3

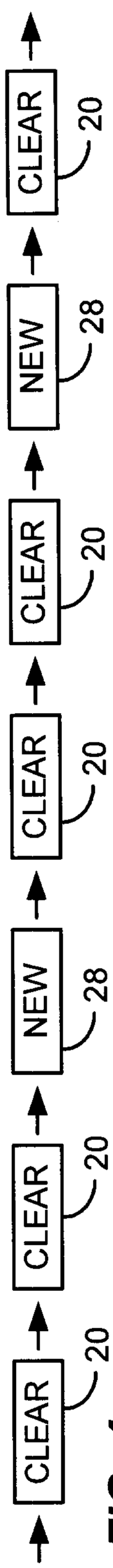


FIG. 4

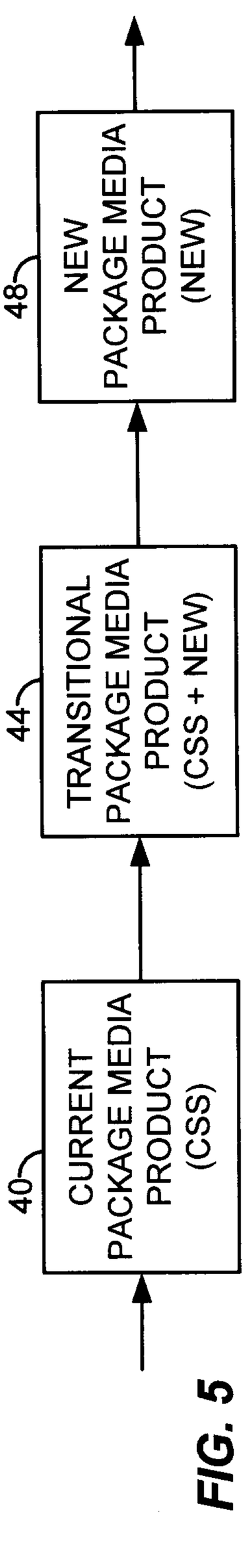


FIG. 5

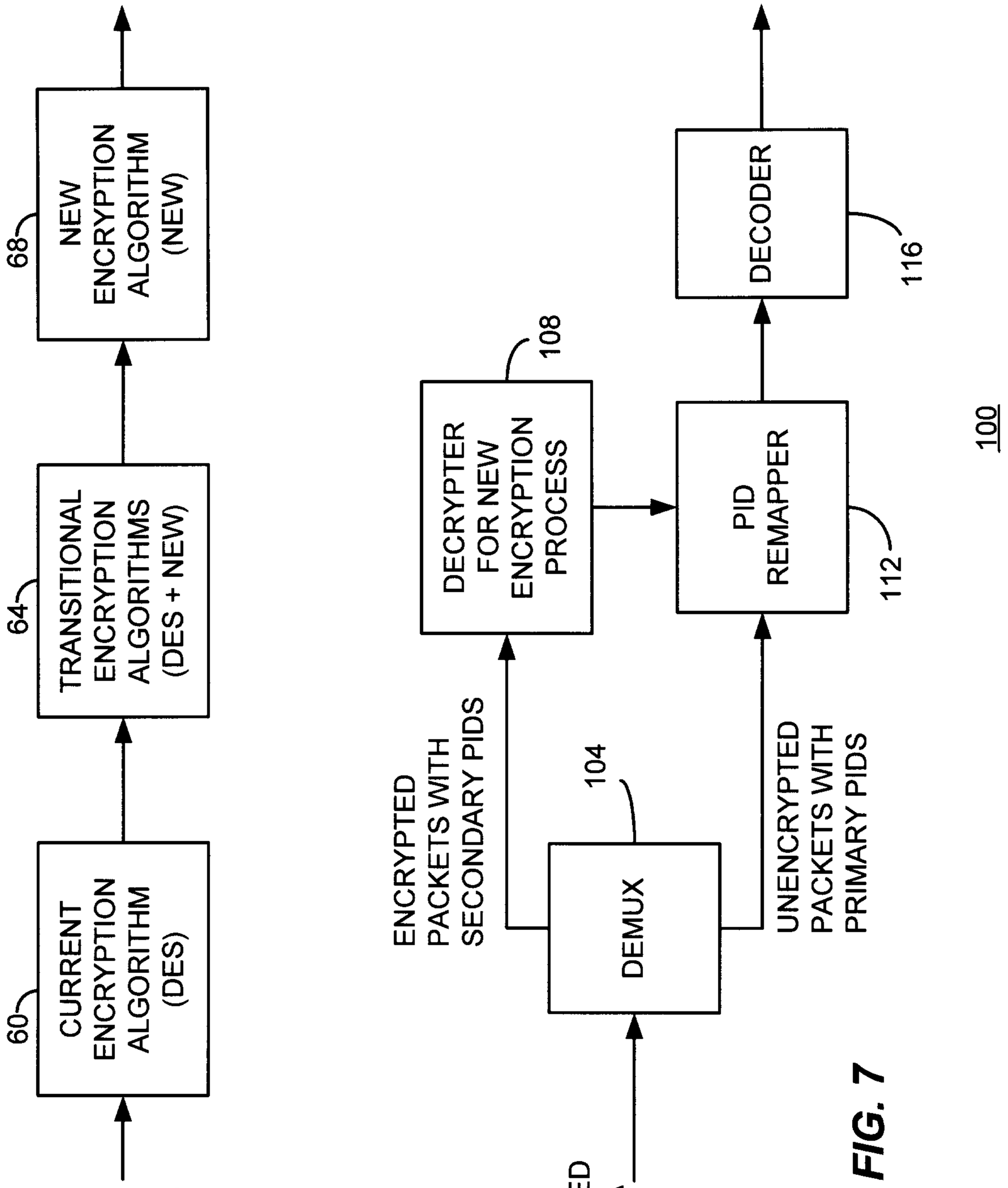

MULTIPLEXED VIDEO DATA STREAM
ENCRYPTED PACKETS WITH SECONDARY PIDS
UNENCRYPTED PACKETS WITH PRIMARY PIDS
DEMUX
104
DECRYPTER FOR NEW ENCRYPTION PROCESS
108
PID REMAPPER
112
DECODER
116
100
CURRENT ENCRYPTION ALGORITHM (DES)
60
TRANSITIONAL ENCRYPTION ALGORITHMS (DES + NEW)
64
NEW ENCRYPTION ALGORITHM (NEW)
68

FIG. 6

FIG. 7

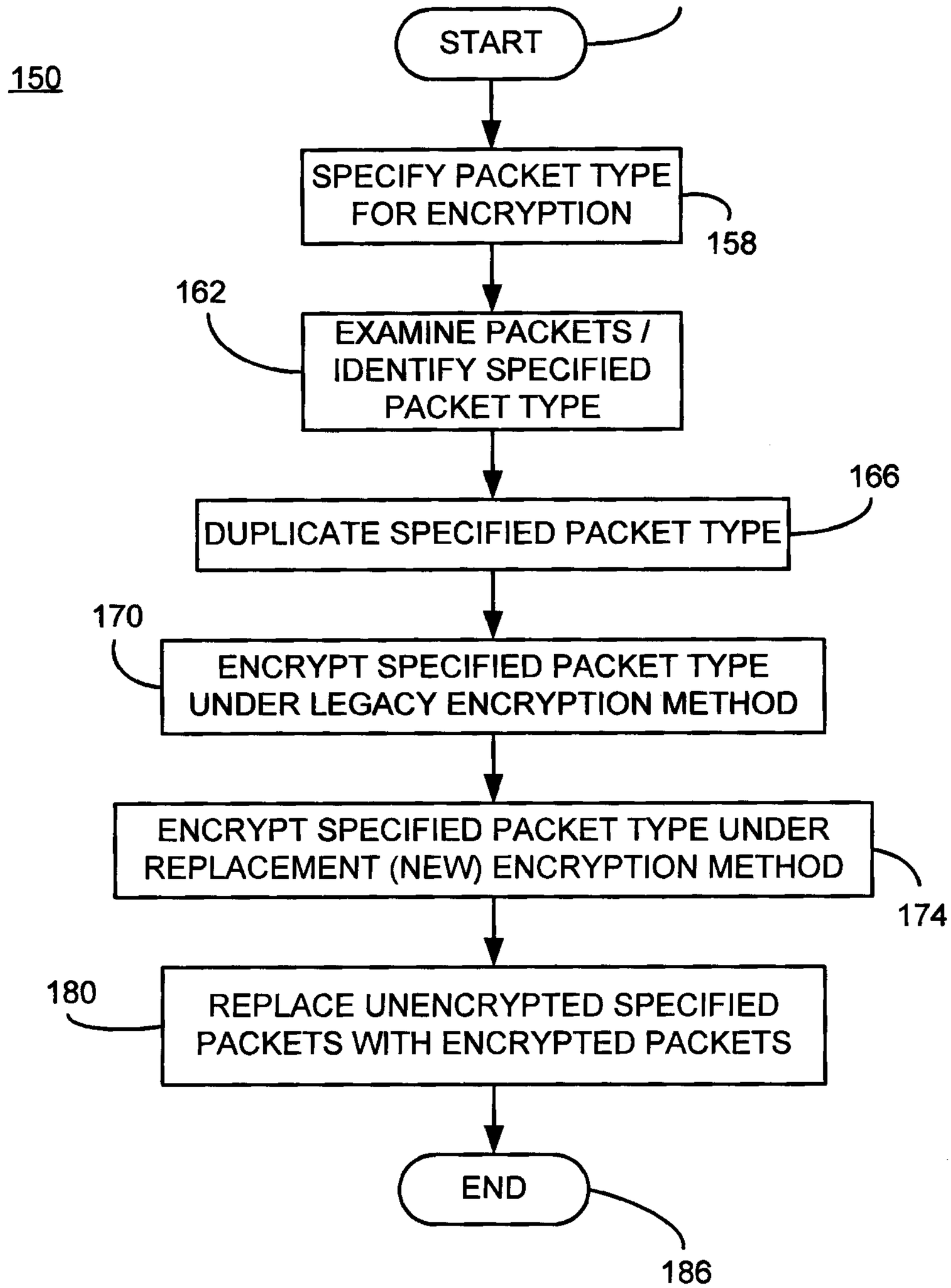
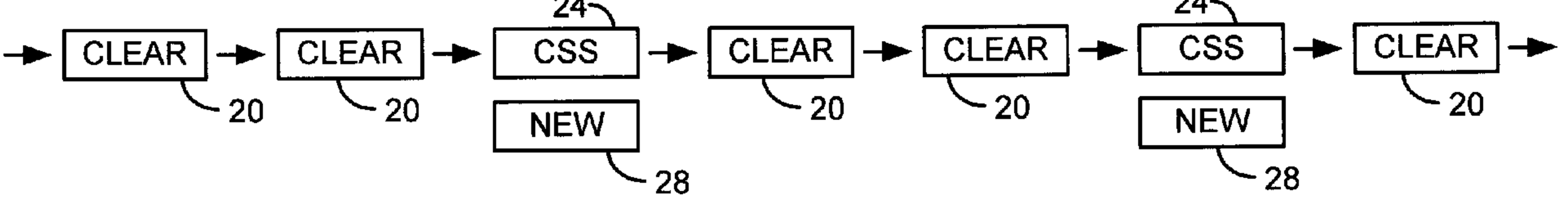

150
START
SPECIFY PACKET TYPE FOR ENCRYPTION
158
162
EXAMINE PACKETS / IDENTIFY SPECIFIED PACKET TYPE
166
DUPLICATE SPECIFIED PACKET TYPE
170
ENCRYPT SPECIFIED PACKET TYPE UNDER LEGACY ENCRYPTION METHOD
ENCRYPT SPECIFIED PACKET TYPE UNDER REPLACEMENT (NEW) ENCRYPTION METHOD
174
180
REPLACE UNENCRYPTED SPECIFIED PACKETS WITH ENCRYPTED PACKETS
END
186

FIG. 8


CLEAR
20
CLEAR
20
24
CSS
NEW
28
CLEAR
20
CLEAR
20
24
CSS
NEW
28
CLEAR
20