US00RE41074E

(19) **United States**

(12) **Reissued Patent**

Park

(10) **Patent Number: US RE41,074 E**

(45) **Date of Reissued Patent: Jan. 12, 2010**

(54) **COPY PREVENTION METHOD AND APPARATUS FOR DIGITAL VIDEO SYSTEM**

(76) Inventor: **Tae Joon Park**, Seoul (KR)

(21) Appl. No.: **11/040,606**

(22) Filed: **Jan. 24, 2005**

Related U.S. Patent Documents

Reissue of:

(64) Patent No.: **6,347,144**
Issued: **Feb. 12, 2002**
Appl. No.: **09/497,465**
Filed: **Feb. 3, 2000**

U.S. Applications:

(63) Continuation of application No. 09/053,288, filed on Apr. 1, 1998, now Pat. No. 6,028,932, which is a continuation of application No. 08/562,042, filed on Nov. 22, 1995, now Pat. No. 5,761,302.

(30) **Foreign Application Priority Data**

Nov. 26, 1994 (KR) 94-31373

(51) **Int. Cl.**
H04N 7/167 (2006.01)
H04K 1/00 (2006.01)
H04L 9/00 (2006.01)

(52) **U.S. Cl.** **380/201**; 380/228; 705/57; 705/58

(58) **Field of Classification Search** ..... None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,554,461	A	11/1985	Oho et al.
4,694,489	A	9/1987	Frederiksen

(Continued)

FOREIGN PATENT DOCUMENTS

EP	0 267 039	A2	5/1988
EP	0 498 617	A2	8/1992
EP	0 519 320	A2	12/1992
EP	0 580 367	A2	1/1994
EP	0 581 227-A 2		2/1994
EP	0 589 459	A1	3/1994
JP	6-070282		3/1994
JP	6-162690		6/1994
JP	6-199288		7/1994
JP	6-339110		12/1994

OTHER PUBLICATIONS

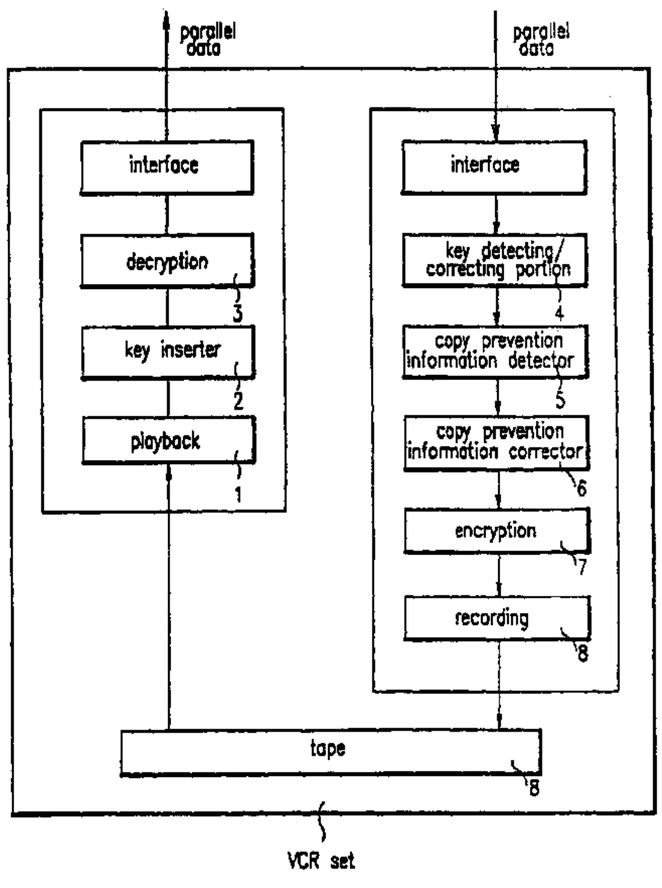
Derfler, F. J. et al., "How Networks Work".
Gralla, P., "How The Internet Works".
Muller, N. J., "Desktop Encyclopedia of the Internet".
White, R., "How Computers Work".

Primary Examiner—Benjamin E Lanier

(57) **ABSTRACT**

[A copy prevention method and apparatus for a digital video system is disclosed including the steps of: (a) adding a header area of a header start code and key field to a reproduced bit stream: (b) decrypting and transmitting the bit stream to which the header area is added: (c) detecting a key field of the decrypted and transmitted bit stream and detecting copy prevention information; and (d) encrypting the bit stream according to information detected from stop (c) and recording it an tape.] *A copy protection method including receiving encrypted digital data to be recorded, key information which is required to decrypt the encrypted digital data, and first copy control information which indicates a copy permission status of the encrypted digital data; and recording the encrypted digital data, the key information, and second copy control information on a digital recording medium, based on at least a status of the first copy control information.*

71 Claims, 7 Drawing Sheets



U.S. PATENT DOCUMENTS

4,796,220	A		1/1989	Wolfe
4,817,140	A		3/1989	Chandra et al.
4,871,140	A		10/1989	Hoskinson et al.
4,890,319	A		12/1989	Seth-Smith et al.
4,937,679	A		6/1990	Ryan
5,003,590	A		3/1991	Lechner et al.
5,014,274	A		5/1991	Higurashi et al.
5,034,981	A		7/1991	Leonard et al.
5,034,985	A		7/1991	Keough
5,054,064	A		10/1991	Walker et al.
5,057,947	A		10/1991	Shimada
5,058,162	A		10/1991	Santon et al.
5,073,925	A		12/1991	Nagata et al.
5,109,413	A		4/1992	Comerford et al.
5,134,656	A		7/1992	Kudelski
5,231,546	A		7/1993	Shimada
5,243,650	A		9/1993	Roth et al.
5,303,294	A		4/1994	Kimoto et al.
5,315,448	A		5/1994	Ryan
5,323,244	A		6/1994	Yamaguchi et al.
5,392,351	A		2/1995	Hasebe et al.
5,406,625	A		4/1995	Kotaka et al.
5,418,853	A		5/1995	Kanota et al.
5,477,276	A		12/1995	Oguro
5,506,903	A		4/1996	Yamashita et al.
5,513,260	A		4/1996	Ryan
5,530,756	A		6/1996	Bourel et al.
5,546,461	A		8/1996	Ibaraki et al.
5,574,787	A		11/1996	Ryan
5,576,843	A		11/1996	Cookson et al.
5,579,120	A		11/1996	Oguro
5,588,058	A		12/1996	Le Berre
5,629,980	A		5/1997	Stefik et al.
5,646,992	A	*	7/1997	Subler et al. 705/53
5,659,613	A		8/1997	Copeland et al.
5,673,357	A		9/1997	Shima
5,689,559	A		11/1997	Park
5,689,561	A		11/1997	Pace
5,757,909	A		5/1998	Park
5,757,910	A		5/1998	Rim
5,761,302	A		6/1998	Park
5,778,064	A		7/1998	Kori et al.
5,799,081	A		8/1998	Kim et al.
5,832,084	A		11/1998	Park
5,862,115	A		1/1999	Matsui et al.
5,881,038	A		3/1999	Oshima et al.
5,898,695	A		4/1999	Fujii et al.
5,907,443	A		5/1999	Hirata
6,028,932	A		2/2000	Park
6,052,242	A		4/2000	Hirata
RE36,763	E		7/2000	Kanota et al.
6,236,971	B1		5/2001	Stefik et al.
6,430,290	B1		8/2002	Van Willigen et al.
7,114,745	B2		10/2006	Schütz et al.

* cited by examiner

FIG.1
prior art

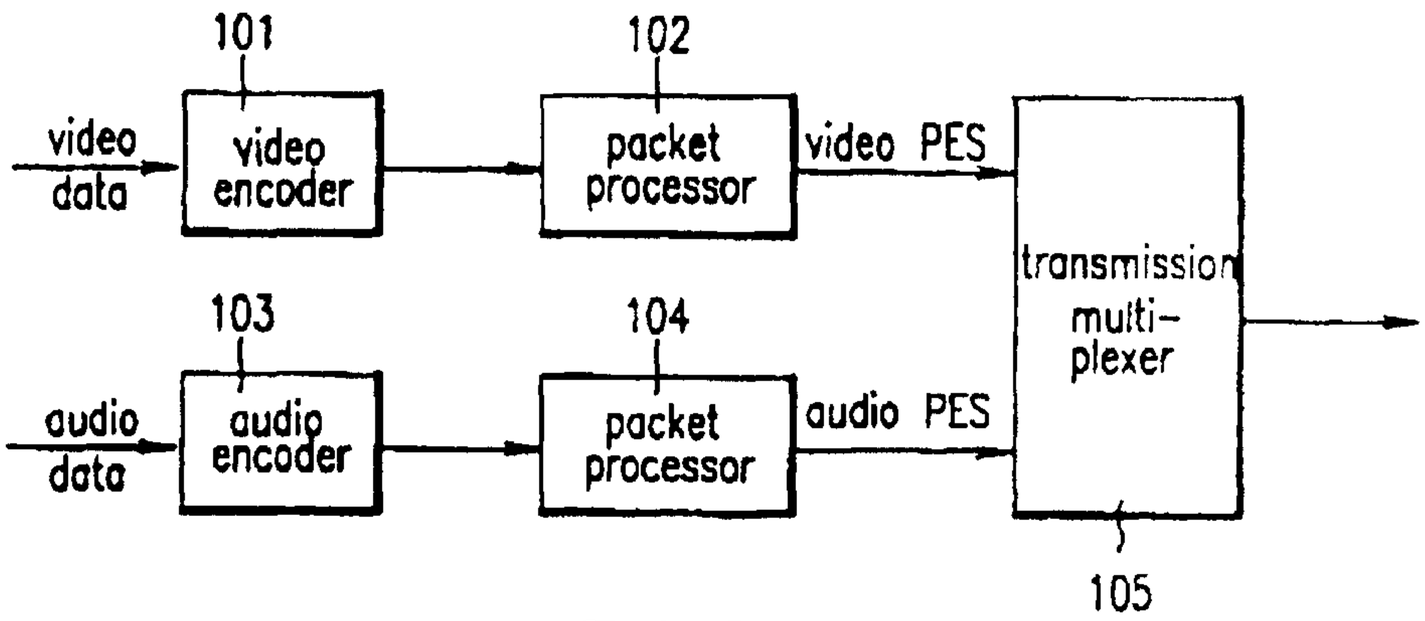


FIG.2

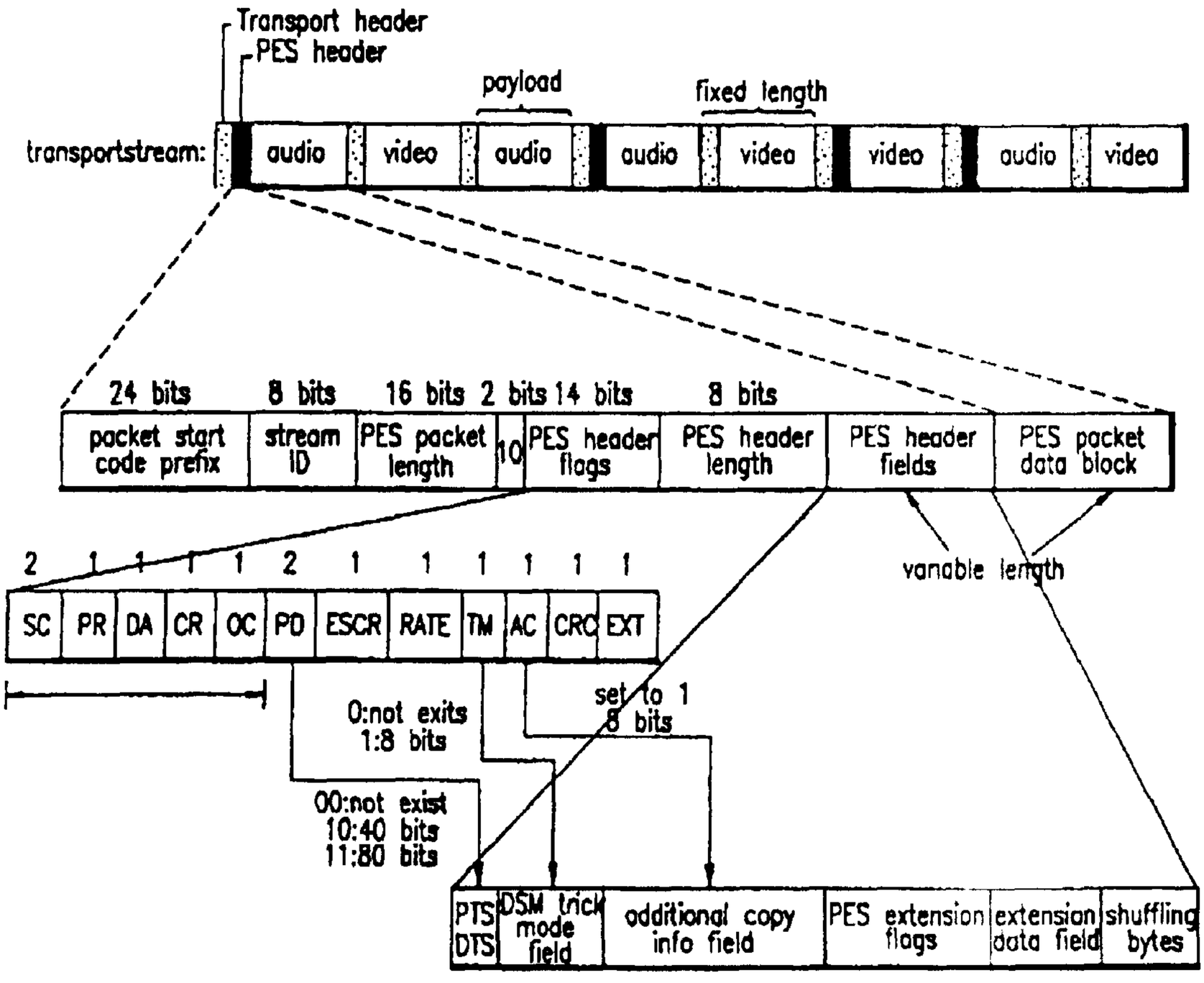


FIG.3
prior art

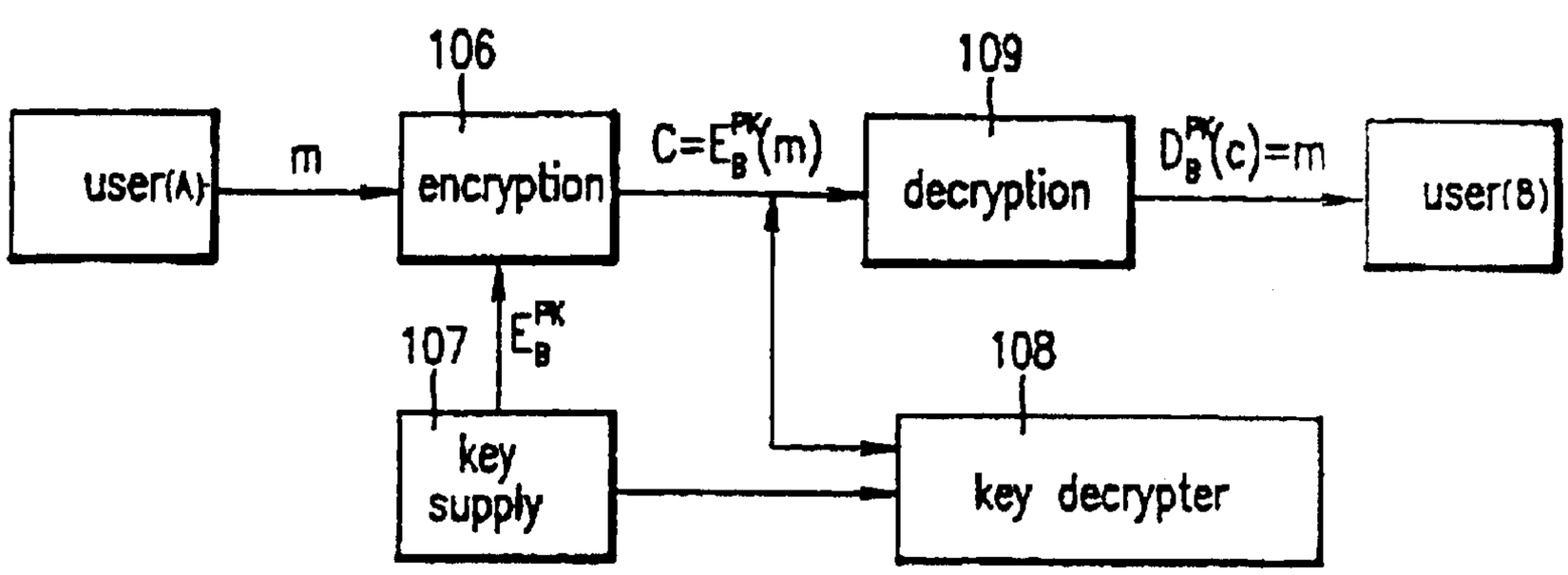


FIG.4

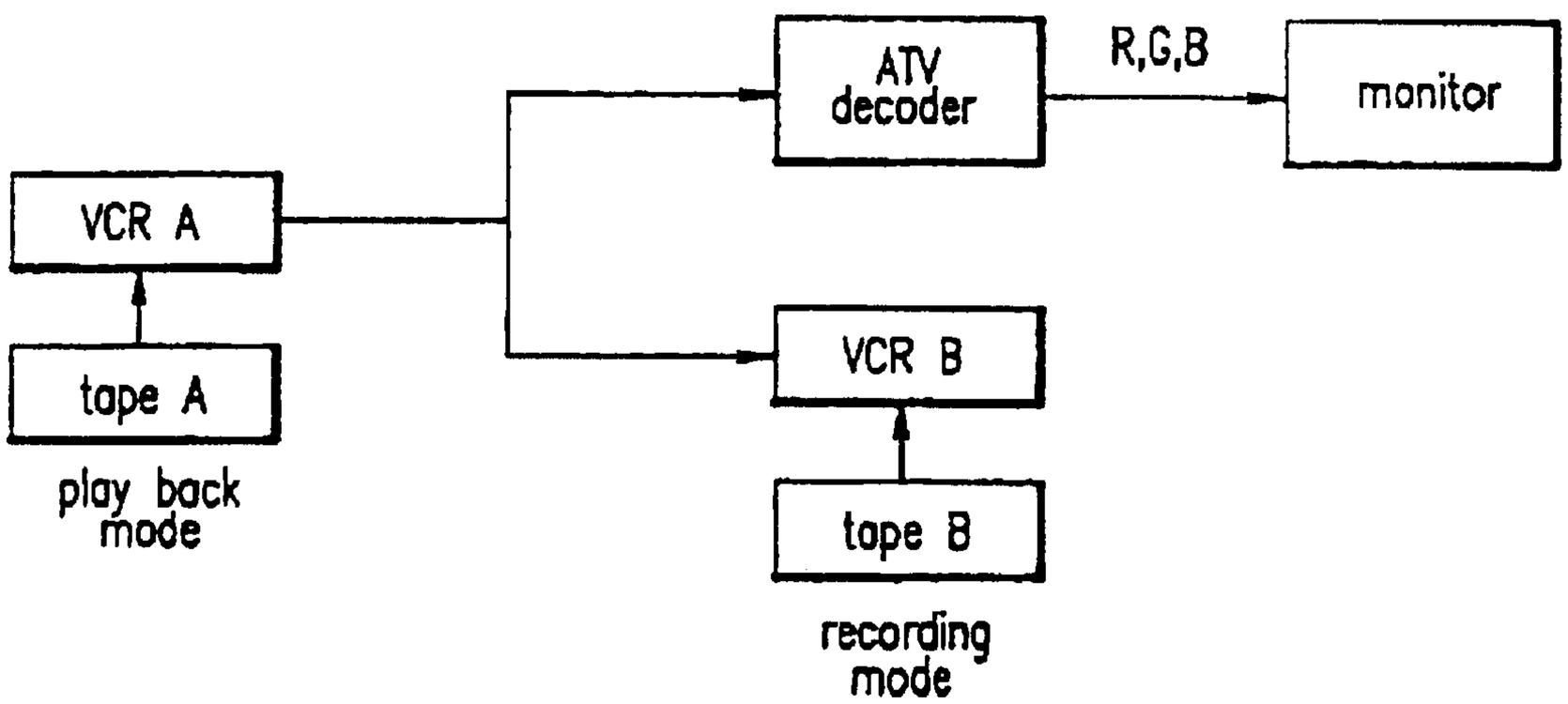


FIG.5

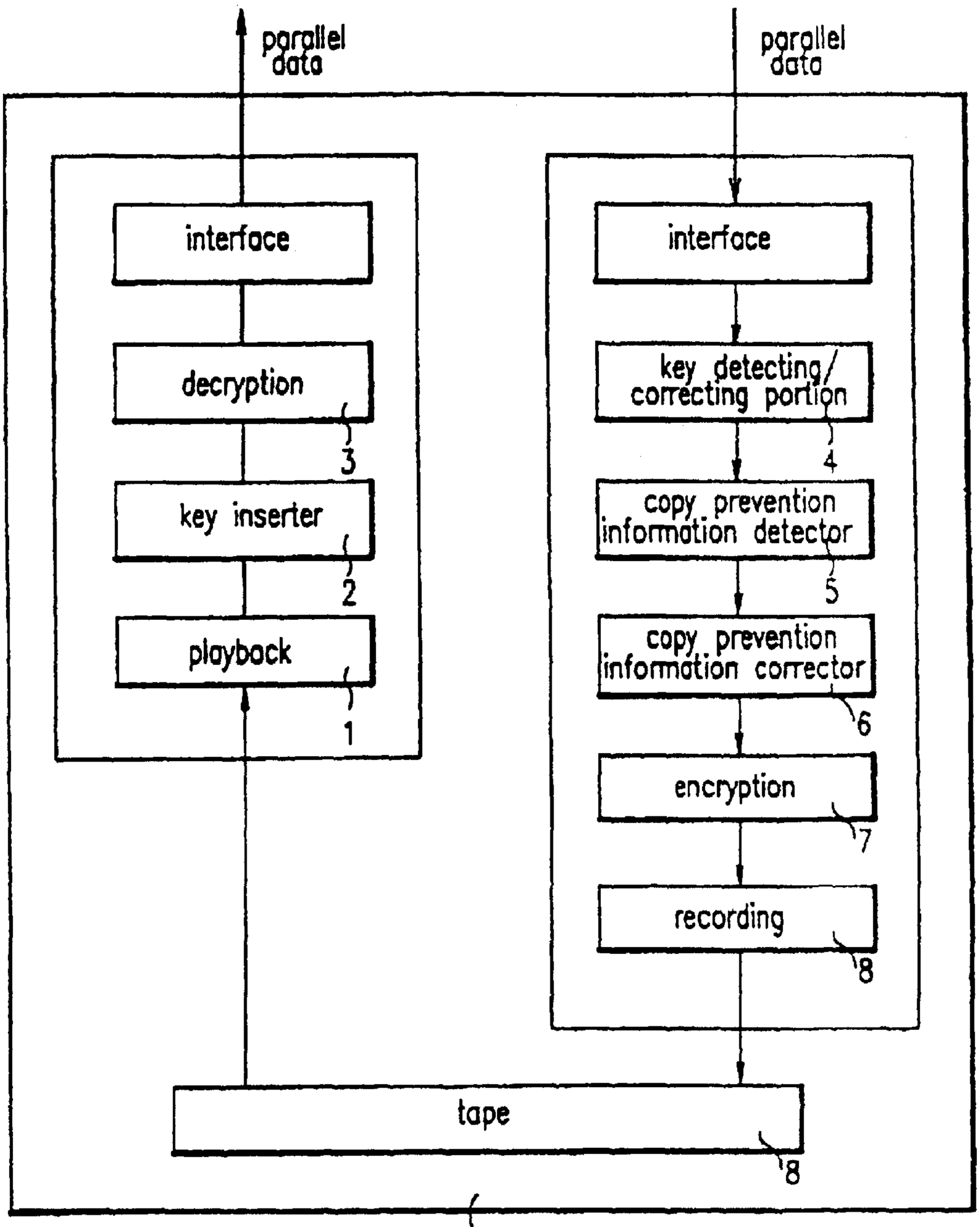

parallel data
parallel data
interface
decryption
3
key inserter
2
playback
1
interface
key detecting/ correcting portion
4
copy prevention information detector
5
copy prevention information corrector
6
encryption
7
recording
8
tape
8
VCR set

FIG.6

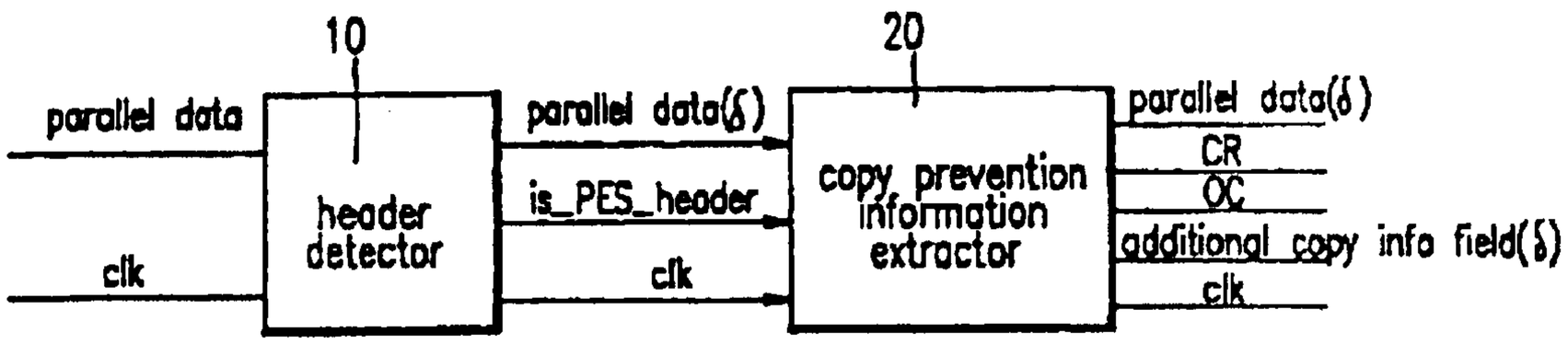
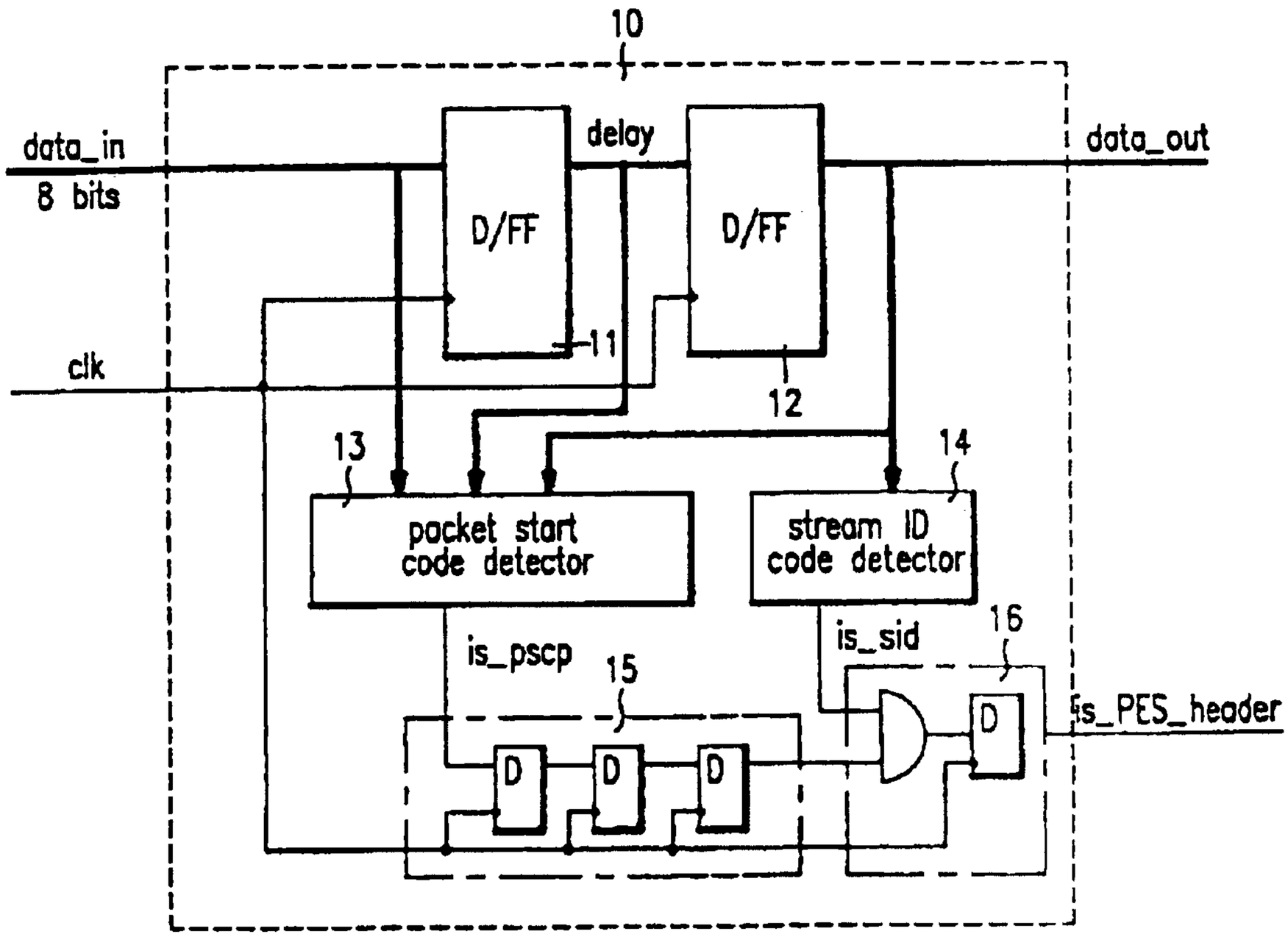

10
20
parallel data
clk
header detector
parallel data(δ)
is_PES_header
clk
copy prevention information extractor
parallel data(δ)
CR
OC
additional copy info field(δ)
clk

FIG.7


10
data_in
8 bits
delay
D/FF
D/FF
data_out
clk
11
12
13
14
pocket start code detector
stream ID code detector
is_pscp
15
is_sid
16
D
D
D
D
is_PES_header

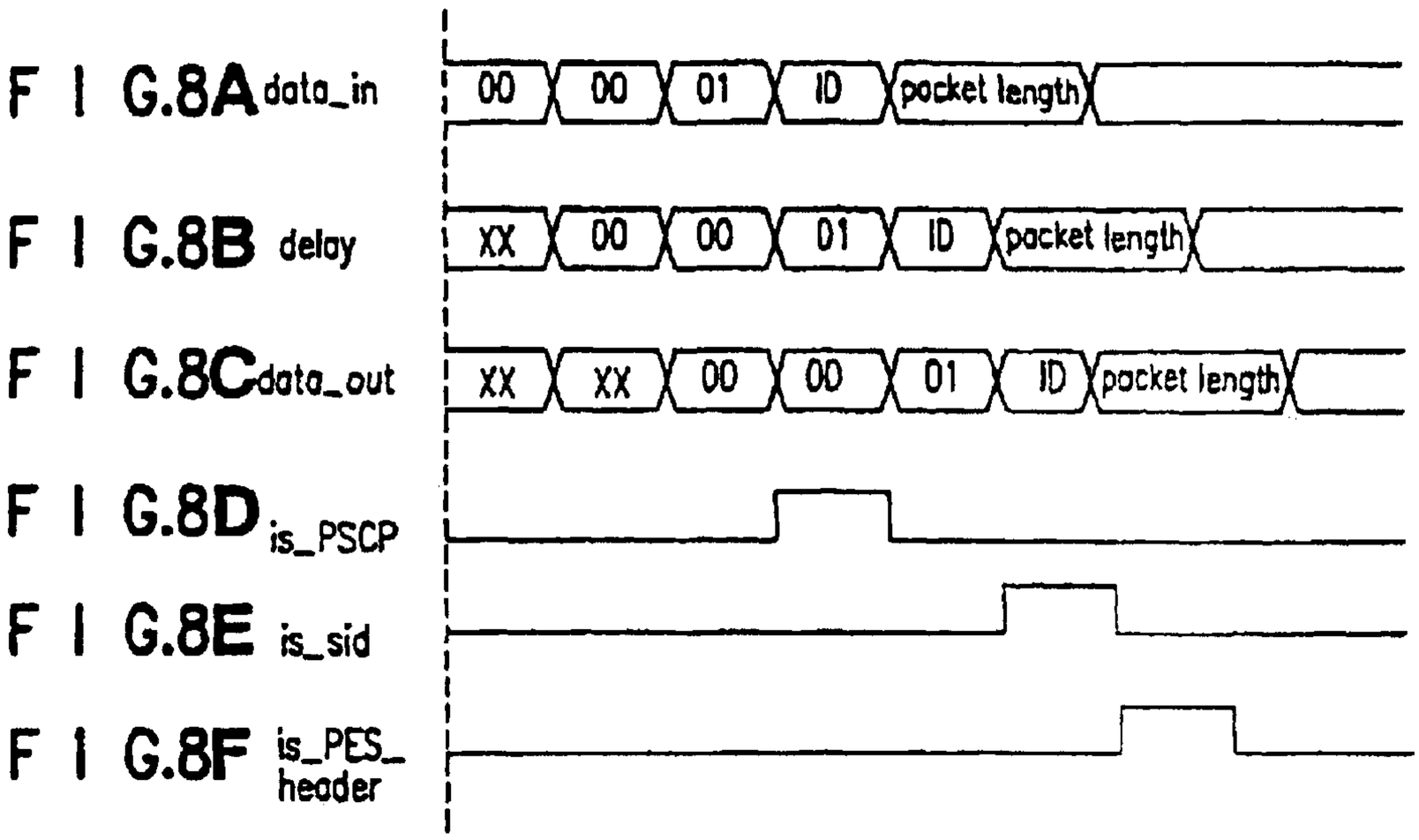


FIG.8A data_in
00
00
01
ID
packet length
FIG.8B delay
XX
00
00
01
ID
packet length
FIG.8C data_out
XX
XX
00
00
01
ID
packet length
FIG.8D is_PSCP
FIG.8E is_sid
FIG.8F is_PES_ header

FIG.9

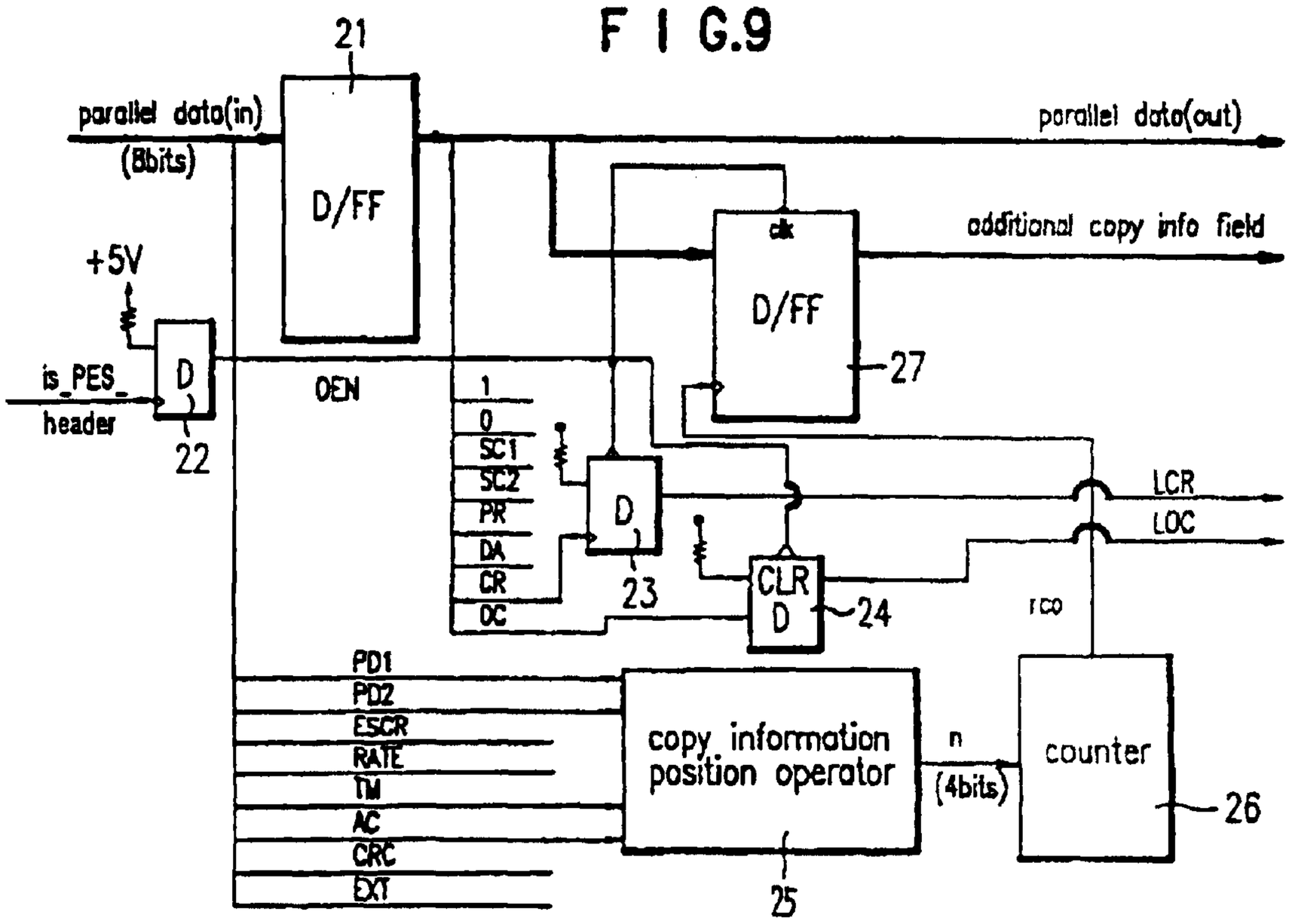

21
parallel data(in)
(8bits)
D/FF
parallel data(out)
additional copy info field
clk
D/FF
27
+5V
is_PES_ header
D
22
OEN
1
0
SC1
SC2
PR
DA
CR
OC
D
23
CLR
D
24
LCR
LOC
rco
PD1
PD2
ESCR
RATE
TM
AC
CRC
EXT
copy information position operator
25
n
(4bits)
counter
26

FIG.10A

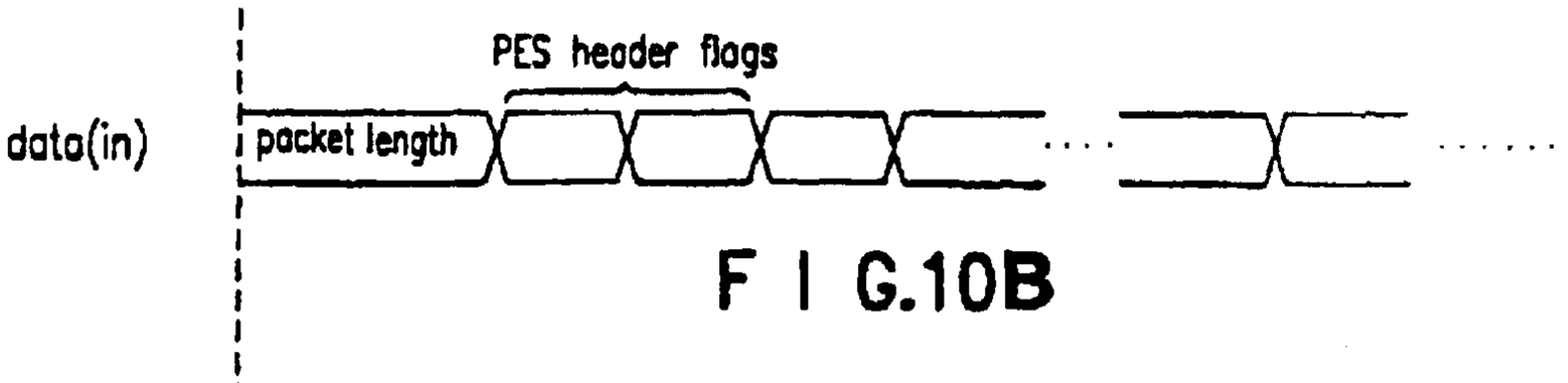


FIG.10B

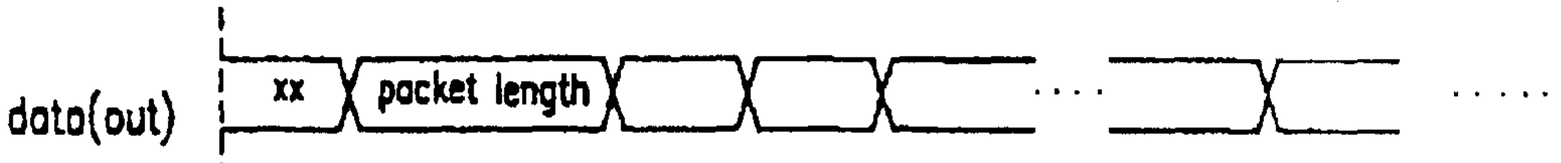


FIG.10C

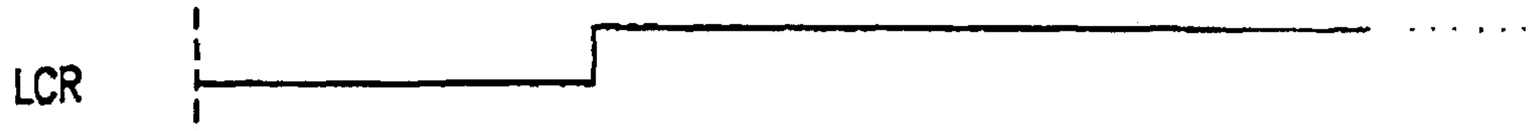


FIG.10D

FIG.10E

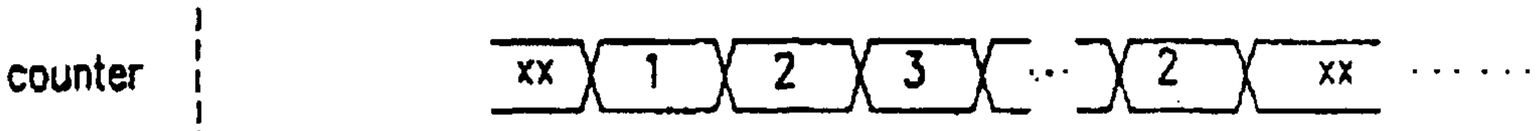


FIG.10F

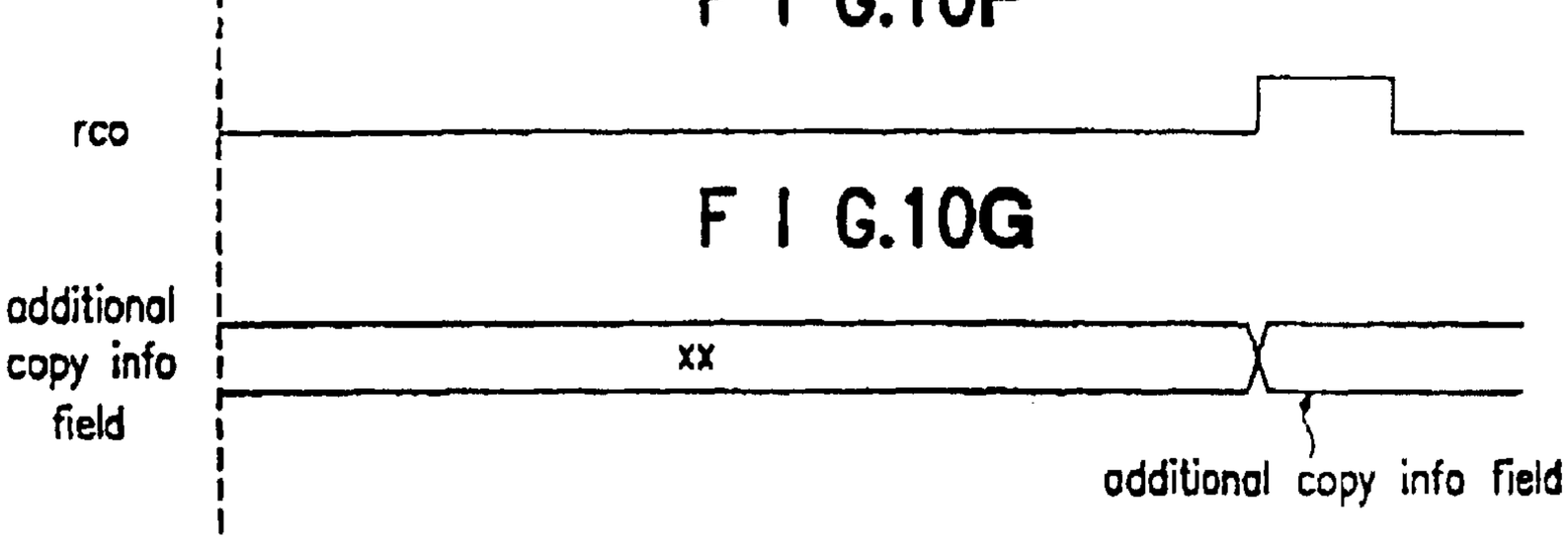


FIG.10G

FIG.11A

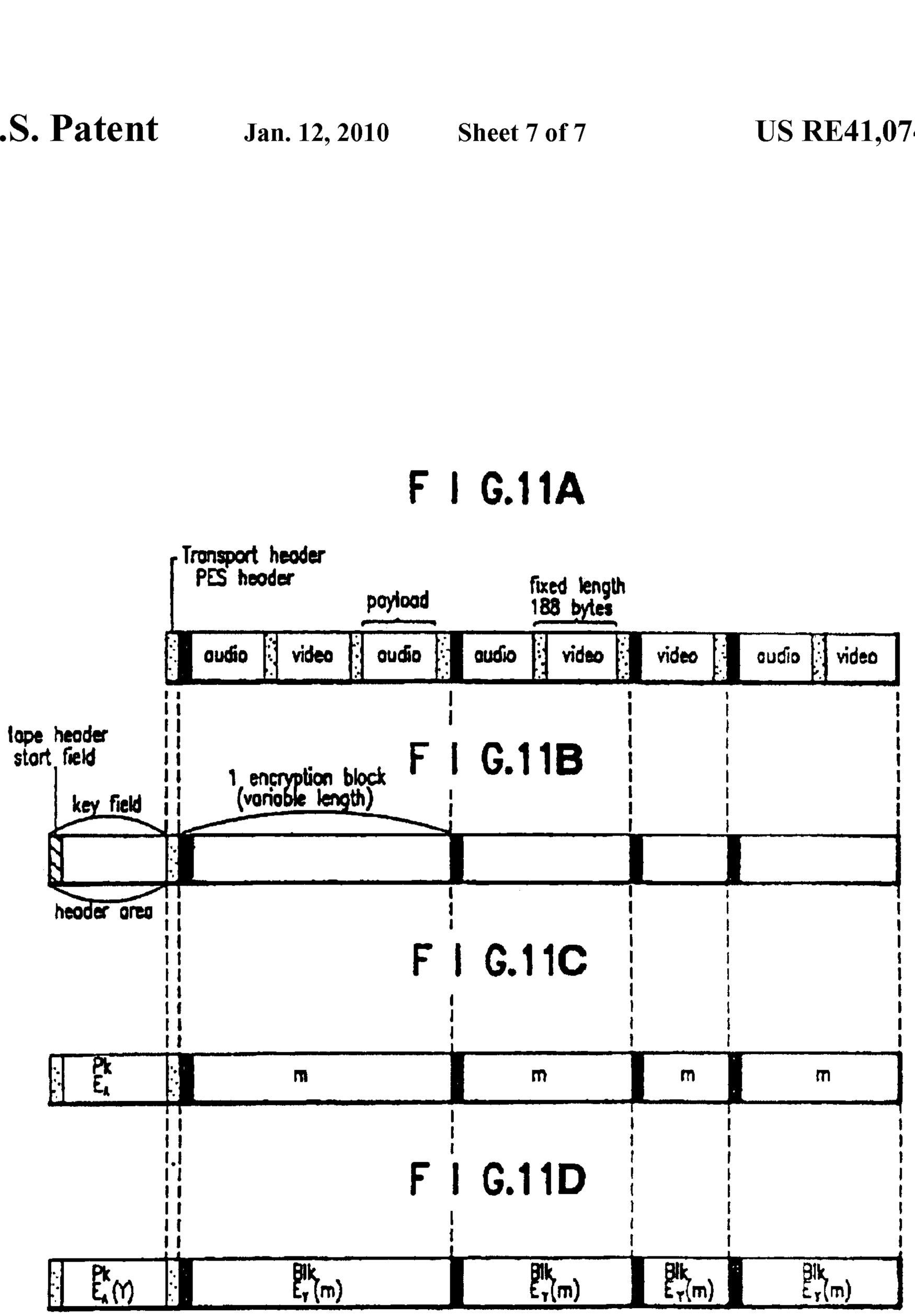


FIG.11B

FIG.11C

FIG.11D

COPY PREVENTION METHOD AND APPARATUS FOR DIGITAL VIDEO SYSTEM

Matter enclosed in heavy brackets [ ] appears in the original patent but forms no part of this reissue specification; matter printed in italics indicates the additions made by reissue.

[This is a continuation of application Ser. No. 09/053,288, filed Apr. 1, 1998, now U.S. Pat. No. 6,028,932, which is a continuation of Ser. No. 08/562,042, filed Nov. 22, 1995, now U.S. Pat. No. 5,761,302, issued Jun. 2, 1998.] *This is a reissue application of U.S. Pat. No. 6,347,144, which is a continuation of application Ser. No. 09/053,288, filed Apr. 1, 1998, now U.S. Pat. No. 6,028,932, which is a continuation of Ser. No. 08/562,042, filed Nov. 22, 1995, now U.S. Pat. No. 5,761,302. The contents of all these applications are incorporated by reference. The above-identified applications also claim priority to Korean Application No. 94-31373 filed on Nov. 26, 1994.*

BACKGROUND OF THE INVENTION

The present invention relates to a copy prevention technology for a digital video system, and more particularly, to a copy prevention method and apparatus for a digital VCR to which encryption is introduced to display a picture only in a VCR internally containing a corresponding encryption code, thereby preventing tape from being copied.

General copy prevention methods for analog VCR are presented in U.S. Pat. Nos. 4,819,098, 4,571,642 and 4,577,216.

First, U.S. Pat. NO. 4,819,098 discloses a method in which an interference signal is inserted into a video waveform in an automatic gain control circuit (AGC) of a VCR. Here, the inserted signal does not affect the AGC of its monitor but has the AGC of the VCR record an accurate level of signal on a video tape.

In U.S. Pat. No. [4,571,642] *4,577,216*, there is presented a method in which a phase noise or other corrected signal is inserted into the [chrome] *chroma* burst of a video waveform.

However, all the conventional technologies insert a distributing signal to an analog signal using the difference between a circuit of a monitor and a corresponding circuit of a VCR. Some VCRs may perform copy normally despite of copy prevention. Some monitors cannot display images of the original video tape. A conventional copy prevention introduced to an analog VCR system is hard to be applied to digital storage media (DSM).

Specifically, in a satellite or high-definition TV decoder, as shown in FIG. **2**, an MPEG bit stream received by a digital VCR is constructed to transmit a transport header, packetized elementary stream [(PEG)] (*PES*) header and audio and video data respectively or simultaneously.

The PES header contains a PES header flag area of 14 bits which is a field for DSM such as digital VCR, and a PES header field having a variable length. The PES header flag area includes 1-bit copyright (CR) flag, 1-bit original-or-copy (OC) flag, 2-bit PD flag, 1-bit TM flag, and 1-bit AC flag.

The PES header field varies in length, and part thereof is set by the [PC] *PD*, TM and AC flags. A PTS/DTS area is not present if the value of the PD flag is "00". It is 40 bits if the value "10". If the value is "11", the area is 80 bits. A DSM trick mode field is not present if the TM flag is "0". If the flag is "1", the field is 8 bits. An additional copy information field is 8 bits if the AC flag is "1".

When recording is carried out by the satellite receiver or high-definition TV decoder and compressed video data is encoded in encoder **101**, it is converted into a packet form in packet processing portion **[122]** *102* as shown in FIG. **1**. If the compressed audio data is encoded in audio encoder **103**, it is converted into a packet form in packet processing portion **104**.

When the outputs of packet processing portions **102** and **104** are multiplexed in transmission multiplexer **105**, a fixed transmission stream shown in FIG. **2** is output to a digital VCR. In this case, for copy prevention, a public-key encryption is applied which is suggested in U.S. Pat. No. 4,200,770. This solves disadvantages in key management or key distribution when a conventional block-cipher or stream cipher algorithm such as data encryption standard (DES) encrypts or decrypts only with a secret key.

This public-key encryption system has all users U hold unique encryption algorithm E^{PK}_{U} and description algorithm D^{PK}_{U}. Here, encryption algorithm E^{PK}_{U} for the public-key is opened as a public-key to key supply portion **107**. Decryption algorithm D_{PKU} for secret key is kept in secret. The characteristics of E^{PK}_{U} and D^{PK}_{U} are as follows.

First, with respect to all users U and message m transmitted, $D^{PK}_{U}(E^{PK}_{U}(m))=m$.

Second, encryption algorithm E^{PK}_{U} and decryption algorithm D^{PK}_{U} do not require complicated calculation.

Third, it is impossible to find $D^{PK''}_{U}$ satisfying $D^{PK''}_{U}(E^{PK}_{U}(m))=m$ from encryption algorithm E^{PK}_{U}.

In the encryption system having the above characteristics, as shown in FIG. **3**, when user A transmits message m to user B, encryptor **106** receiving public-key algorithm E^{PK}_{U} for user B's public-key from key supply portion **107** encrypts message m $(E^{PK}_{U}(m))=c$ and transmits the result to decrypter **109** via a public channel. Here, the public channel indicates a channel in which transmitted data is not kept in secret.

Key decrypter **108** receiving the key information from key supply portion **107** outputs an algorithm D^{PK}_{B}, corresponding to encryption algorithm E^{PK}_{B}, decryptor **109** decrypts $(D^{PK}_{B}(c))=m$ the output of encrypter **106** with decryption algorithm D^{PK}_{B}, and then transmits *to* user B. In other words, only user B can decrypt decryption algorithm D^{PK}_{B} corresponding to encryption algorithm E^{PK}_{B}.

A concept developed from the public-key encryption is presented in U.S. Pat. No. 4,405,829. This public-key encryption system is called RSA system. A method in which the RSA public-key encryption is efficiently calculated via batch processing is presented in U.S. Pat. No. 4,964,164.

However, this public-key encryption is inappropriate for high-velocity encryption. A CA system is *intended* to [present] *prevent* illegal [view] *viewing*. However, there is no method of protecting a program distributed through a digital storage medium such as *a* digital VCR.

SUMMARY OF THE INVENTION

Therefore, it is an object of the present invention to an illegal copy prevention method and apparatus for a digital video system in which, in copy tape, encrypted key information is transmitted and recorded so that a copied tape is reproducible only in a VCR having a corresponding encrypted key information, thereby prevented copy.

[To accomplish the object of the present invention, there is provided a copy prevention method for a digital video sys-

tem comprising the steps of: (a) adding a header area of a header start code and key field to a reproduced bit stream; (b) decrypting and transmitting the bit stream to which the header area is added; (c) detecting a key field of the decrypted and transmitted bit stream and detecting copy prevention information; and (d) encrypting the bit stream according to information detected from step (c) and recording it on tape.]

[For the object of the present invention, there is provided a copy prevention apparatus for a digital video system comprising: a reproduction block for adding key information to a reproduced bit stream, and decrypting and transmitting it; and a recording block for searching key information of the bit stream transmitted from the reproduction block is extract copy prevention information, and encrypting and recording the bit stream according to the extracted copy prevention information.]

[The reproduction block comprises: reproduction means for reproducing data recorded on tape; key insertion means for adding key information to the bit stream of the reproduction means; and decryption means for decrypting the output of the key insertion means and transmitting it to a recording-side VCR.]

[The recording block comprises: key detecting/correcting means for detecting key information from the transmitted bit stream of a reproducing-side VCR: copy prevention information detecting means for searching the key information detected from the key detecting/correcting means to detect copy prevention information; encrypting means for encrypting the bit stream according the copy prevention information of the copy prevention information detecting means; and recording means for recording the bit stream encrypted in the encrypting means.]

[The copy prevention information detecting means comprises: a PES header detecting portion for detecting a PES header from parallel data output from the key detecting/correcting means; and a copy prevention information extractor enabled by a PES header detection signal of the PES header detecting portion to detect an additional copy information field.]

To accomplish the objects of the present invention, there is provided a copy protection method comprising receiving encrypted digital data to be recorded, key information which is required to decrypt the encrypted digital data, and first copy control information which indicates a copy permission status of the encrypted digital data; and recording the encrypted digital data, the key information, and second copy control information on a digital recording medium, based on at least a status of the first copy control information.

According to another object there is provided a copy protection method comprising (a) providing digital content, key information for controlling at least decryption of the digital content, and copy control information for controlling copying of the digital content; and (b) recording the key information, the copy control information and the digital content on a digital recording medium.

According to another object there is provided a copy protection method comprising receiving encrypted digital content, first key information for decrypting the encrypted digital content, and copy control information which indicates whether or not a copy of the encrypted digital content is permitted; and controlling a recording or a reproducing of the encrypted digital content on or from a recording medium based on the first key information and/or the copy control information.

According to another object there is provided a copy protection apparatus comprising a receiving unit configured to receive encrypted digital data to be recorded, key information which is required to decrypt the encrypted digital data, and first copy control information which indicates a copy permission status of the encrypted digital data; and a recording unit configured to record the encrypted digital data, the key information, and second copy control information on a digital recording medium, based on at least a status of the first copy control information.

According to another object there is provided a copy protection apparatus comprising a providing unit configured to provide digital content, key information for controlling at least decryption of the digital content, and copy control information for controlling copying of the digital content; and a recording unit configured to record the key information, the copy control information and the digital content on a digital recording medium.

According to another object there is provided a copy protection apparatus comprising a receiving unit configured to receive encrypted digital content, first key information for decrypting the encrypted digital content, and copy control information which indicates whether or not a copy of the encrypted digital content is permitted; and a controlling unit configured to control a recording or a reproducing of the encrypted digital content on or from a recording medium based on the first key information and/or the copy control information.

BRIEF DESCRIPTION OF THE ATTACHED DRAWINGS

FIG. **1** is a block diagram of a conventional packet processing apparatus;

FIG. **2** shows an example of a general transmission stream;

FIG. **3** is a block diagram of a conventional public-key encryption system;

FIG. **4** shows connections of systems of the present invention;

FIG. **5** is a block diagram of a copy prevention apparatus for a digital video system of the present invention;

FIG. **6** is a block diagram of the copy prevention information detector of FIG. **5**;

FIG. **7** is a circuit diagram of the PES header detector of FIG. **6**;

FIGS. **8**A–**8**F are waveform diagrams of input/output at the [respect] *respective* portions of FIG. **7**;

FIG. **9** is a circuit diagram of the copy prevention information extractor of FIG. **4**;

FIGS. **10**A–**10**G are waveform diagrams of input/output at the respective portions of FIG. **9**; and

FIGS. **11**A–**11**D show examples of a bit stream of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Hereinafter, a preferred embodiment of the present invention will be described below with reference to the attached drawings.

Referring to FIG. **5**, a copy prevention apparatus of the present invention comprises a reproducing portion **1** for reproducing data recorded on tape, a key inserting portion **2** for adding a tape header start code and key field at the front end of a bit stream of reproducing portion **1**, a decrypting portion **3** for decrypting the output of key inserting portion **2** and transmitting it as parallel data, a key detecting/correcting portion **4** for detecting a key field from the paral-

lel data transmitted from decrypting portion **3**, a copy prevention information detecting portion **5** for detecting a PES header from the key field detected and extracting copy prevention information, a copy prevention information correcting portion **6** for correcting the output of copy prevention information detecting portion **5** if necessary, an encrypting portion **7** for encrypting the output of copy prevention information correcting portion **6**, and a recording portion **8** for recording the output of encrypting portion **7** on tape.

As shown in FIG. **6**, copy prevention information detecting portion **[6]** *5* comprises a PES header detecting portion **10** for searching the parallel data in synchronization with a clock clk to detect the PES header, and a copy prevention information extractor **20** enabled by the PES header signal of PES header detecting portion **10** to detect the copy prevention information field.

Referring to FIG. **7**, PES header detecting portion **10** comprises first and second flipflops **11** and **12** for sequentially delaying the parallel data according to clock **[**elk**]** *clk*, a packet start code detector **13** for searching the parallel data and the output of first and second flipflops **11** and **12** to detect the packet start code of the PES header, a stream ID detector **14** for searching the output of second flipflop **12** to detect the stream ID of the PES header, a delay **15** for sequentially delaying the output is-pscp of packet start code detector **13** according to clock clk, and a detection signal generator **16** for logically multiplying the outputs of delay **15** and stream ID detector **14** and outputting a PES header detection signal is-PES-header.

As shown in FIG. **9**, a copy prevention information extractor **20** comprises a D-flipflop **21** for holding the parallel data output from PES header detector **10**, a D-flipflop **22** for holding PES header detection signal is-PES-header of PES header detector **10**, a D-flipflop **23** cleared by the output of D-flipflop **22** and holding voltage (+5V) by a CR signal of the output of D-flipflop **21** and outputting a signal LCR, a D-flipflop **24** cleared by the output of D-flipflop **22** and holding voltage (+5V) by an OC signal of the output of D-flipflop **21** and outputting a signal **[**LOR**]** *LOC*, a copy prevention information position operator **25** for searching the parallel data of PES header detector **10** and calculating the position of an additional copy information field, a counter **26** for counting the output of copy information position operator **25**, and a D-flipflop **27** for holding the additional copy information field of the output of D-flipflop **21**.

The operation and effect of the present invention will be explained below. Generally, in case of reproducing or copy recording data on **[**tapa**]** *tape*, connections between systems are made as shown in FIG. **4**.

With those connections, an MPEG bit stream reproduced from VCR A is input to a satellite receiver or high-definition TV so that it cannot be recognized whether the stream is displayed on a screen or input to VCR B and recorded on another video tape.

For this reason, according to the present invention, in case that the bit stream reproduced from VCR A is copied from VCR B, information on copy prevention is transmitted to VCR B from VCR A. VCR B analyzes this information which is recorded with the bit stream.

Here, the insertion position of the copy prevention information contained in a GA bit stream is very limited because it must not affect decoding of the decoder of the satellite receiver or high-definition TV so that an image is displayed normally on a monitor. The copy prevention information may be inserted into the front end of the MPEG bit stream or inside the PES header.

When the MPEG bit stream is decoded in units **[**or**]** *of* group of picture (GOP), the respective GOPs are classified by their **[**cop**]** *GOP* start codes. This is useful in transmitting initialization data to a recording-side VCR because decoding is never affected even when a slight amount of data is added to the front end of the MPEG bit stream.

The case of inserting the copy prevention information into the PES header is useful in repeated transmission of information because copy prevention of a recording medium such as DSM is decided using CR and OC flaps of the PES header and additional copy information field. In this case, there are a variety of copy preventing methods.

First, when a mode of "No Copy" is detected from the additional copy information field of the PES header, VCR B is not able to enter its recording mode.

Second, when a mode of "Copy Permitted" is detected in order to implement a copy prevention such as DAT mode, VCR B records but "No Copy" mode is recorded in the additional copy information field to interrupt recopying from a copying tape. This means that a secondary source *tape can be made*, but a third source tape cannot.

Third, for "Back-up Copy", tape B copied from VCR B is reproducible normally only in VCR A. According to this method, reproducing-side VCR A encrypts the bit stream with its own inherent key and records it on tape so that only reproducing-side VCR A decrypts the MPEG bit stream recording on the tape. For every VCR set, a unique key is provided, encrypted by VCR's key and recorded on tape B. However, the VCR set for recording tape B is VCR B and tape B is encrypted by VCR A's key so that VCR A's key needs to be transmitted to VCR B with GA bit stream.

Accordingly, when the key information of VCR A is transmitted as a header in advance prior to the bit stream in the "Back-up Copy", it is recorded at the front end of tape B, which satisfies the insertion position of the copy prevention information mentioned before.

Here, as shown in FIG. **2**, the position of the additional copy information field is varied within the PES header according to whether presentation time stamp (PTS)/Decoding time stamp (DTS) and DSM trick mode field are present or not. This varied position must be compensated. Here, information transmitted through the additional copy information is a copy prevention method to be performed by recording-side VCR B.

In case of recording the bit stream shown in FIG. **11**A in the method of "Back-up Copy", the format of the bit stream recorded on tape is determined as shown in FIG. **11**B.

Here, a header area added to the front of the MPEG bit stream is formed with a tape header start code, that is, the header identifier code, and a key field for storing key information. In case of encrypting the MPEG bit stream in units of GOP, encryption blocks are classified by the packet start code prefix and stream ID of the PES header. The encryption block is a basic unit of encryption and can change whether encryption is performed in units of the encryption block, and encryption algorithm and key selection. Here, the encryption blocks must not be encrypted until the additional copy information field of the PES header. Encryption is performed until the end of the encryption block after the additional copy information field. The first 'transmission header' is not encrypted.

The operation of performing the "back-up Copy" mode by adding the header will be described below.

First, in copying, when recording data of tape A is encrypted, reproducing-side VCR A decrypts it using the key

information of the key field so as to make message m. Its key information is added to the header and transmitted in the format of FIG. **11**C.

Recording-side VCR B records the key information transmitted from reproducing-side VCR A on the header of copying tape B and then records the encrypted bit stream. Here, when the key information is transmitted from reproducing side to recording side, for security, a public-key encryption may be employed to the system because the information may be exposed to a pirate.

Such public-key encryption system ensures the secret of data even though the public-key is exposed but cannot be processed in real-time due to a great amount of calculation. Therefore, this system is not improper when the MPEG bit stream is encrypted directly. The "Back-up Copy" can be implemented when the MPEG bit stream is encrypted using a block-cipher algorithm or stream-cipher algorithm such as DES and a key used is encrypted in the public-key encryption.

In this case, every VCR u incorporates encryption algorithm E^{PK}_{U} corresponding to the public-key and decryption algorithm D^{PK}_{U} corresponding to the secret key. Encryption algorithm E^{PK}_{U} takes a power key of VCR u, and decryption algorithm D^{PK}_{U} an internal key of VCR u.

Here, the internal key may be opened to the public. Reproducing-side VCR A transmits the internal key on the key field of the header because another VCR encrypts using the internal key. Recording-side VCR B randomly selects a key Y used in the block-cipher algorithm such as DES and encrypts it with the public-key encryption system using an external key E^{PK}_{A}. The result is recorded on the key field of copying tape B.

Sequentially, the data is divided into encryption blocks and encrypted and recorded in the block-cipher algorithm using key Y. In this method, the bit stream of FIG. **11**D is recorded on copying tape B.

When copying tape B is reproduced in reproducing-side VCR A, key Y can be restored by decryption $D^{PK}_{A}[E^{PK}_{A}(Y)]$ in which data is decrypted properly. In other VCRs, key Y cannot be found, which disables the decryption of the bit stream.

[As**]** *An* embodiment of the present invention, shown in FIG. **5**, for performing such *an* operation will be described below.

When playback starts for tape copying, reproducing portion **1** detects data recorded on tape as shown in FIG. **11**A, and amplifies it by a predetermined level. As shown in FIG. **11**B, key inserting portion **2** adds a header having a tape header start code and key field to the GA bit stream of reproducing portion **1** shown in FIG. **11**A. Copy prevention information is loaded on the additional copy information field of the PES header to form a format shown in FIG. **11**C. Here, decrypting portion **3** decrypts the bit stream formed in key inserting portion **2** and transmits it as parallel data to the recording-side VCR via an interface.

When the bit stream of FIG. **11**C is transmitted to the recording-side VCR via the interface, key detecting/correcting portion **4** detects the key field added to the bit stream and corrects the key field if necessary.

Copying prevention information detecting portion **5** searches the PES header area to detect the additional copy information field. Here, though a slight amount of information is recorded in the additional copy information field, redundancy is provided in several areas of the bit stream to increase reliability of information transmitted.

Copy prevention information detecting portion **5** extracts the value of AC flag from the PES header flag in order to calculate the position of the additional copy information field because it varies within the PES header. Here, when copy prevention information correcting portion **6** corrects the output of copy prevention information detecting portion **5**, encrypting portion **7** performs encryption using the block-cipher algorithm such as DES. Here, copy prevention information correcting portion **6** performs correction while the input data is stored in a RAM. Accordingly, encrypting portion **7** records the encrypted bit stream on tape in recording portion **8**. Because the key information of the reproducing-side VCR is added on the copying tape, only a VCR having this key information can reproduce tape normally.

As shown in FIG. **6**, in copy prevention information detecting portion **5**, PES header detecting portion **10** searches the output of key detecting/correcting portion **4** and outputs a header detection signal is-PES-header. After header detection signal is-PES-header is input, copy prevention information extractor **20** detects the additional copy information field and OC and CR flags.

PES header detector **10** for detecting the PES header is formed as shown in FIG. **7**. When bit stream data_in is input as shown in FIG. **8**A, first flipflop **11** synchronized to clock clk is delayed for a predetermined time to output the bit stream delayed as shown in FIG. **8**B. Second flipflop **12** delays the output of first flipflop **11** by are predetermined time and outputs the bit stream delayed as shown in FIG. **8**C.

Here, packet start code detecting portion **13** searches the bit stream shown in FIG. **8**A and the output of first and second flipflops **11** and **12** shown in FIGS. **8**B and **8**C in order to detect the packet start code of the PES header. When detection signal is-pscp is output as shown in FIG. **8**D, delay **15** in which flipflops are coupled at multi-stages delays it sequentially according to clock clk.

Meanwhile, stream ID code detector **14** searches the output of second flipflop **12** and detects the stream ID area of the PES header. Then, detection signal is-sid shown in FIG. **8**E is output to detection signal generator **16**. Detection signal generator **16** logically multiplies the output of delay **15** and stream ID code detector **14**, and the flipflops hold the output of the AND gate according to clock clk so that PES header detection signal is-PES-header is output to copy prevention information extractor **20**, as shown in FIG. **[8**P**]** *8F*.

Here, copy prevention information extractor **20** for detecting the copy prevention information is formed as shown in FIG. **9**. When the parallel data output from PES header detector **10** and shown in FIG. **10**A is held and output as shown in FIG. **10**B, D-flipflop **22** synchronized to PES header detection signal is-PES-header of PES header detector **10** shown in FIG. **8**F holds voltage +5V so that a HIGH signal is output to the clear ports of D-flipflops **23**, **24** and **27** to release the clear states.

D-flipflop **23** is synchronized to the CR flag or the output of D-flipflop **21** shown in FIG. **10**B to hold voltage Vcc so that a HIGH signal LCR is output as shown in FIG. **10**C. D-flipflop **24** is synchronized to the OC flag of the output of D-flipflop **21** to hold voltage Vcc so that a HIGH signal LOC is output as shown in FIG. **10**D.

Copy prevention position detector **25** searches the PD, TM and AC flags of the parallel data of PES header detector **10** shown in FIG. **10**A to calculate the position of the additional copy information field, which is output to counter **26** as shown in FIG. **10**E. Counter **26** receiving the 4-bit value performs counting so that a HIGH signal is output as shown in FIG. **10**F at a predetermined counting value.

D-flipflop **27** synchronized to HIGH output rco of counter **26** holds the additional copy information field from the parallel data of D-flipflop **21** shown in FIG. **10**B. The field is output as shown in FIG. **10**C.

As described above, in the copy prevention method and apparatus for a digital video system of the present invention, a key information is recorded with a bit stream so that a VCR having the key information reproduces tape normally, thereby preventing illegal copy of tape. In addition, for key information transmission, the public-key encryption is introduced to disable a pirate to release the copy prevention, increasing reliability of copy prevention.

What is claimed is:

[1. A copy prevention method for a digital video system comprising the steps of:

(a) receiving a digital data stream reproduced from a digital medium;

(b) detecting an encryption key, which is a portion of said received digital data stream;

(c) decrypting said encryption key using key information;

(d) decrypting said received digital data stream based on said decrypted encryption key; and

(e) transmitting said decrypted digital data stream to at least one of a monitor and a digital recorder.**]**

[2. A copy prevention method for a digital video system as claimed in claim **1**, wherein said key information is predetermined by said digital video system.**]**

[3. A copy prevention method for a digital video system as claimed in claim **1**, wherein said decrypting step (d) is operated in units of predetermined block of said received digital data stream.**]**

[4. A copy prevention apparatus for a digital video system comprising:

receiving means for receiving a digital data stream reproduced from a digital medium;

a key detector to detect an encryption key, which is a portion of said received digital data stream;

a decryption unit to decrypt said encryption key using key information and to decrypt said received digital data stream based on said decrypted encryption key; and

a controller to control transmission of said decrypted digital data stream to at least one of a monitor and a digital recorder.**]**

[5. A copy prevention apparatus for a digital video system as claimed in claim **4**, wherein said key information is predetermined by said digital video system.**]**

[6. A copy prevention apparatus for a digital video system as claimed in claim **4**, wherein said decryption unit is operated in units of predetermined block of said received digital data stream.**]**

[7. A copy prevention method for a digital video system comprising the steps of:

(a) receiving a digital data stream reproduced from a digital medium;

(b) detecting an encryption key, which is a portion of said received digital data stream;

(c) decrypting said encryption key using key information;

(d) decrypting said received digital data stream based on said decrypted encryption key.**]**

[8. A copy prevention method for a digital video system as claimed in claim **7**, wherein said key information is predetermined by said digital video system.**]**

[9. A copy prevention method for a digital video system as claimed in claim **7**, wherein said decrypting step (d) is operated in units of predetermined block of said received digital data stream.**]**

[10. A copy prevention apparatus for a digital video system comprising:

receiving means for receiving a digital data stream reproduced from a digital medium;

a key detector to detect an encryption key, which is a portion of said received digital data stream;

a decryption unit to decrypt said encryption key using key information and to decrypt said received digital data stream based on said decrypted encryption key.**]**

[11. A copy prevention apparatus for a digital video system as claimed in claim **10**, wherein said key information is predetermined by said digital video system.**]**

[12. A copy prevention apparatus for a digital video system as claimed in claim **10**, wherein said decryption unit is operated in units of predetermined block of said received digital data stream.**]**

[13. A copy prevention method for a digital video system comprising the steps of:

(a) receiving a digital data stream reproduced from a digital medium;

(b) detecting an encryption key, which is a portion of said received digital data stream;

(c) decrypting said encryption key using predetermined key information;

(d) decrypting said received digital data stream based on said decrypted encryption key.**]**

[14. A copy prevention method for a digital video system as claimed in claim **13**, wherein said decrypting step (d) is operated in units of predetermined block of said received digital data stream.**]**

[15. A copy prevention apparatus for a digital video system comprising:

receiving means for receiving a digital data stream reproduced from a digital medium;

a key detector to detect an encryption key, which is a portion of said received digital data stream;

a decryption unit to decrypt said encryption key using predetermined key information and to decrypt said received digital data stream based on said decrypted encryption key.**]**

[16. A copy prevention apparatus for a digital video system as claimed in claim **15**, wherein said decrypting unit is operated in units of predetermined block of said received digital data stream.**]**

[17. A copy prevention method for a digital data system, comprising the steps of:

(a) receiving first key information;

(b) encrypting second key information using said first key information;

(c) encrypting digital data streams using said second key information; and

(d) recording at least said encrypted second key information and said encrypted digital data streams on a digital medium.**]**

[18. The method of claim **17**, wherein said (b) randomly selects said second key information.**]**

[19. The method of claim **17**, wherein said step (c) encrypts said digital data streams in blocks.**]**

[20. A copy prevention apparatus for a digital data system, comprising the steps of:

an encryption unit receiving first key information, encrypting second key information using said first key information, and encrypting digital data streams using said second key information; and

a controller controlling recording of at least said encrypted second key information and said encrypted digital data streams on a digital medium.]

[21. The apparatus of claim 20, wherein said encryption unit randomly selects said second key information.]

[22. The apparatus of claim 20, wherein said encryption unit encrypts said digital data streams in blocks.]

[23. A recording medium having a data structure for controlling operation of copy prevention function in a digital data processing device, comprising:

a digital data area storing digital data encrypted using first key information; and

a key information area storing said first key information encrypted using second key information, said first key information operatively controlling the decryption of said encrypted digital data in a digital data process device.]

[24. A copy prevention method for a digital data system, comprising:

receiving first key information, said first key information for encrypting digital data;

encrypting said first key information using second information; and

transferring said encrypted first key information.]

[25. The method of claim 24, wherein said encrypting step public key encrypts said second key information.]

[26. The method of claim 24, wherein said transferring step records said encrypted first key information on a digital medium.]

[27. The method of claim 24, wherein said transferring step transmits said encrypted first key information.]

[28. A copy prevention apparatus for a digital data system, comprising:

an encryption unit receiving first key information, said first key information for encrypting digital data, and encrypting said first key information using second key information; and

a controller controlling a transfer of said encrypted first key information.]

[29. The apparatus of claim 28, wherein said encryption unit public key encrypts said first key information.]

[30. The apparatus of claim 28, wherein said controller controls recording said encrypted first key information on a digital medium.]

[31. The apparatus of claim 28, wherein said controller controls transmitting said encrypted first key information.]

32. A copy protection method, comprising:

receiving encrypted digital data to be recorded, key information which is required to decrypt the encrypted digital data, and first copy control information which indicates a copy permission status of the encrypted digital data; and

recording the encrypted digital data, the key information, and second copy control information on a digital recording medium, based on at least a status of the first copy control information,

wherein the encrypted digital data is partitioned into a GOP (Group Of Picture) unit, and

wherein the recording step includes recording the encrypted digital data partitioned into the GOP unit and recording the second copy control information followed by the GOP unit.

33. The method of claim 32, wherein said recording step records the encrypted digital data only when the first copy control information indicates that a copy is permitted.

34. The method of claim 33, wherein said recording step includes encrypting the key information and recording the encrypted key information in a control area followed by the encrypted digital data.

35. The method of claim 33, wherein the second copy control information indicates that the copy has been generated.

36. The method of claim 35, further comprising:

recording an identifier to identify that the second copy control information is included.

37. The method of claim 33, further comprising:

recording classification information to classify the encrypted digital data.

38. The method of claim 37, wherein the classification information is recorded in a header portion of the encrypted digital data.

39. The method of claim 32, wherein the key information is followed by the GOP unit.

40. A copy protection method, comprising:

receiving encrypted digital data to be recorded, key information which is required to decrypt the encrypted digital data, and first copy control information which indicates a copy permission status of the encrypted digital data; and

recording the encrypted digital data, the key information, and second copy control information on a digital recording medium, based on at least a status of the first copy control information,

wherein the received encrypted digital data is recorded as a GOP (Group Of Picture) unit, which is partitioned into a plurality of packets, each packet comprising a header portion and a data portion, and

wherein the second copy information is included in the header portion of at least one packet.

41. The method of claim 40, wherein an identifier is recorded in the header portion.

42. The method of claim 41, wherein the key information is recorded in a control data area followed by the GOP unit.

43. The method of claim 42, wherein classification information is recorded in the header portion of the packet, the classification information for classifying that the data portion of the packet is encrypted.

44. A copy protection method, comprising:

receiving encrypted digital data to be recorded, key information which is required to decrypt the encrypted digital data, and first copy control information which indicates a copy permission status of the encrypted digital data;

recording the encrypted digital data, the key information, and second copy control information on a digital recording medium, based on at least a status of the first copy control information, the encrypted digital content being partitioned into one or more first data units, the first data unit including a header portion and a data portion, and wherein said step of recording the encrypted digital data includes recording the one or more first data units; and

recording the second copy control information in the header portion followed by the data portion.

45. A copy protection method, comprising:

providing digital content, key information for controlling at least a decryption of the digital content, and copy control information for controlling copying of the digital content, the digital content being partitioned into a GOP (Group Of Picture) unit; and

recording the key information, the copy control information and the digital content partitioned into the GOP unit on a digital recording medium,

wherein the copy control information is followed by the GOP unit.

46. The method of claim 45, wherein the key information in said providing step is encrypted key information.

47. The method of claim 46, wherein the encrypted key information is recorded in a control area followed by the digital content.

48. The method of claim 47, wherein the copy control information is recorded in the control area followed by the digital content.

49. The method of claim 46, wherein said recording step records the digital content as encrypted by the key information.

50. The method of claim 45, wherein said recording step includes recording a flag to indicate that the copy control information is included thereby identifying an existence of the copy control information.

51. The method of claim 50, wherein the flag and the copy control information are recorded in a control area followed by the digital content.

52. The method of claim 45, wherein said recording step further records a flag to indicate that the copy control information is included, in the area followed by the GOP unit.

53. A copy protection method, comprising:

providing digital content, key information for controlling at least decryption of the digital content, and copy control information for controlling copying of the digital content; and

recording the key information, the copy control information and the digital content on a digital recording medium, the digital content being partitioned into one or more first data units, the first data unit being partitioned into one or more second data units, the second data unit including a header portion and a data portion, and

the copy control information being included in the header portion followed by the data portion of at least one second data unit.

54. The method of claim 53, wherein said recording step further records a flag to indicate that the copy control information is included.

55. The method of claim 53, wherein the key information is recorded in a control data area followed by a first of the first data units.

56. A recording medium, comprising:

a plurality of first data units, which are partitioned into a plurality of second data units, which include a header portion and a data portion respectively, an encrypted digital content being included in the data portions of the second data units;

copy control information indicating whether or not a copy of the encrypted digital content is permitted;

an identifier which identifies whether or not the copy control information exists; and

encrypted key information, which is required to decrypt the encrypted digital content,

wherein the copy control information and the identifier are included in the header portion of the second data unit.

57. The recording medium of claim 56, wherein the copy control information and identifier are included in a control data area followed by a first of the first data units.

58. The recording medium of claim 56, wherein the copy control information can have a status to indicate that no more copies are permitted.

59. The recording medium of claim 57, wherein the encrypted key information is recorded in the control data area.

60. The recording medium of claim 59, wherein one of the plurality of first data units comprises at least one GOP (Group Of Picture) unit.

61. The recording medium of claim 56, wherein classification information is included in the header portion to indicate if the data portion is encrypted.

62. The recording medium of claim 56, wherein the encrypted digital content is decrypted only when the encrypted key information is normally decrypted.

63. A copy protection method, comprising:

retrieving encrypted digital content, first key information for decrypting the encrypted digital content, and copy control information which indicates whether or not a copy of the encrypted digital content is permitted; and

controlling a reproducing of the encrypted digital content from a recording medium based on the first key information and/or the copy control information, the digital content being partitioned into one or more first data units, the first data unit including a header portion and a data portion, the encrypted digital content being included in the data portion and the copy control information being included in the header portion followed by the data portion.

64. The method of claim 63, wherein said controlling step includes decrypting the encrypted digital content based on the first key information.

65. The method of claim 64, further comprising:

decrypting the first key information based on second key information, and then decrypting the encrypted digital content based on the decrypted first key information.

66. A copy protection apparatus, comprising:

a receiving unit configured to receive encrypted digital data to be recorded, key information which is required to decrypt the encrypted digital data, and first copy control information which indicates a copy permission status of the encrypted digital data;

a recording unit configured to record the encrypted digital data, the key information, and second copy control information on a digital recording medium; and

a controller operably coupled to the recording unit, to determine at least a status of the first copy control information, and to allow the recording unit to record the encrypted digital data based on the determined result,

wherein the encrypted digital data is partitioned into a GOP (Group Of Picture) unit, and

wherein the controller is further configured to control the recording unit to record the encrypted digital data in the GOP unit, and record the second copy control information in an area followed by the GOP unit.

67. The apparatus of claim 66, wherein said controller is configured to control the recording unit to record the encrypted digital data only when the first copy control information indicates that a copy is permitted as a result of the determination.

68. The apparatus of claim 67, further comprising:

an encrypting unit configured to encrypt the key information,

wherein the recording unit is further configured to record the encrypted key information in a control portion followed by the encrypted digital data, according to a control of the controller.

69. The apparatus of claim 67, wherein the second copy control information indicates that the copy has been generated.

70. The apparatus of claim 69, wherein the recording unit is further configured to record an identifier to identify that the second copy control information is included, according to a control of the controller.

71. The apparatus of claim 67, wherein the recording unit is further configured to record classification information to classify the encrypted digital data, according to a control of the controller.

72. The apparatus of claim 71, wherein the recording unit is further configured to record the classification information in a header portion of the encrypted digital data, under control of the controller.

73. The apparatus of claim 66, wherein the recording unit is further configured to record key information in the portion followed by the GOP unit, under control of the controller.

74. A copy protection apparatus, comprising:

a receiving unit configured to receive encrypted digital data to be recorded, key information which is required to decrypt the encrypted digital data, and first copy control information which indicates a copy permission status of the encrypted digital data;

a recording unit configured to record the encrypted digital data, the key information, and second copy control information on a digital recording medium; and

a controller operably coupled to the recording unit, to determine at least a status of the first copy control information, and to allow the recording unit to record the encrypted digital data based on the determined result, the received encrypted digital data being partitioned into a GOP (Group Of Picture) unit, which is partitioned into a plurality of packets, each packet comprising a header portion and a data portion,

wherein the recording unit is further configured to record the GOP unit, and record the second copy control information in the header portion of at least one packet under control of the controller.

75. The apparatus of claim 74, wherein the recording unit is further configured to record an identifier in the header portion, under control of the controller.

76. The apparatus of claim 75, wherein the recording unit is further configured to record the key information in a control data portion followed by the GOP unit, under control of the controller.

77. The apparatus of claim 76, wherein the recording unit is further configured to record classification information in the header portion of the packet under control of the controller, the classification information for classifying that the data portion of the packet is encrypted.

78. A copy protection apparatus, comprising:

a receiving unit configured to receive encrypted digital data to be recorded, key information which is required to decrypt the encrypted digital data, and first copy control information which indicates a copy permission status of the encrypted digital data;

a recording unit configured to record the encrypted digital data, the key information, and second copy control information on a digital recording medium; and

a controller operably coupled to the recording unit, to determine at least a status of the first copy control information, and to allow the recording unit to record the encrypted digital data based on the determined result, the received encrypted digital data being partitioned into a plurality of first data units, each of which includes a header portion and a data portion respectively,

wherein the recording unit is further configured to record the plurality of units, and to record the second copy control information in the header portion followed by the data portion in at least one first data unit, under control of the controller.

79. A copy protection apparatus, comprising:

a providing unit configured to provide digital content, key information for controlling at least decryption of the digital content, and copy control information for controlling copying of the digital content;

a partitioning unit configured to partition the provided digital content into a plurality of first data units;

a recording unit configured to record the key information, the copy control information and the partitioned digital content on a digital recording medium; and

a controller, operably coupled to the recording unit, to control the recording operation,

wherein the digital content is partitioned into a GOP (Group Of Picture) unit, and

wherein the recording unit is further configured to record the digital content in the GOP unit, and record the copy control information in an area followed by the GOP unit, under control of the controller.

80. The apparatus of claim 79, wherein the key information provided by the providing unit is encrypted key information.

81. The apparatus of claim 80, wherein the recording unit is further configured to record the encrypted key information in a control portion followed by the digital content or in a portion of at least one of first data unit, under control of the controller.

82. The apparatus of claim 81, wherein the recording unit is further configured to record the copy control information in the control portion followed by the digital content or in a portion of at least one of first data unit, under control of the controller.

83. The apparatus of claim 80, further comprising:

an encryption circuit configured to encrypt the digital content in a predetermined encryption algorithm, the digital content being encrypted by the key information,

wherein the recording unit is further configured to record the digital content as encrypted by the encryption circuit, under control of the controller.

84. The apparatus of claim 79, wherein the recording unit is further configured to record an identifier to indicate that the copy control information is included under control of the controller, thereby identifying an existence of the copy control information.

85. The apparatus of claim 84, wherein the recording unit is further configured to record the identifier and the copy control information in a control portion followed by the digital content or in a portion of at least one [[of]] *first data unit, under control of the controller.*

86. The apparatus of claim 79, wherein the recording unit is further configured to record an identifier to indicate that the copy control information is included in the portion followed by the GOP unit or the portion of at least one GOP unit, under control of the controller.

87. A copy protection apparatus, comprising:

a providing unit configured to provide digital content, key information for controlling at least decryption of the digital content, and copy control information for controlling copying of the digital content;

a partitioning unit configured to partition the provided digital content into a plurality of first data units;

a recording unit configured to record the key information, the copy control information and the partitioned digital content on a digital recording medium; and

a controller operably coupled to the recording unit, to control the recording operation, the digital content being partitioned into one or more first data units, the first data unit being partitioned into one or more second data units, the second data unit including a header portion and a data portion,

wherein the recording unit is further configured to record the copy control information in the header portion followed by the data portion in at least one second data unit, under control of the controller.

88. The apparatus of claim 87, wherein the recording unit is further configured to record an identifier to indicate that the copy control information is included, under control of the controller.

89. The apparatus of claim 87, wherein the recording unit is further configured to record the key information in a control data portion followed by a first of the first data units, under control of the controller.

90. A copy protection apparatus, comprising:

a retrieving circuit configured to retrieve a digital data, the digital data including encrypted digital content, first key information for decrypting the encrypted digital content, and copy control information which indicates whether or not a copy of the encrypted digital content is permitted; and

a control circuit configured to control a reproducing of the encrypted digital content from a recording medium based on the first key information and/or the copy control information, the digital data being partitioned into one or more first data units, the first data unit including a header portion and a data portion, the encrypted digital content being included in the data portion and the copy control information being included in the header portion followed by the data portion.

91. The apparatus of claim 90, further comprising:

a decrypting circuit configured to decrypt the data portion including the encrypted digital content based on the first key information.

92. The apparatus of claim 91, wherein the decrypting circuit is configured to decrypt the first key information based on second key information, and then decrypt the encrypted digital content based on the decrypted first key information.

93. The method of claim 44, wherein said step of recording the encrypted digital data records the encrypted digital data only when the first copy control information indicates that a copy is permitted.

94. The method of claim 93, wherein said step of recording the encrypted digital data includes encrypting the key information and recording the encrypted key information in a control area followed by the encrypted digital data.

95. The method of claim 93, wherein the second copy control information indicates that the copy has been generated.

96. The method of claim 95, further comprising:

recording an identifier to identify that the second copy control information is included.

97. The method of claim 93, further comprising:

recording classification information to classify the encrypted digital data.

98. The method of claim 97, wherein the classification information is recorded in a header portion of the encrypted digital data.

99. The apparatus of claim 78, wherein said recording unit is further configured to record the encrypted digital data only when the first copy control information indicates that a copy is permitted.

100. The apparatus of claim 99, wherein said recording unit includes an encrypting unit configured to encrypt the key information and said recording unit is further configured to record the encrypted key information in a control area followed by the encrypted digital data, under control of the controller.

101. The apparatus of claim 99, wherein the second copy control information indicates that the copy has been generated, and

wherein the recording unit is further configured to record an identifier to identify that the second copy control information is included, under control of the controller.

102. The apparatus of claim 99, wherein the recording unit is further configured to record classification information to classify the encrypted digital data, under control of the controller.

* * * * *