

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
20 April 2006 (20.04.2006)

PCT

(10) International Publication Number
WO 2006/040708 A2

(51) International Patent Classification:
H04N 7/167 (2006.01)

(21) International Application Number:
PCT/IB2005/053237

(22) International Filing Date: 3 October 2005 (03.10.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
04105040.2 14 October 2004 (14.10.2004) EP

(71) Applicant (for all designated States except US): **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL];
Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **BRONDIJK, Robert, A.** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agents: **UITTENBOGAARD, Frank** et al.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

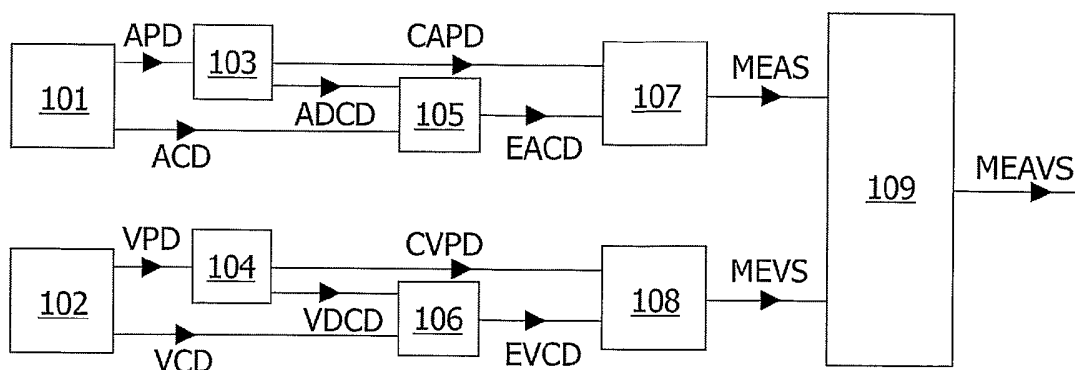
— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

Published:

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND DEVICE FOR ENCRYPTING A DATA STREAM



(57) Abstract: A method is described for transferring an encrypted data stream which comprises compressed payload data and control data, the control data comprising decompression control data necessary for decompression of the payload data, wherein the payload data is transferred as non-encrypted data, the decompression control data is transferred as encrypted data, the data stream may be an audio/video stream, for example an MPEG-stream.

WO 2006/040708 A2

Method and device for encrypting a data stream

FIELD OF THE INVENTION

The present invention relates in general to the field of encryption of a data stream. By way of example, the present invention will be explained for the context of an MPEG data stream, but it is to be noted that this example is not intended to restrict the scope of the invention as the invention is applicable to many types of data stream.

BACKGROUND OF THE INVENTION

As is generally known, an MPEG data stream contains different types of data in a multiplexed way. A distinction can be made between "actual" data of interest, also indicated as payload data, and control data. The data are organized in data blocks having a body and a header, the payload data being contained in the body and the control data in the header. The payload data are also jointly denoted the transport stream; the control data together are also denoted the program stream. It is further possible to distinguish between audio data and video data.

The control data relate, for example, to the timing of the data. Furthermore, the data stream is typically compressed, and the control data contain data necessary for decompression. The control data necessary for decompression is denoted "essential" control data; the remaining control data is denoted "non-essential" control data. Thus, the entire data stream contains:

- video payload data;
- essential video control data;
- non-essential video control data;
- audio payload data;
- essential audio control data;
- non-essential audio control data.

In some cases, it is required to protect the data stream against unauthorized access. In cases of pay-per-view, for example, a user must acquire the right to access material. The data stream is typically encrypted in such a case, and the data stream needs to be decrypted before access is possible. An apparatus receiving the data stream, such as a

television apparatus or a PC running a television application, typically comprises separate audio and video decoders (hardware), so the multiplexed data stream must be de-multiplexed to obtain the elementary audio and video data streams which can be provided to the separate audio and video decoders. Before de-multiplexing is possible, the data stream needs to be
5 decrypted.

A first problem in this respect relates to the fact that this decryption process requires many computations. Especially in the case where it is desired to run an audio/video application (television application) on a PC, the processor needs to be very powerful and hence expensive if it is to be able to perform the decryption process.

10 A second problem in this respect relates to the fact that the PC needs to be aware of the decryption keys in order to perform decryption,. Transferring the decryption keys to the PC over public buses involves the risk that the decryption keys are intercepted.

A further problem in this respect relates to the fact that encryption tends to increase the number of bits to be transferred.

15 It is a general objective of the present invention to overcome the above-mentioned problems.

SUMMARY OF THE INVENTION

The present invention is based on the understanding that a powerful encryption
20 does not necessarily require that the entire data stream is encrypted. According to the present invention, only the control data is encrypted, while the payload data is left non-encrypted. As a consequence, the receiving apparatus only needs to decrypt the control data. Since the amount of control data is much less than the amount of payload data, the calculation burden for the processor is substantially reduced.

25 In a preferred embodiment, only the essential control data is encrypted. This further reduces the calculation burden for the processor. Nevertheless, the encryption is still effective in that decompression is only possible after decryption. Without decryption no decompression is possible, and without decompression no rendering is possible.

30 BRIEF DESCRIPTION OF THE DRAWINGS

These and other aspects, features and advantages of the present invention will be further explained by the following description with reference to the drawings, in which same reference numerals indicate same or similar parts, and in which:

figure 1A is a block diagram schematically illustrating a prior art process for generating and transmitting an audio/video data stream;

figure 1B is a block diagram schematically illustrating a prior art process for receiving and decoding an encrypted audio/video stream;

5 figure 2 is a block diagram schematically illustrating a process for generating an audio/video data stream in accordance with the present invention;

figure 3 is a block diagram schematically illustrating a process for receiving a multiplexed encrypted audio/video stream in accordance with the present invention.

10 DETAILED DESCRIPTION OF THE INVENTION

Figure 1A is a block diagram schematically illustrating a prior art process for generating an audio/video data stream. Audio payload data APD and audio control data ACD are generated by an audio data source 1. Video payload data VPD and video control data VCD are generated by a video data source 2. An audio compression circuit 3 receives the audio payload data APD and performs a compression so as to provide compressed audio payload data CAD. An audio multiplexing circuit 5 receives the compressed audio payload data CAPD and audio control data ACD and performs a multiplexing operation so as to provide a multiplexed audio stream MAS. A video compression circuit 4 receives the video payload data VPD and performs a compression so as to provide compressed video payload data CVPD. A video multiplexing circuit 6 receives the compressed video payload data CVPD and video control data VCD and performs a multiplexing operation so as to provide a multiplexed video stream MVS. An overall multiplexing circuit 7 receives the multiplexed audio stream MAS and the multiplexed video stream MVS and performs a multiplexing operation so as to provide a multiplexed audio/video stream MAVS. An encryption circuit 8 receives the multiplexed audio/video stream MAVS and performs an encryption operation so as to provide an encrypted audio/video stream EAVS.

Figure 1B is a block diagram schematically illustrating a prior art process for receiving this encrypted audio/video stream EAVS and deriving the original audio and video data therefrom. A decryption circuit 11 receives the encrypted audio/video stream EAVS and performs a decryption operation so as to provide the decrypted yet multiplexed audio/video stream MAVS. A demultiplexing circuit 12 receives the multiplexed audio/video stream MAVS and performs a demultiplexing operation so as to separately provide the multiplexed audio stream MAS and the multiplexed video stream MVS. An audio processing circuit 13 receives the multiplexed audio stream MAS, separates the compressed audio payload data

CAPD from the audio control data ACD, and performs a decompression process on the compressed audio payload data CAPD, based on the audio control data ACD, in order to provide the original audio payload data APD for further processing. A video processing circuit 14 receives the multiplexed video stream MVS, separates the compressed video payload data CVPD from the video control data VCD, and performs a decompression process on the compressed video payload data CVPD, based on the video control data VCD, in order to provide the original video payload data VPD for further processing.

It is noted that the decryption circuit 11 and the demultiplexing circuit 12, or the software implementing these functions, are part of the central processing unit 17 of a PC, whereas the audio processing circuit 13 is part of an audio card 15, and the video processing circuit 14 is part of a video card 16. The compressed audio data CAD from the CPU 17 are transferred to the audio card 15 and the compressed video data CVD from the CPU 17 to the video card 16, including the control data necessary for decompression, over a public data bus 20.

Figure 2 is a block diagram schematically illustrating a process in accordance with the present invention for generating an audio/video data stream. Audio payload data APD and audio control data ACD (relating, for example, to timing, audio bit rate, etc) are generated by an audio data source 101. An audio compression circuit 103 receives the audio payload data APD and performs a compression operation so as to provide compressed audio payload data CAPD. The audio compression circuit 103 also provides audio decompression control data ADCD, i.e. control data essential for being able to decompress the compressed audio payload data CAPD. An audio encryption circuit 105 receives the audio decompression control data ADCD and audio control data ACD and performs an encryption operation in order to provide encrypted audio control data EACD. An audio multiplexing circuit 107 receives the compressed audio payload data CAPD and the encrypted audio control data EACD and performs a multiplexing operation so as to provide a multiplexed encrypted audio stream MEAS.

Video payload data VPD and video control data VCD (relating, for example, to timing, video bit rate, frame rate, picture size, etc) are generated by a video data source 102. A video compression circuit 104 receives the video payload data VPD and performs a compression operation in order to provide compressed video payload data CVPD. The video compression circuit 104 also provides video decompression control data VDCD, i.e. control data essential for being able to decompress the compressed video payload data CVPD. A video encryption circuit 106 receives the video decompression control data VDCD and video

control data VCD and performs an encryption operation so as to provide encrypted video control data EVCD. A video multiplexing circuit 108 receives the compressed video payload data CVPD and the encrypted video control data EVCD and performs a multiplexing operation in order to provide a multiplexed encrypted video stream MEVS.

5 An overall multiplexing circuit 109 receives the multiplexed encrypted audio stream MEAS and the multiplexed encrypted video stream MEVS and performs a multiplexing operation in order to provide a multiplexed encrypted audio/video stream MEAVS.

10 The audio encryption circuit 105 may be designed to encrypt all control data, i.e. the audio decompression control data ADCD as well as the audio control data ACD. It is sufficient, however, if the audio encryption circuit 105 encrypts only part of the control data. In a preferred embodiment, the audio encryption circuit 105 is designed to encrypt only the audio decompression control data ADCD and to leave the audio control data ACD un-encrypted. In this preferred embodiment, the audio control data ACD may by-pass the audio encryption circuit 105. The same applies, mutatis mutandis, to the video encryption circuit 106.

 Figure 3 is a block diagram schematically illustrating a process in accordance with the present invention for receiving the multiplexed encrypted audio/video stream MEAVS and deriving the original audio and video data therefrom. A demultiplexing circuit 111 receives the multiplexed encrypted audio/video stream MEAVS and performs a demultiplexing operation in order to provide the compressed audio payload data CAPD, the encrypted audio control data EACD, the compressed video payload data CVPD, and the encrypted video control data EVCD separately of one another.

25 A first decryption circuit 113 receives the encrypted audio control data EADCD and performs a decryption operation in order to provide the audio control data ACD and the audio decompression control data ADCD. An audio processing circuit 115 receives the compressed audio payload data CAPD and performs a decompression process, based on the audio decompression control data ADCD, in order to provide the original audio payload data APD and the original audio control data ACD for further processing.

30 A second decryption circuit 114 receives the encrypted video control data EVDCD and performs a decryption operation so as to provide the video control data VCD and the video decompression control data VDCD. A video processing circuit 116 receives the compressed video payload data CVPD and performs a decompression process, based on the

video decompression control data VDCD, so as to provide the original video payload data VPD and the original video control data VCD for further processing.

It is noted that the demultiplexing circuit 111 may be part of the central processing unit 117 of a PC, whereas the first decryption circuit 113 and the audio processing circuit 115, or the software implementing these functions, are part of an audio card 118, and the second decryption circuit 114 and the video processing circuit 116, or the software implementing these functions, are part of a video card 119. The transfer of the compressed audio payload data CAPD from the CPU 117 to the audio card 118 and of the compressed video payload data CVPD from the CPU 117 to the video card 119 takes place over a public data bus 120. The transfer of the control data necessary for decompression also takes place over this public data bus 120. However, this control data is still encrypted, so it is not possible to decompress the audio and video information on the basis of the information intercepted from the public bus.

The CPU 117 only needs to demultiplex the multiplexed data stream; and the demultiplexed data streams can be sent to the audio decoder and the video decoder, respectively, which are specialized pieces of hardware containing the decryption keys.

It should be clear to those skilled in the art that the present invention is not limited to the exemplary embodiments discussed above, but that several variations and modifications are possible within the protective scope of the invention as defined in the appending claims.

For instance, the advantages offered by the present invention are also obtained if part of the non-essential control data is encrypted. Compared with the prior art, furthermore, an improvement is already achieved if less than 100% of the payload data is encrypted.

Furthermore, it is assumed in the above description that the control data are not compressed. However, the present invention is also applicable in cases where the control data is compressed.

It is furthermore possible that the audio multiplexing circuit 107, the video multiplexing circuit 108, and the overall multiplexing circuit 109 are implemented as one combined circuit.

Furthermore, although the data stream to be transferred may comprise audio and/or video data, this is not essential. The present invention offers advantages in all cases where a data stream comprises compressed payload data and control data including control data necessary for decompression.

The present invention was explained above with reference to block diagrams, which illustrate functional blocks of the device according to the present invention. It is to be understood that one or more of these functional blocks may be implemented in hardware, where the function of such a functional block is performed by individual hardware components, but it is equally possible that one or more of these functional blocks are
5 implemented in software, so that the function of such a functional block is performed by one or more program lines of a computer program or a programmable device such as a microprocessor, microcontroller, digital signal processor, etc.

CLAIMS:

1. A method of transferring an encrypted data stream which comprises compressed payload data and control data, the control data comprising decompression control data necessary for decompression of the payload data;
wherein at least part of the payload data is transferred as non-encrypted data,
5 and wherein at least part of the control data is transferred as encrypted data.
2. Method according to claim 1, wherein 100% of the payload data is transferred as non-encrypted data.
- 10 3. Method according to claim 1, wherein 100% of the control data is transferred as encrypted data.
4. Method according to claim 1, wherein only the decompression control data is transferred as encrypted data, while the remaining control data is transferred as non-
15 encrypted data.
5. Method according to claim 1, wherein the data stream comprises audio information.
- 20 6. Method according to claim 1, wherein the data stream comprises video information.
7. Data transmission system, capable of performing a method according to any of claims 1 to 6.
- 25 8. Device for transmitting an encrypted data stream, comprising:
a data source (101; 102) for providing payload data (APD; VPD) and control data (ACD; VCD);
a compression circuit (103; 104) for compressing the payload data and

providing compressed data (CAPD; CVPD) and decompression control data (ADCD; VDCD);

an encryption circuit (105; 106) for encrypting at least part of the control data (ADCD; VDCD) and providing encrypted control data (EACD; EVCD);

5 multiplexing means (107, 108, 109) for multiplexing the compressed data (CAPD; CVPD) and the encrypted control data (EACD; EVCD) and providing a multiplexed encrypted stream (MEAVS).

9. Device for receiving an encrypted data stream, comprising:

10 a demultiplexing circuit (111) for demultiplexing a multiplexed encrypted stream (MEAVS) and for thus retrieving encrypted control data (EACD; EVCD) and compressed data (CAPD; CVPD);

a decryption circuit (113; 114) for decrypting the retrieved encrypted control data (EACD; EVCD) and for thus retrieving decompression control data (ADCD; VDCD);

15 a processing circuit (115) for decompressing the retrieved compressed data (CAPD; CVPD) on the basis of the retrieved decompression control data (ADCD; VDCD), and for thus retrieving payload data (APD; VPD).

10. A multiplexed data signal (MEAVS) comprising:

20 compressed payload data (APD; VPD), at least partly non-encrypted, preferably entirely non-encrypted;

control data (ADCD; VDCD), at least partly encrypted, preferably entirely encrypted.

25 11. Signal according to claim 10, wherein the control data comprises decompression control data (ADCD; VDCD), which decompression control data is at least partly encrypted, preferably entirely encrypted.

1/2

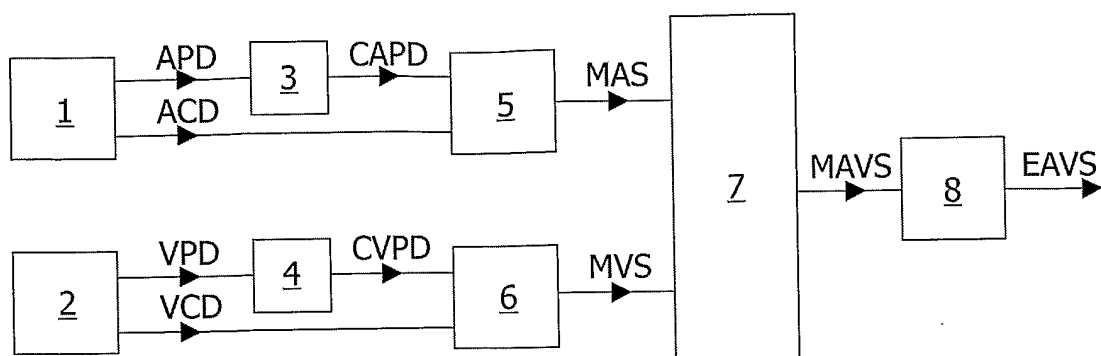


FIG. 1A

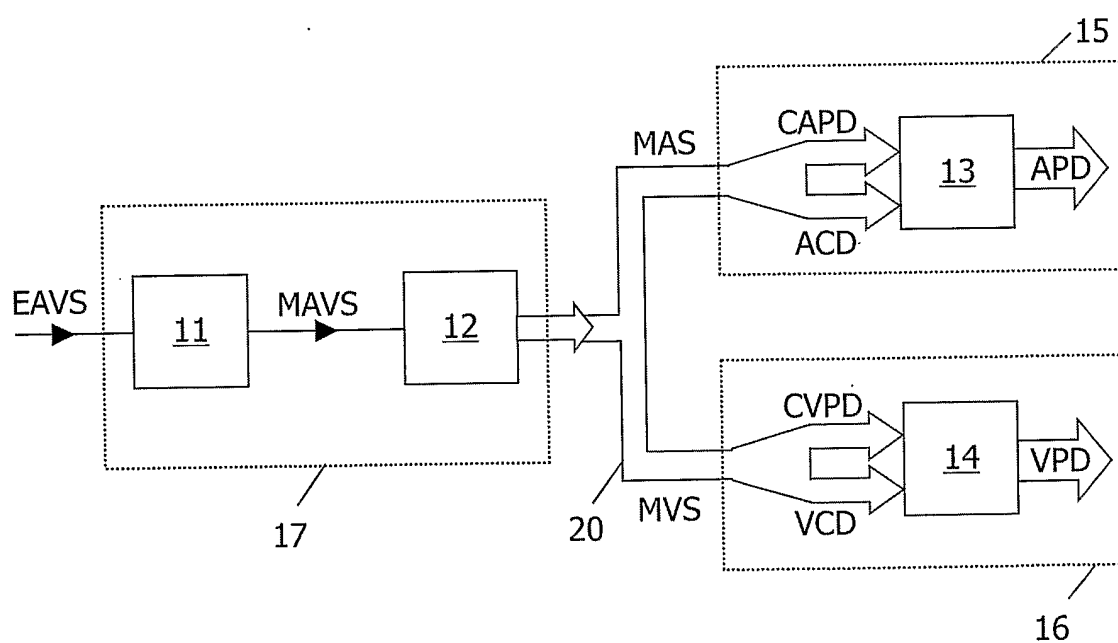


FIG. 1B

2/2

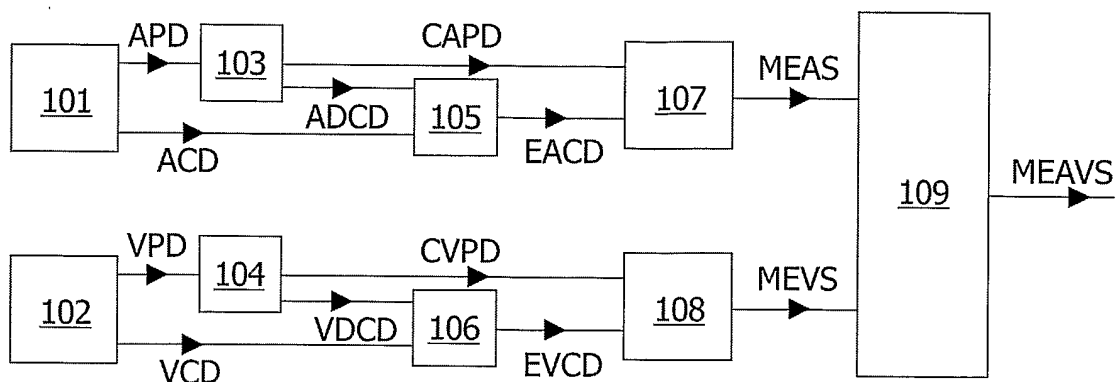


FIG. 2

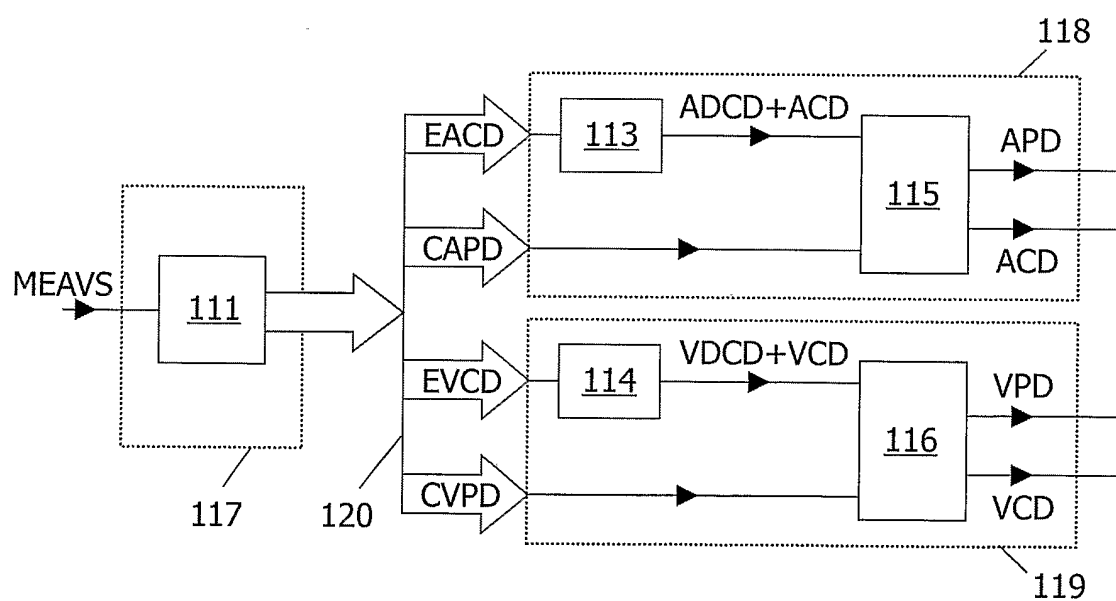


FIG. 3