[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04K 1/04

[12] 发明专利说明书

[21] ZL 专利号 97109393.8

[45] 授权公告日 2004 年 11 月 3 日

[11] 授权公告号 CN 1174578C

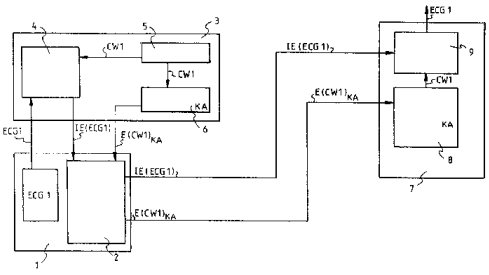
[22] 申请日 1997.11.14 [21] 申请号 97109393.8
[30] 优先权
[32] 1996.11.14 [33] FR [31] 9613889
[71] 专利权人 汤姆森多媒体公司
地址 法国布洛涅
[72] 发明人 阿诺多·坎皮诺斯
路易斯·格雷古瑞
让－玛丽·维格内龙
审查员 李 明
[74] 专利代理机构 北京市柳沈律师事务所
代理人 吕晓章

权利要求书 5 页 说明书 10 页 附图 8 页

[54] 发明名称 通过扰频进行数据确认的方法和采用该方法的确认系统

[57] 摘要

本发明涉及数据确认方法以及实施该确认方法的系统。 数据确认通过扰频进行。 独立于控制数据源的机构和将要使用这些数据的用户的特许装置借助控制字对数据扰频和借助具有密钥 K 的加密算法对控制字加密。 因此，一个或多个用户可对由独立特许装置扰频的数据解扰，将包含加密密钥 K 的确认验证装置提供给处在独立特许装置控制下的一个或多个用户。 该确认方法和与其相关的系统特别适用于条件访问的系统。



ISSN1008-4274

1. 一种确认从构成第一机构一部分的数据源生成的并将供至少一个用户使用的数据(ECG1)的方法，所述方法包括步骤：

－利用第一串控制字 CW1 对从所述数据源生成的所述数据进行扰频，以构成第一扰频项 IE(ECG1)，

－利用第一密钥 KA 对第一串控制字 CW1 加密，以构成第一串加密控制字 $E(CW1)_{KA}$，

其中所述扰频和加密步骤是由独立于第一机构和用户的特许装置进行的，所述方法还包括步骤：

－向用户传送所述第一扰频项 IE(ECG1)和所述第一串加密控制字 $E(CW1)_{KA}$，和

－利用提供给处在所述独立特许装置控制下的用户的装置对所述第一串加密的控制字 $E(CW1)_{KA}$ 解密和对所述第一扰频数据 IE(ECG1)解扰。

2. 根据权利要求 1 所述的方法，其中还包括在所述第一扰频项 IE(ECG1)和所述第一串加密控制字 $E(CW1)_{KA}$ 被传送到用户之前，将所述第一扰频项 IE(ECG1)和所述第一串加密控制字 $E(CW1)_{KA}$ 存储到构成第一机构一部分的数据库中的步骤。

3. 根据权利要求 1 所述的方法，其中还包括步骤：

－利用与所述第一密钥 KA 不同的第三密钥 KSP 对所述第一串加密控制字 $E(CW1)_{KA}$ 加密，以构成第三串加密控制字 $E(E(CW1)_{KA})_{KSP}$，其中由独立于所述第一机构和所述独立特许装置的第二机构执行所述加密步骤，

－向用户传送所述第三串加密控制字 $E(E(CW1)_{KA})_{KSP}$，和

－利用在所述独立特许装置控制下提供给用户的所述装置所述对第三串加密控制字解密以产生所述第一串加密控制字 $E(CW1)_{KA}$。

4. 根据权利要求 1 所述的方法，其中对所述第一串加密控制字 $E(CW1)_{KA}$ 解密和对所述第一扰频项 IE(ECG1)解扰的步骤禁止访问未加密的控制字 CW1。

5. 根据权利要求 1 所述的方法，还包括步骤：

－利用第二串控制字 CW2 对从至少一个另外的源生成的数据(ECG2)扰频，以构成第二扰频项 IE(ECG2)，

－利用不同于所述第一密钥 KA 的第二密钥 KB 对第二串控制字加密，以构成第二串加密控制字 $E(CW2)_{KB}$，

其中对从至少一个另外的源生成的数据扰频和对所述第二串控制字加密的所述步骤是在所述独立特许装置的控制下进行的，所述方法还包括步骤：

－向用户传送所述第二扰频项 IE(ECG2)和所述第二串加密控制字 $E(CW2)_{KB}$，和

－利用在所述独立特许装置的控制下提供给用户的所述装置对所述第二串加密的控制字 $E(CW2)_{KB}$ 解密和对所述第二扰频项 IE(ECG2)解扰。

6. 根据权利要求 5 所述的方法，其中还包括步骤：

－利用不同于所述第一和第二密钥的第三密钥 KSP 对所述第二串加密控制字 $E(CW2)_{KB}$ 加密，以构成第四串加密控制字 $E(E(CW1)_{KB})_{KSP}$，其中所述加密步骤是由独立于所述第一机构和所述独立特许装置的第二机构执行的，

－向用户传送所述第四串加密控制字，

－利用在所述独立特许装置的控制下提供给用户的所述装置对所述第四串加密控制字解密，以产生所述第二串加密控制字 $E(CW2)_{KB}$。

7. 根据权利要求 5 所述的方法，其中对所述第二串加密控制字 $E(CW2)_{KB}$ 解密和对所述第二扰频项 IE(ECG2)解扰的步骤禁止访问未加密的控制字 CW2。

8. 一种确认从一数据源生成的并供至少一个用户使用的数据的系统，所述数据源构成第一机构的一部分，其中它包括：

－一个第一扰频和加密装置，该装置构成独立于第一机构以及用户的特许装置一部分并利用第一串控制字 CW1 对从所述源生成的数据扰频，以构成第一扰频项 IE(ECG1)，和利用第一密钥 KA 对所述第一串控制字加密以构成第一串加密控制字 $E(CW1)_{KA}$，和

－一个确认验证装置，该确认验证装置提供给处在独立特许装置控制下的用户并包括对所述第一串加密的控制字 $E(CW1)_{KA}$ 解密和利用所述第一串解密的控制字 CW1 对所述第一扰频项 IE(ECG1)解扰的电路。

9. 根据权利要求 8 所述的确认系统，其中所述第一机构包括存储所述第一扰频项 IE(ECG1)和所述第一串加密的控制字 $E(CW1)_{KA}$ 的数据库，所

述数据库链接到确认验证装置，以便向所述确认验证装置提供所述第一扰频项 IE(ECG1)以及所述第一串加密的控制字 $E(CW1)_{KA}$。

10. 根据权利要求 8 所述的确认系统，其中对所述第一串加密的控制字解密和对所述第一扰频项解扰的电路包括：

含有对其接收的所述第一串加密控制字 $E(CW1)_{KA}$ 解密的所述第一加密密钥 KA 的芯片卡(8)；和

利用所述第一串解密控制字 CW1 对所述第一扰频项解扰解码器。

11. 根据权利要求 8 所述的确认系统，其中对所述第一串加密的控制字解密和对所述第一扰频项解扰的电路由一芯片卡构成。

12. 根据权利要求 8 所述的确认系统，其中所述第一机构包括至少一个另外的数据(ECG2)源，和被委托给处在所述独立特许装置控制下的所述第一机构的第二扰频与加密装置，其用于借助第二串控制 CW2 对所述另外的数据扰频以构成第二扰频项 IE(ECG2)和利用不同于所述第一密钥 KA 的第二密钥 KB 对所述第二串控制字 CW2 加密以构成第二串加密控制字 $E(CW2)_{KB}$，并将所述第二扰频项 IE(ECG2)和所述第二串加密控制字 $E(CW2)_{KB}$ 传送到确认验证装置。

13. 根据权利要求 12 所述的确认系统，其中所述确认验证装置包括：

含有所述第一和第二加密密钥 KA 和 KB 以对所述第一串加密控制字 $(E(CW1)_{KA})$或所述第二串加密控制字$(E(CW2)_{KB})$解密的芯片卡；和

利用所述第一串控制字(CW1)或所述第二串控制字(CW2)对所述第一扰频项 IE(ECG1)或所述第二扰频项 IE(ECG2)解扰的解码器。

14. 根据权利要求 12 所述的确认系统，其中所述确认验证装置包括一芯片卡，该芯片卡含有所述第一和第二加密密钥 KA 和 KB，以对所述第一串加密控制字$(E(CW1)_{KA})$或所述第二串加密控制字$(E(CW2)_{KB})$解密并用于对所述第一扰频项 IE(ECG1)或所述第二扰频项 IE(ECG2)解扰。

15. 根据权利要求 8 所述的确认系统，还包括一分配电路，它构成独立于第一机构和独立特许装置的第二机构一部分，其中所述分配电路接收所述第一扰频项 IE(ECG1)和所述第一串加密控制字 $E(CW1)_{KA}$ 并包含：

－一个利用不同于所述第一密钥密钥 KA 的第三密钥 KSP 对所述第一串加密控制字 $E(CW1)_{KA}$ 加密，以产生第三串加密的控制字 $E(E(CW1)_{KA})_{KSP}$ 的电路，

一一个存储所述第一扰频项 IE(ECG1)以及所述第三串加密控制字 $E(E(CW1)_{KA})_{KSP}$ 的数据库，所述数据库链接到确认验证装置，以便为所述确认验证装置提供所述第一扰频项 IE(ECG1)以及所述第三串加密控制字 $E(E(CW1)_{KA})_{KSP}$，

所述确认验证装置包括用于对所述第三串加密控制字 $E(E(CW1)_{KA})_{KSP}$ 解密以产生所述第一串加密控制字 $E(CW1)_{KA}$ 的装置。

16. 根据权利要求 15 所述的确认系统，其中所述确认验证装置包括:

一芯片卡，它含有所述第一和第三加密密钥 KA 和 KSP 以便对所述第三串控制字 $E(E(CW1)_{KA})_{KSP}$ 和所述第一串控制字 $E(CW1)_{KA}$ 解密；和

一解码器，利用所述第一串解密控制字 CW1 对所述第一扰频项解扰。

17. 根据权利要求 15 所述的确认系统，其中所述确认验证装置包括:

一芯片卡，它包含所述第一和第二加密密钥 KA 和 KSP，以便对所述第三串控制字 $E(E(CW1)_{KA})_{KSP}$ 和所述第一串控制字 $E(CW1)_{KA}$ 解密，并利用所述第一串解密控制字 CW1 对所述第一扰频项解扰。

18. 根据权利要求 15 所述的确认系统，其中所述第一机构包括至少一个另外的数据(ECG2)源，其中所述第二机构包括在独立特许装置控制下提供的委托扰频和加密装置，用于借助第二串控制字(CW2)对所述另外的数据扰频，以构成第二扰频项 IE(ECG2)，和利用不同于所述第一密钥 KA 的第二密钥 KB 对所述第二串控制字(CW2)加密，以构成第二串加密控制字 $E(CW2)_{KB}$，所述第二串加密控制字和所述第二扰频项 IE(ECG2)被送至所述分配电路，所述分配电路还包含:

利用所述第三密钥 KSP 对所述第二串加密控制字 $E(CW2)_{KB}$ 加密的电路，以构成第四串加密控制字串 $E(E(CW2)_{KB})_{KSP}$，以及

用于存储所述第四串加密控制字 $E(E(CW2)_{KB})_{KSP}$ 和所述第二扰频项 IE(ECG2)的数据库，所述数据库链接到确认验证装置，以便将所述第四串加密控制字 $E(E(CW2)_{KB})_{KSP}$ 以及所述第二扰频项 IE(ECG2)提供给所述确认验证装置。

19. 根据权利要求 18 所述的确认系统，其中所述确认验证装置包括:

一芯片卡，包含所述第一、第二和第三加密密钥 KA、KB 和 KSP，以便对所述第三串加密控制字 $E(E(CW1)_{KA})_{KSP}$ 或所述第四串加密控制字 $E(E(CW2)_{KB})_{KSP}$ 以及所述第一串加密控制字 $E(CW1)_{KA}$ 或所述第二串加密控

制字 $E(CW2)_{KB}$ 解密；及

一解码器，利用所述第一串解密控制字 CW1 对所述第一扰频项 IE(ECG1)解扰或利用所述第二串加密控制字 CW2 对第二扰频项 IE(ECG2)解扰。

20. 根据权利要求 18 所述的确认系统，其中所述确认验证装置包括一芯片卡，所述芯片卡包含所述第一、第二和第三加密密钥 KA、KB 和 KSP，以便对所述第三串加密控制字 $E(E(CW1)_{KA})_{KSP}$ 或所述第四串加密控制字 $E(E(CW2)_{KB})_{KSP}$ 以及所述第一串加密控制字 $E(CW1)_{KA}$ 或所述第二串加密控制字 $E(CW2)_{KB}$ 解密；并利用所述第一串解密控制字 CW1 对所述第一扰频项 IE(ECG1)解扰或利用所述第二串加密控制字 CW2 对第二扰频项 IE(ECG2)解扰。

21. 根据权利要求 15 所述的确认系统，其中所述第一机构是一个数据提供者，所述第二机构是一个业务提供者，和所述用户是该业务提供者的一个用户。

22. 根据权利要求 12 所述的确认系统，其中所述第一串控制字(CW1)由构成第一扰频与加密装置一部分的第一控制字发生器产生，而所述第二串控制字(CW2)由构成第二委托的扰频与加密装置一部分的第二控制字发生器产生。

23. 根据权利要求 12 所述的确认系统，其中所述第一串控制字(CW1)与所述第二串控制字(CW2)相同。

24. 根据权利要求 12 所述的确认系统，其中所述第一串控制字(CW1)与所述第二串控制字(CW2)不同。

25. 如权利要求 18 所述的确认系统，其中所述第一串控制字(CW1)由构成第一扰频与加密装置一部分的第一控制字发生器产生，而所述第二串控制字(CW2)由构成第二委托的扰频与加密装置一部分的第二控制字发生器产生。

26. 如权利要求 18 所述的确认系统，其中所述第一串控制字(CW1)与所述第二串控制字(CW2)相同。

27. 如权利要求 18 所述的确认系统，其中所述第一串控制字(CW1)与所述第二串控制字(CW2)不同。

通过扰频进行数据确认的方法和采用该方法的确认系统

本发明涉及数据确认方法以及实施该方法的系统.

本发明特别应用于包含诸如具有约4至5兆比特/秒的比特率的视频数据之类大信息量的数据的确认.

根据现有技术，视频数据的确认是通过加标记进行的：借助于散列算法对视频信号进行散列和借助密钥对从该散列算法生成的每个信息块加标记.

该确认方法具有耗时的缺陷.处理信息的系统的中央单元必须实际考虑可提供给确认操作的处理能力，该中央单元通常被为 CPU(“中央处理单元”).

本发明没有这种缺陷.

本发明的目的是提供一种通过对将要从数据源传送到至少一个接收装置的数据扰频来进行确认的方法，以及使其能够实施该方法的系统.

根据本发明，独立于控制数据源的机构和将要使用这些数据的用户的特许装置借助控制字对数据扰频并借助具有密钥 KA 的加密算法对控制字加密.因此，一个或多个用户可对由独立特许装置扰频的数据解扰，将包含加密密钥 KA 的确认验证装置提供给处在独立特许装置控制下的一个或多个用户.

涉及控制数据源的机构和将要被提供数据的用户的短语“独立特许装置”应被理解为是指由独立特许装置进行的数据扰频以及控制字加密不为控制数据源的机构和数据用户所知.

同样，所说的提供给处在独立特许装置控制下的用户的确认验证装置是指该确认验证装置包含仅有独立特许装置独自了解并能够从其接收的扰频项恢复一个不加密项的信息.

因此，本发明涉及对从构成第一机构一部分的数据源生成的并将供至少一个用户使用的数据进行确认的方法.该方法包括：

- 借助一个第一串控制字 CW1 对从数据源生成的数据 ECG1 进行扰

频，以构成第一扰频项 IE(ECG1)的步骤，

－借助具有密钥 KA 的加密算法对第一串控制字 CW1 加密，以构成第一串加密控制字 $E(CW1)_{KA}$ 的步骤，

所述扰频和加密步骤是由独立于第一机构和用户的特许装置(authority)进行的，

－向用户传送第一扰频项 IE(ECG1)和第一串加密控制字 $E(CW1)_{KA}$ 的步骤，和

－借助提供给处在独立特许装置控制下的用户的装置对加密的控制字 $E(CW1)_{KA}$ 解密和对扰频数据 IE(ECG1)解扰的步骤.

作为实例，可在 DES 标准("数据加密标准")或 DVB 超级扰频器标准("数字视频广播超级扰频器")下由一扰频算法进行对数据 ECG1 扰频的步骤.

本发明还有一个目的是提供一种用于对从一数据源生成的并供至少一个用户使用的数据进行确认的系统，数据源构成第一机构的一部分．该确认系统包括:

－一个扰频和加密装置，该装置构成独立于第一机构的特许装置一部分并能够用第一串控制字 CW1 对从数据源生成的数据扰频，以构成第一扰频项 IE(ECG1)，和借助具有密钥 KA 的加密算法对第一串控制字 CW1 加密以构成加密控制字 $E(CW1)_{KA}$，和

－一个确认验证装置，该确认验证装置提供给处在独立特许装置控制下的用户并包括能够对加密的控制字 $E(CW1)_{KA}$ 解密和借助解密的控制字 CW1 对第一扰频项 IE(ECG1)解扰的电路.

其优点在于，设置有确认验证装置的用户可仅对在独立特许装置控制下扰频的数据解扰.

根据本发明，可由独立特许装置直接或间接进行数据的确认。

在直接确认的情况下，扰频和加密电路构成由独立特许装置本身构成的结构的一部分。

在间接确认的情况下，由独立特许装置将扰频和加密电路委托给与独立特许装置不同的机构．与独立特许装置不同的这种机构可以是控制数据源的机构或与控制数据源的机构不同的机构.

根据本发明优选实施例的有益改进，在构成独立特许装置一部分的扰频和加密装置外部，在确认系统的任何位置都不能访问未加密控制字．在间接确认

情况下，被委托的扰频和加密装置具体体现为一个电路，例如一个芯片卡，该电路不允许对其在其自身内生成的控制字的未加密存取。

如前所述，本发明的一个优点在于在很大程度上减少了与数据确认操作有关的处理时间。因此允许大信息量的确认。

通过阅读参考附图给出的优选实施例将使本发明的其它特征和优点显而易见。

图 1 表示根据本发明通过扰频进行确认的第一系统的示意图；

图 2 表示根据前面提到的本发明的改进通过扰频进行确认的第一系统的示意图；

图 3 表示根据本发明通过扰频进行确认的第二系统的示意图；

图 4 表示根据前面提到的本发明的改进通过扰频进行确认的第二系统的示意图；

图 5 表示根据本发明的确认系统的第一应用；

图 6 表示根据前面提到的本发明的改进的确认系统的第一应用；

图 7 表示根据本发明的确认系统的第二应用；

图 8 表示根据前面提到的本发明的改进的确认系统的第二应用。

在所有附图中，相同标号表示同一种元件。

图 1 表示根据本发明通过扰频进行确认的第一系统的示意图。

图 1 的系统包括一个信息源 1，一个扰频和加密装置 3 以及一个确认验证装置 7。

扰频和加密装置 3 构成前面提到的独立特许装置构成的结构的一部分，确认验证装置 7 是提供给处在独立特许装置控制下的用户的装置。

根据本发明，信息源 1 中包含的项 ECG1 是被送到扰频和加密装置 3 中包含的扰频装置 4 的未加密项。

在视频数据情况下，未加密项 ECG1 是在 MPEG2 标准下以例如数据流的形式发送的。

扰频和加密装置 3 还包括一个控制字 CW1 发生器 5，以及一个借助具有密钥 KA 的算法用于对控制字加密的装置 6。

一方面将控制字 CW1 应用到扰频装置 4 以使后者产生扰频项 IE(ECG1)，另一方面将控制字 CW1 应用到加密装置 6，以使后者产生借助具有密钥 KA 的加密算法加密的控制字 $E(CW1)_{KA}$。

从扰频和加密装置3生成的扰频项IE(ECG1)和加密控制字$E(CW1)_{KA}$存储在构成包含信息源1的机构的一部分的数据库2中.

数据库2以可将扰频项IE(ECG1)和加密控制字$E(CW1)_{KA}$传输到装置7的方式链接到确认验证装置7．装置7是一个包括例如包含用于对控制字加密的密钥KA的芯片卡8和解码器9的解扰装置.

芯片卡8接收加密的控制字$E(CW1)_{KA}$，将它们解密并将它们传送到解码器9.

扰频项IE(ECG1)被传送到解码器9．在从芯片卡8生成的控制字CW1的作用下，解码器9产生解扰项ECG1.

根据本发明，控制扰频和加密装置3和确认验证装置7的独立特许装置是待传送数据的规定通路.

其优点在于，除实际执行经独立特许装置传送的数据的确认外，独立特许装置可保证数据的原貌和/或完整性．短语“数据的完整性”应被理解为是指由接收电路恢复的未加密数据确实是信息源输出的那些数据.

图2表示根据本发明的改进通过扰频进行确认的第一系统的示意图.

扰频和加密装置3以及信息源1与图1中描述的相同.

图2的确认验证装置7包含与图1的装置7中包含的那些元件完全或部分不同的元件.

根据图2表示的本发明的改进，用户卡23使得不仅能够借助它所包含的密钥KA对控制字解密，而且能对扰频项IE(ECG1)解扰．作为实例，该芯片卡可以是遵照“电子工业协会”协会公布的美国标准“国家可更新安全标准”、DIS679的卡，或者可以是符合本领域技术人员已知的接口标准作为“DVB公用接口”的PCMCIA型芯片卡.

用户卡接收由扰频项IE(ECG1)和加密控制字$E(CW1)_{KA}$构成的数据流.从卡23生成的项C(ECG1)是以例如MPEG数据流形式编码的解扰项．解码器24接收项C(ECG1)以便对其解码.

如前所述，其优点在于，在用户一级不能访问未加密的控制字CW1，因此，除属于独立特许装置的装置3之外，没有任何地方可访问控制字.

图3表示根据本发明通过扰频进行确认的第二系统的示意图.

图3描述的系统由与图1和2描述的相同结构构成：一个信息源1，一个扰频和加密装置3以及一个确认验证装置7.

根据通过扰频进行确认的第二系统，未加密数据 ECG1 的第一部分经与图 1 中描述的电路相同的电路传送，未加密数据 ECG2 的第二部分经与图 1 描述的电路不同的电路传送。

传送数据 ECG2 的电路包括被委托用于扰频和加密的装置 10。根据图 3 表示的实例，装置 10 构成包含信息源 1 的机构的一部分。根据其它实施例，电路 10 可属于与包含源 1 的机构不同的机构。

电路 10 包括控制字 CW2 发生器 12，通过加密密钥 KB 对控制字加密的装置 13 和扰频装置 11。

一方面将控制字 CW2 施加到扰频装置 11，另一方面将控制字 CW2 施加到加密装置 13，以使后者产生借助具有密钥 KB 的加密算法加密的控制字 $E(CW2)_{KB}$。

控制字 CW2 起到对项 ECG2 扰频的作用。从电路 10 生成的扰频项 IE(ECG2)和加密控制字 $E(CW2)_{KB}$ 被从信息源 1 送到确认装置 7。

确认验证装置 7 是包括例如芯片卡 14 和解码器 15 的解扰电路。将加密的控制字 $E(CW2)_{KB}$ 施加到不仅包含加密密钥 KA 而且包含加密密钥 KB 的卡 14。它遵循由卡 14 产生控制字 CW2 和 CW1。然后在其输入端接收扰频数据 IE(ECG1)和/或 IE(ECG2)的解码器 15 可对它们解扰并产生未加密项 ECG1 和/或 ECG2。

根据图 2 表示的本发明的实施例，确认装置 10 被前面提到的独立特许装置委托给控制信息源的机构。

这种通过委托进行确认的系统的优点在于使得能够将待确认的信息项等级化。在图 7 和 8 中描述的实例应用中将使待确认数据的这种等级化更加显而易见。

图 4 表示根据本发明的改进通过扰频进行确认的第二系统的示意图。

扰频和加密装置 3 以及信息源 1 与图 3 中描述的相同。

根据本发明的改进，用户卡 25 接收数据 IE(ECG1)、$E(CW1)_{KA}$、IE(ECG2)、$E(CW2)_{KB}$ 的集合。用户卡借助其所包含的密钥 KA 和 KB 对加密的控制字解密，并借助解密的控制字对扰频项解扰。

从卡 25 生成的项则包括解扰和编码项 C(ECG1)和 C(ECG2)。正如图 2 描述的实施例的情况，由因此使得能够产生未加密项 ECG1 和 ECG2 的解码器 26 对例如 MPEG 数据流形式的编码项进行解码。

图5、6、7和8表示根据本发明的确认系统对一个条件访问系统的实例应用.

正如本领域技术人员所了解的，条件访问系统使业务提供者将其业务仅提供给那些已获得与这些业务有关的权利的用户．例如付费电视系统中的情况就是这样.

正如本领域技术人员所了解的，由业务提供者提供的业务包括用控制字扰频的项．可仅对扰频项解扰，并由用户根据分配给该用户的权利阅读.

为对该项解扰，业务提供者向每个用户提供用来对该项扰频的控制字．为使控制字保密，在借助具有密钥KSP的算法对其加密后提供该控制字，密钥KSY是专用于该业务提供者的密钥.

各种加密控制字在下面将表示为ECM的消息中送到各个用户.

为仅允许被许可的单独用户访问其业务，业务提供者为每个用户提供一个芯片卡和一个解码器．由该芯片卡和解码器构成的设备使得能够对扰频项解扰.

一方面，芯片卡使得能够确认和记录与传送的业务有关的用户的权利，另一方面能借助密钥KSP对加密的控制字解密．对此目的，芯片卡包含使控制字加密成为可能的算法的密钥KSP．

在下面将表示为EMM的消息中传送每个用户的权利.

根据已知技术，专用于一个用户的EMM包含三个主项:

- 给出用户卡的地址的第一项;

- 给出用户权利说明的第二项;

- 使得能够确认EMM并验证该EMM中包含的用户权利确实是供该用户使用的权利的第三项.

如前所述，被加密的控制字经ECM送到用户.

根据已知技术，一个ECM包括一个标题和一个主体;

其中，标题给出ECM的主体中包含的项的类型和大小; 其中，主体由包含访问提供者提供的业务的条件集合的项、包含借助具有密钥KSP的算法加密的控制字的项和包含取决于密钥 KSP 的数据并使得能够确认和验证ECM、特别是ECM中包含的访问条件的内容的项构成.

当用户的解码器从业务提供者分配的各个地址中识别出与其相关的卡的地址时，由该卡分析与所识别地址对应的EMM． EMM的分析通常是借

助于取决于用于加密控制字的密钥KSP的分析算法进行的.

条件访问系统主要有两种类型.

第一种系统通常被称为在线系统. 在一在线条件访问系统中, 被扰频的项是由从一个单一信息源同时分配给一个业务提供者的各个用户的信号构成的项. 例如, 可采取无线或有线方式进行这种分配. 正如本领域技术人员所了解的, 在这种条件访问系统中, 由业务提供者将 ECM 与被扰频的项一起发送.

第二种条件访问系统通常被称为独立系统. 在一独立的条件访问系统中, 被扰频的项和ECM被包含在诸如例如密致盘(光盘)或数字视频盘之类的独立信息介质上.

在本发明应用于条件访问系统的架构内, 用与业条提供者无关的特许装置将控制字扰频后由该业务提供者向其用户提供加密的控制字.

因此, 本发明涉及一条件访问系统, 该条件访问系统包括至少一个在通过业务提供者分配给至少一个用户之前将被扰频的信息项源. 该系统包括一个能够通过一第一串控制字对所述信息项扰频的装置, 一个借助具有密钥KA的加密算法对第一串控制字加密的装置和一个能够借助具有密钥KSP的算法对所加密的控制字加密的加密装置, 密钥KSP取决于业务提供者, 而密钥KA取决于与业务提供者无关的特许装置.

图5表示根据本发明的确认系统对一条件访问系统的第一实例应用.

该系统由未加密数据源1, 分配电路16, 扰频和加密装置3和确认验证装置7组成.

未加密数据ECG1的源1构成由一数据提供者构成的机构的一部分. 分配电路16属于业务提供者, 分配电路的功能是分配其从数据提供者接收的数据. 扰频和加密装置3构成由独立特许装置构成的结构的一部分. 装置7被提供给处在独立特许装置控制下的业务提供者的各个用户.

短语"独立特许装置"在此应被理解为是指与数据提供者、业务提供者以及业务提供者的用户无关的一个机构.

如前所述, 未加密项ECG1发送到包含在装置3中的扰频装置4, 被扰频的项IE(ECG1)存储在数据库2中. 借助具有密钥KA的加密算法对使未加密项的扰频成为可能的控制字CW1加密并将加密的控制字$E(CW1)_{KA}$存储在数据库2中.

业务提供者的分配电路16包括一个加密电路17和一个数据库18。

将被扰频的项IE(ECG1)发送到数据库18并将加密的控制字$E(CW1)_{KA}$发送到加密装置17。加密装置17是一个具有加密密钥KSP的加密装置，密钥KSP是一个专用于业务提供者的密钥并且最好与密钥KA不同。

由业务提供者发送到用户的数据包括被扰频的项IE(ECG1)和从数据$E(CW1)_{KA}$的加密生成的项$E(E(CW1)_{KA})_{KSP}$。

确认验证装置7包括一个用户卡19和一个解码器20。

通过图3中表示为ECMA的ECM将项$E(E(CW1)_{KA})_{KSP}$发送到包含加密密钥KA和KSP的用户卡19。

用户卡19对其接收的项解密，并因此使得能够产生施加到解码器20、允许对项IE(ECG1)解扰的控制字CW1。

用户卡包含两个加密密钥KA和KSP。根据本发明的优选实施例，由独立特许装置发布用户卡，以使密钥KA对在其控制下工作的该业务提供者或各个业务提供者和该数据提供者或各个数据提供者保密。

图6表示根据前面提到的本发明改进的确认系统的第一应用。

用户卡27接收由被扰频的项IE(ECG1)和消息ECMA构成的数据流。从用户卡生成的项是编码的解扰项C(ECG1)。解码器28使以产生未加密项ECG1这样一种方式解码编码的项C(ECG1)成为可能。

根据如图5和6中描述的本发明的系统特别应用于从例如前面提到的介质之类独立信息介质生成数据ECG1的独立条件访问系统，或在数据ECG1包括记录业务和/或节目的情况下应用到在线条件访问系统。

最好是，在不仅广播记录业务和/或节目上而且直播业务和/或节目的在线条件访问系统的情况下，本发明涉及诸如图7和8中表示的那些条件访问系统。

在这种条件访问系统中，独立特许装置将其鉴别权委托给各个业务提供者。每个业务提供者则包括一个其加密密钥不同于密钥KA的确认装置。

图7中描述的系统由与图5和6中描述的相同结构组成：一个数据提供者，至少一个业务提供者，一个独立特许装置和至少一个配备有包括一个用户卡21和一个解码器22的确认验证装置7的业务提供者的用户。

根据条件访问系统的第二种类型，从信息源1生成的未加密数据包括两种项ECG1和ECG2。

数据ECG1与前面提到的那些类型相同．这些数据的广播对应用到在线条件访问系统以及独立条件访问系统同样适合．

数据ECG2构成仅应用到在线条件访问系统的直播业务和/或节目，或其确认等级不需要与经装置3直接传送的数据ECG1的确认等级同样高的记录节目．

为确认数据ECG2，在每个业务提供者一级和分配给每个用户的确认验证装置7中引入新电路．

扰频和加密装置10提供给处在独立特许装置控制下的每个业务提供者．仅有独立特许装置知道加密装置12的密钥KB．根据本发明的优选实施例，密钥KB对从一个和相同提供者接收数据的所有业务提供者是公用的．根据其它实施例，密钥KB从一个业务提供者到另一个业务提供者或从一组业务提供者到另一组业务提供者是不同的。

从装置10生成的项$E(CW2)_{KB}$被发送到允许生成项$E(E(CW2)_{KB})_{KSP}$的业务提供者的加密装置17．

从发生器12生成的控制字CW2被发送到另外接收包括由数据提供者现场传送的节目和/或业务的数据ECG2的扰频装置11．从扰频装置11的输出则包括被发送到业务提供者的数据库18的被扰频的项IE(ECG2).

项$E(E(CW2)_{KB})_{KSP}$经图4中表示为ECMB的ECM发送到除加密密钥KA和KSP外还包含加密密钥KB的用户卡21．

根据图4的条件访问系统，用户卡21使用密钥KA和KSP解密由ECMA携带的控制字，或使用密钥KB和KSP解密由ECMB携带的控制字.

由业务提供者发送到其各个用户的ECM包含一能发出表示其特性的信号、也就是说是ECMA还是ECMB的项．可借助ECM中携带的信令比特和表明其是否是一ECMA的第一值和补充第一值、表明这是否是一ECMB的第二值设计该项．用户卡21则包含用于处理信令比特以便能触发对ECMA携带的控制字解密的密钥KA和KSP的使用，或触发对ECMB携带的控制字解密的密钥KB和KSP的使用的电路。

图8表示根据前面提到的本发明改进的确认系统的第二应用.

用户卡29接收数据IE(ECG1)、ECMA、IE(ECG2)和ECMB的集合.

从卡29生成的项C(ECG1)和C(ECG2)是被解扰和编码的项。

解码器30使得能够从其接收的项C(ECG1)和C(ECG2)恢复未加密的项

ECG1 和 ECG2 .

其优点在于，通过由诸如图 5 、 6 、 7 和 8 中所描述的那些确认保护的条件访问系统仅保证仅有由与提供未加密数据的那些提供者以及业务提供者无关的特许装置确认的数据可在该系统中流过。

本发明的另一个优点是保证在条件访问系统内流动的数据的完整性。

因此，由于通过独立特许装置对基于数据扰频的确认技术的使用，使得各个业务提供者不会因担忧防范其用户能对扰频项解扰而修改数据内容。

另外，通过证明，未加密数据的提供者总可借助独立特许装置提出其提供的数据版本。

根据上述实施例，数据提供者和业务提供者构成相互独立的分离结构。根据其它实施例，数据提供者和业务提供者构成一个并且是同一个单一的机构。

根据本发明的优选实施例，第一串控制字的控制字 CW1 与第二串控制字的控制字 CW2 不同。然而，本发明涉及控制字 CW 与控制字 CW2 相同的情况。

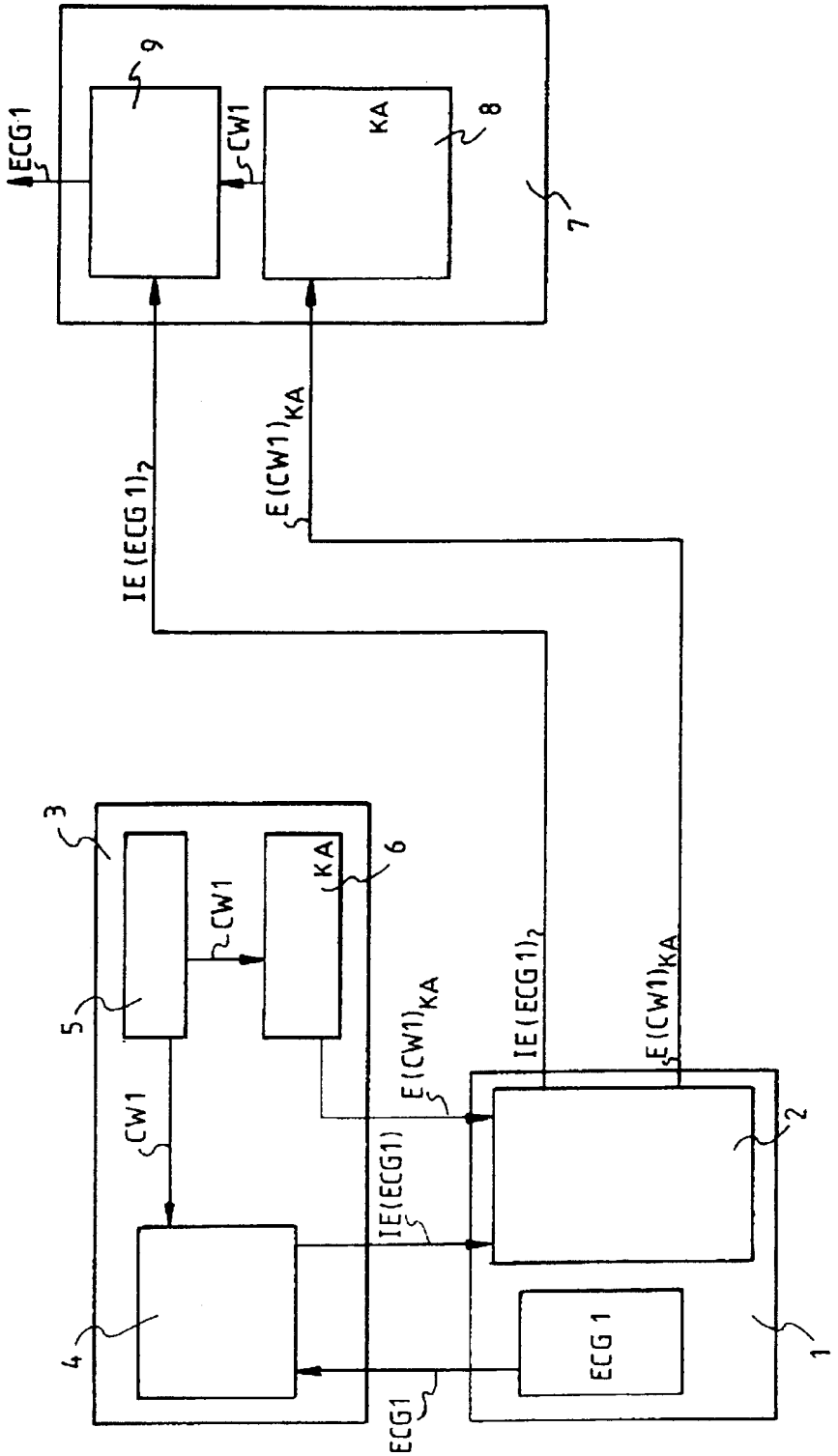

ECG 1
9
CW1
KA
8
7
$IE(ECG\,1)_2$
$E(CW1)_{KA}$
3
5
CW1
KA
6
CW1
$E(CW1)_{KA}$
$IE(ECG\,1)_2$
$E(CW1)_{KA}$
IE(ECG1)
2
4
ECG 1
1
ECG1

图 1

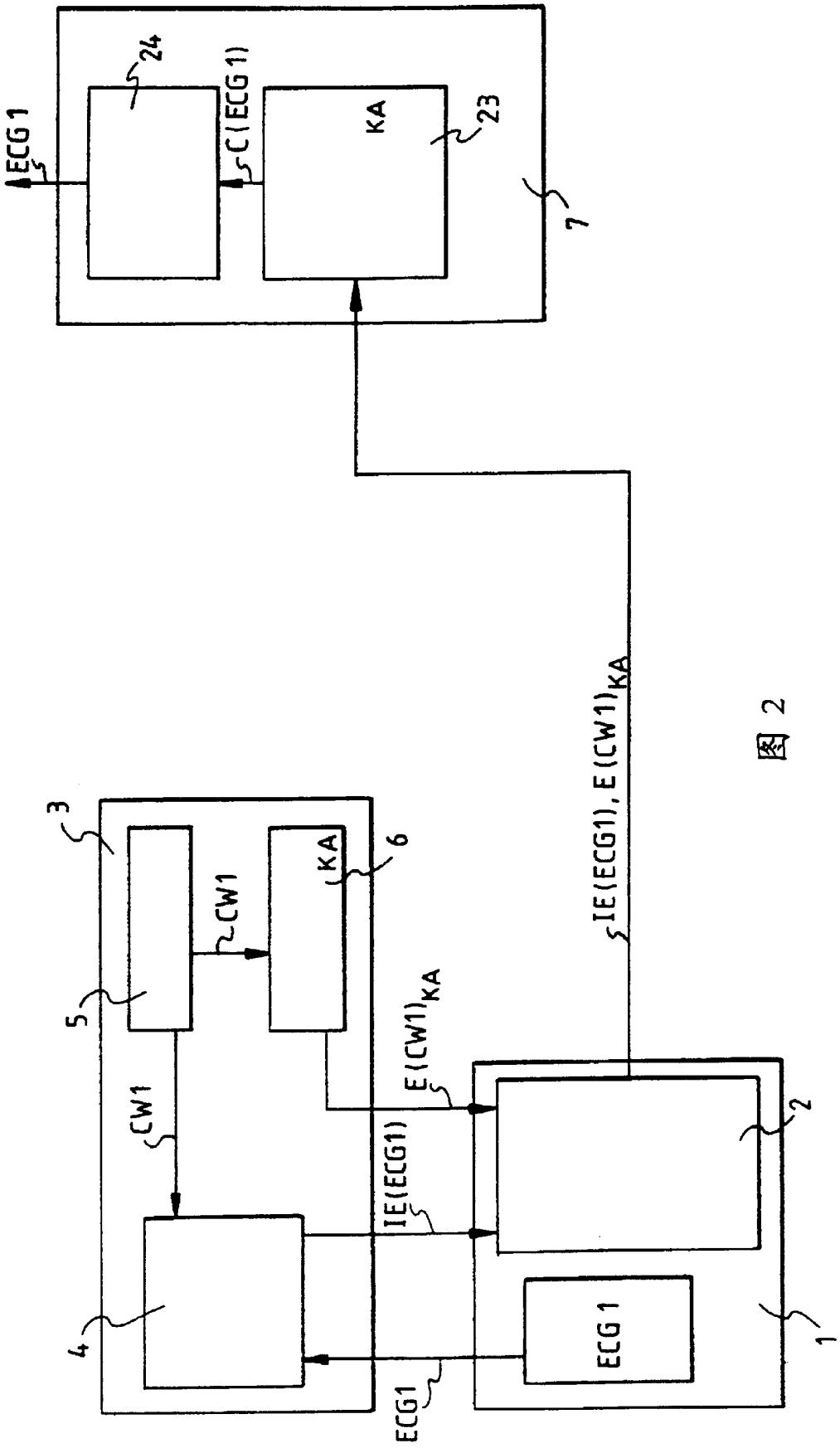

ECG 1
24
C(ECG 1)
KA
23
7
IE(ECG1), E(CW1)KA
3
CW1
KA
6
5
E(CW1)KA
CW1
IE(ECG1)
2
4
ECG 1
1
ECG1

图 2

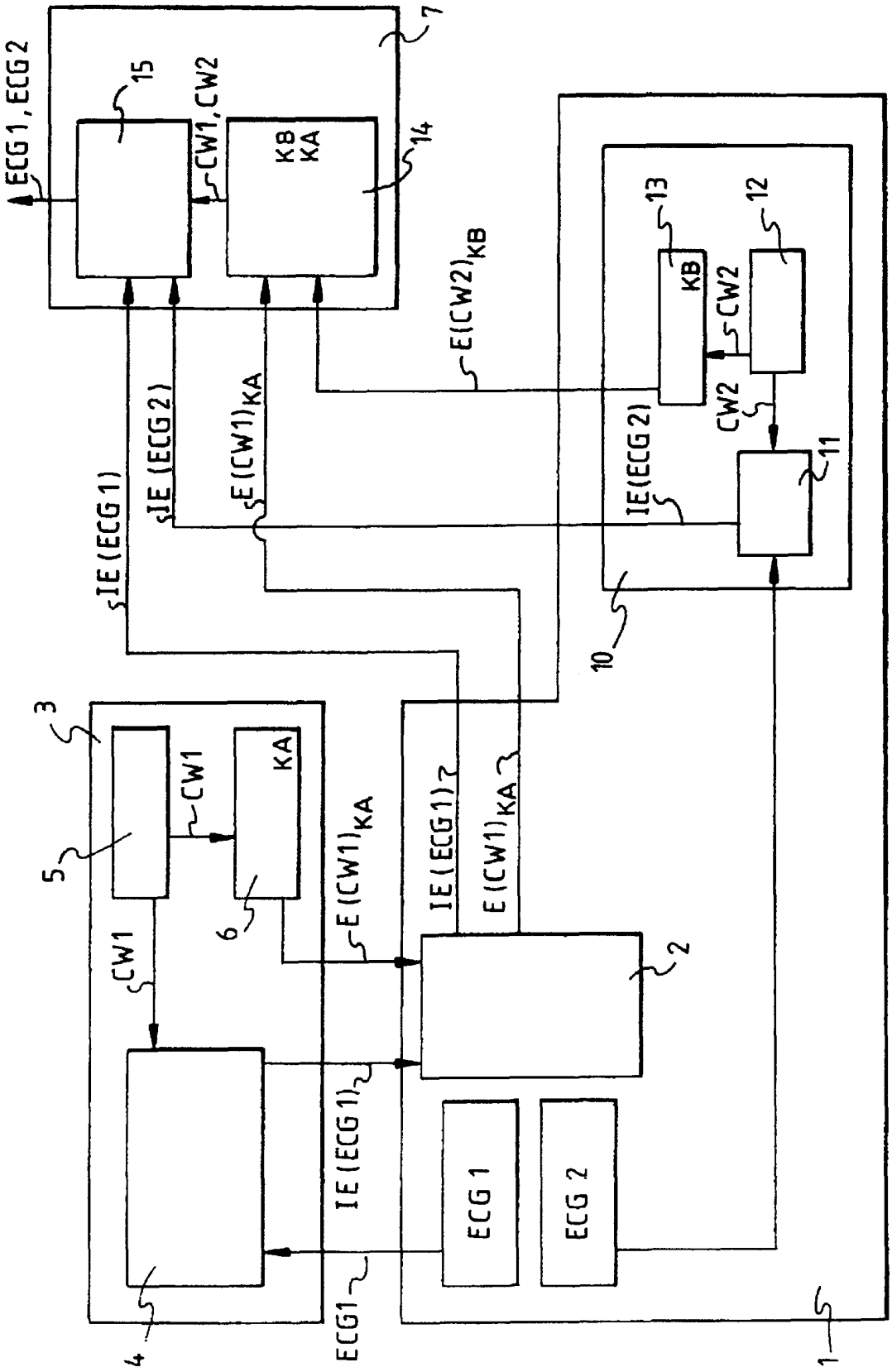

ECG1, ECG2
15
CW1, CW2
KB
KA
14
7
E(CW2)KB
13
KB
12
CW2
CW2
11
IE(ECG2)
10
IE(ECG1)
IE(ECG2)
E(CW1)KA
3
5
CW1
KA
6
CW1
E(CW1)KA
IE(ECG1)
E(CW1)KA
2
IE(ECG1)
ECG 1
ECG 2
4
ECG1
1

图 3

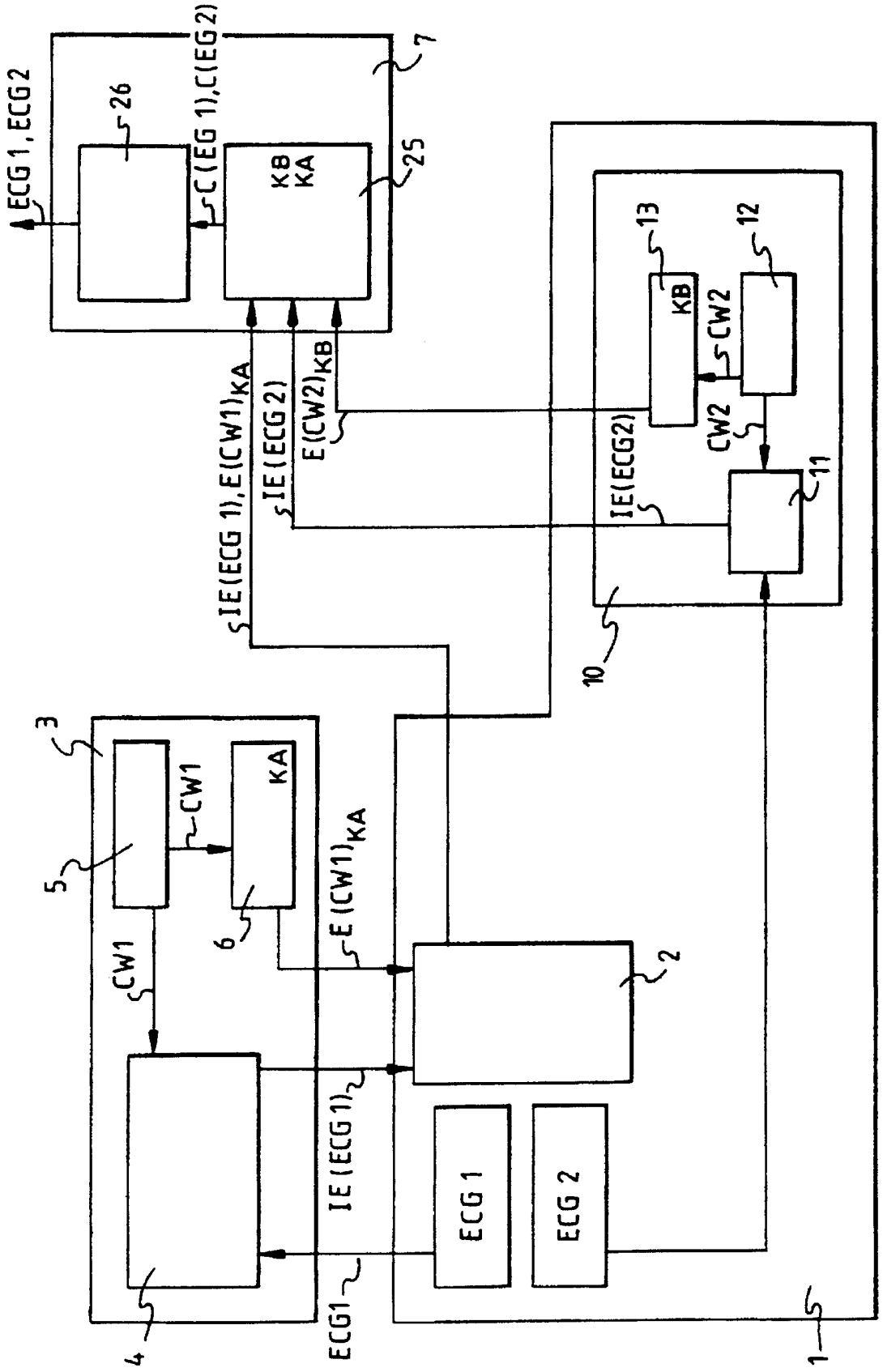

ECG1, ECG2
26
C(EG1), C(EG2)
7
KB
KA
25
13
12
KB
CW2
CW2
11
IE(ECG2)
IE(ECG1), E(CW1)KA
IE(ECG2)
E(CW2)KB
10
3
CW1
KA
5
6
E(CW1)KA
CW1
2
IE(ECG1)
ECG 1
ECG 2
4
ECG1
1

图 4

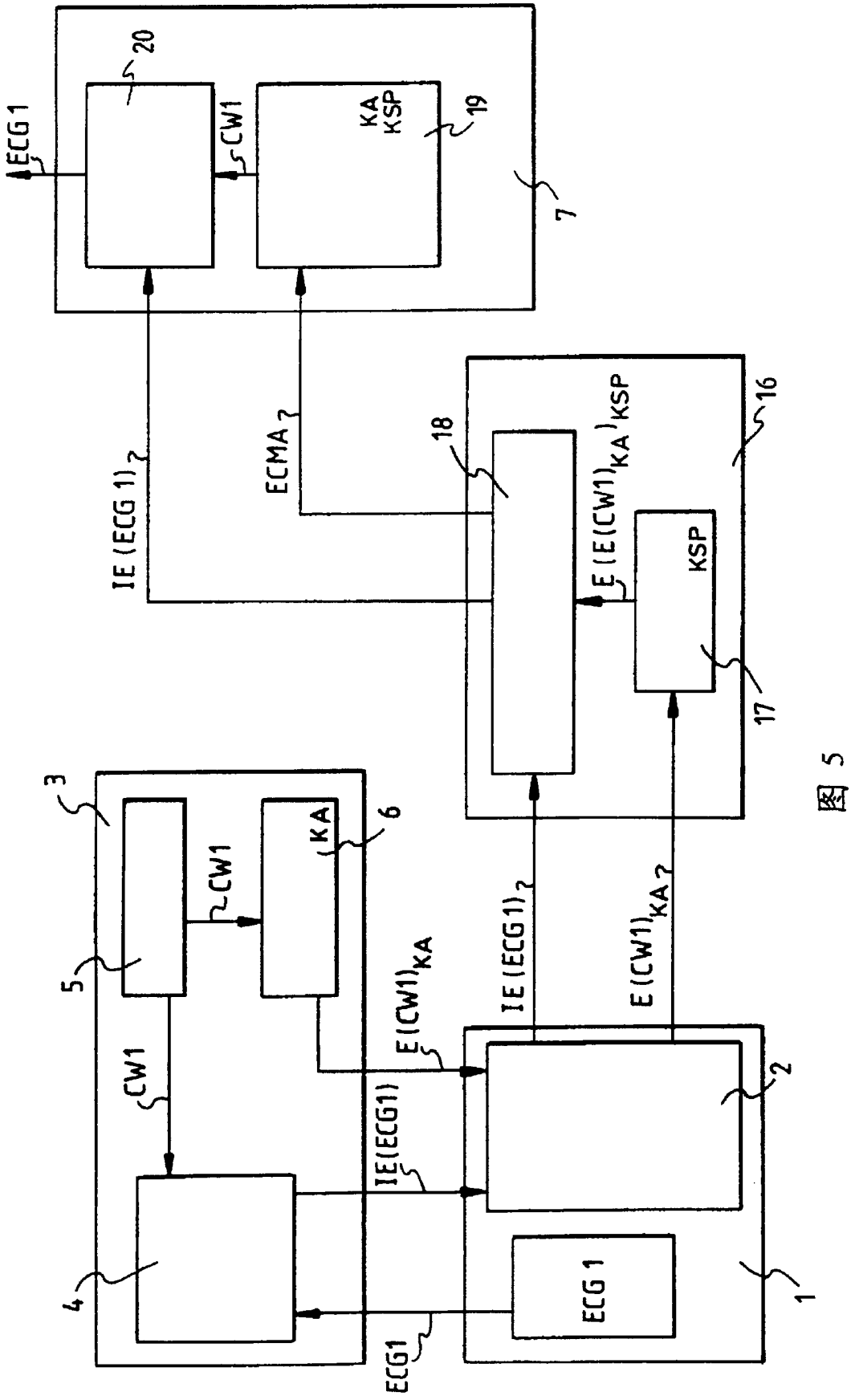

ECG 1
20
CW1
KA
KSP
19
7
IE (ECG 1)₂
ECMA₂
18
E (E(CW1)KA)KSP
16
KSP
17
3
5
CW1
KA
6
CW1
E(CW1)KA
IE(ECG1)
IE (ECG1)₂
E(CW1)KA₂
2
4
ECG 1
1
ECG1

图 5

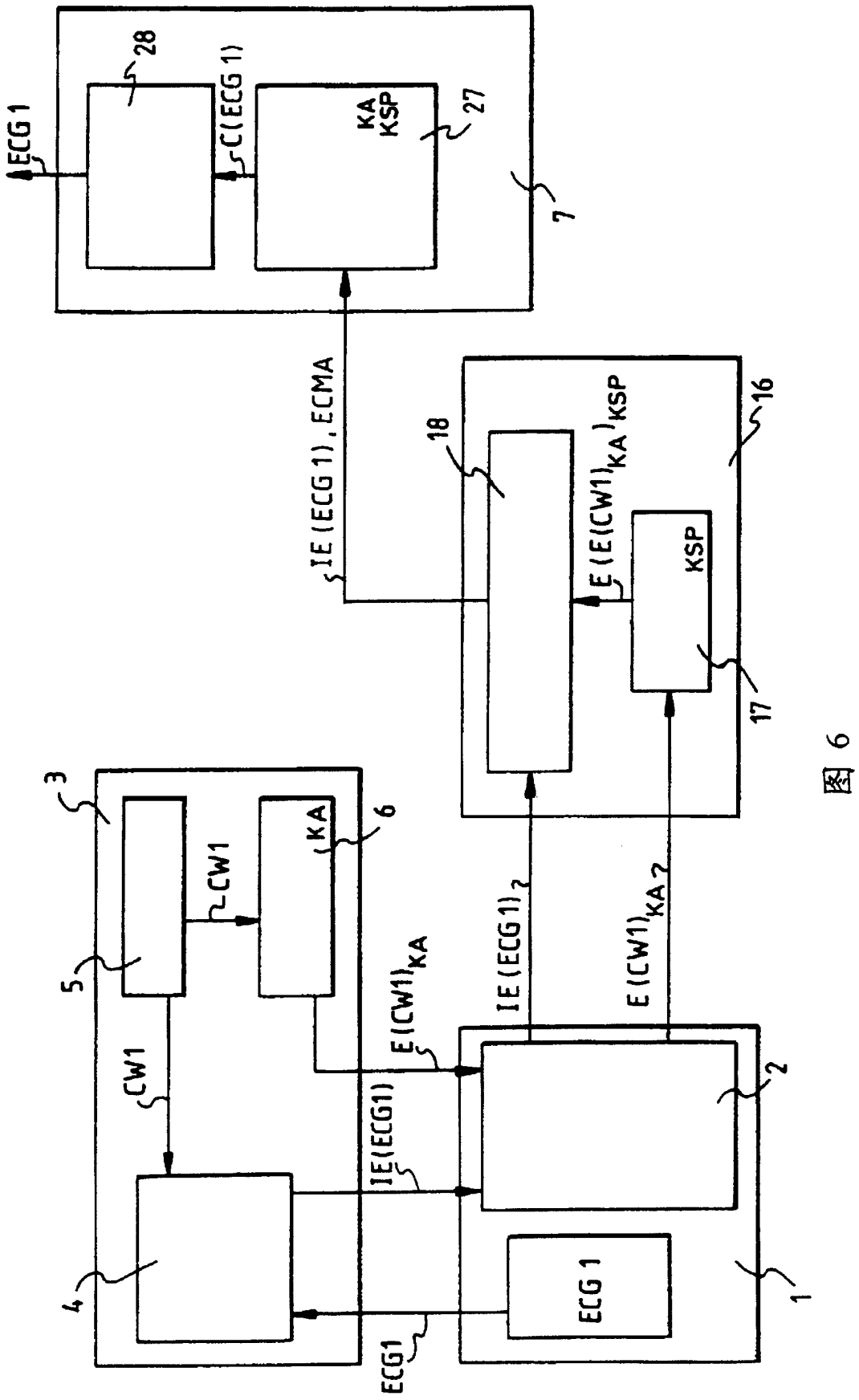

ECG 1
28
C(ECG 1)
KA
KSP
27
7
IE (ECG 1), ECMA
18
E (E(CW1)KA)KSP
KSP
16
17
3
CW1
KA
6
5
CW1
E(CW1)KA
IE (ECG1)2
E (CW1)KA2
IE(ECG1)
2
4
ECG 1
1
ECG1

图 6

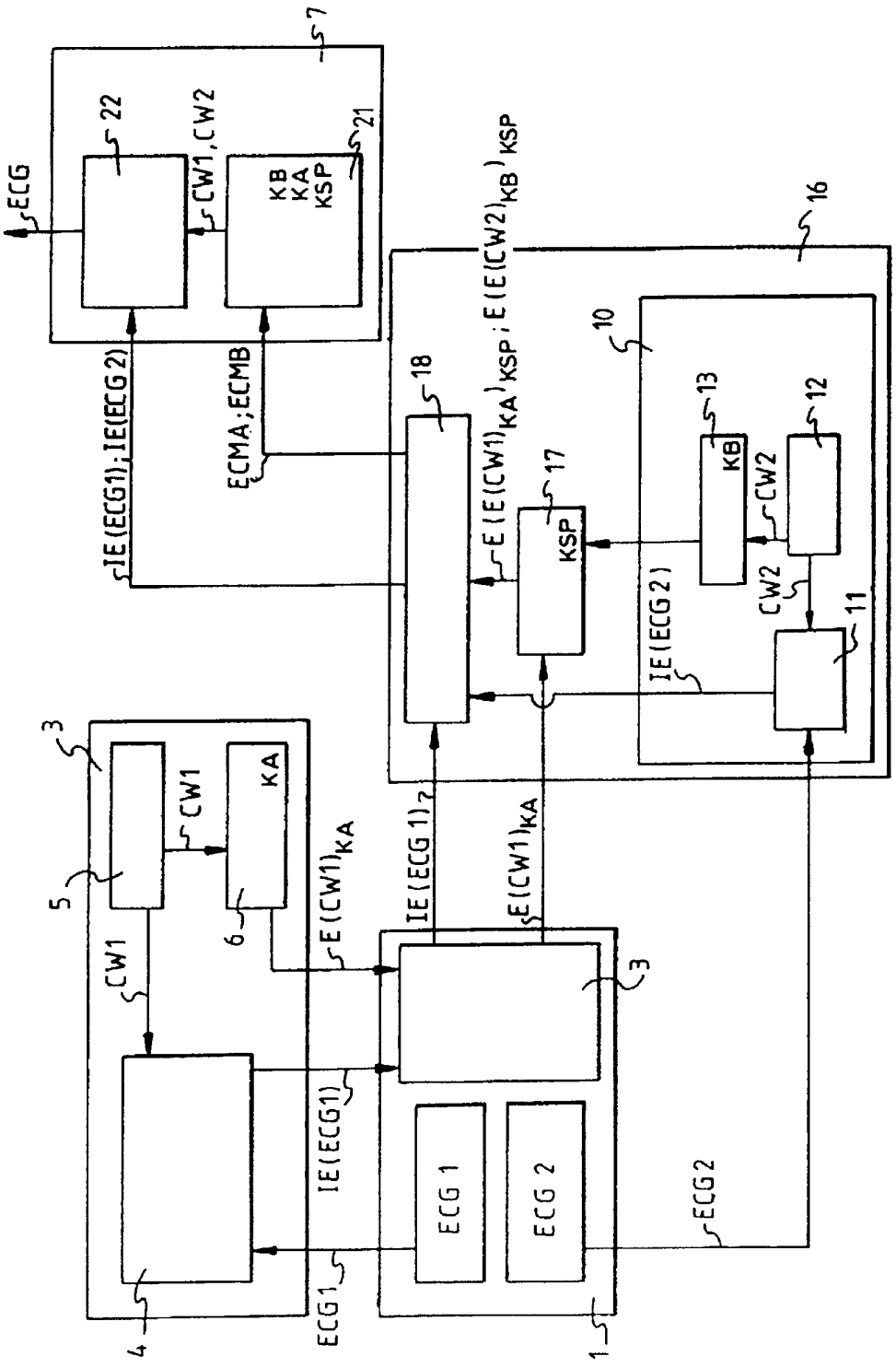

ECG
CW1,CW2
KB
KA
KSP
IE(ECG1);IE(ECG2)
ECMA;ECMB
E(E(CW1)KA'KSP;E(E(CW2)KB'KSP
IE(ECG1)2
E(CW1)KA
CW1
KA
KB
KSP
CW2
IE(ECG2)
IE(ECG1)
ECG1
ECG2
ECG 1
ECG 2

图 7

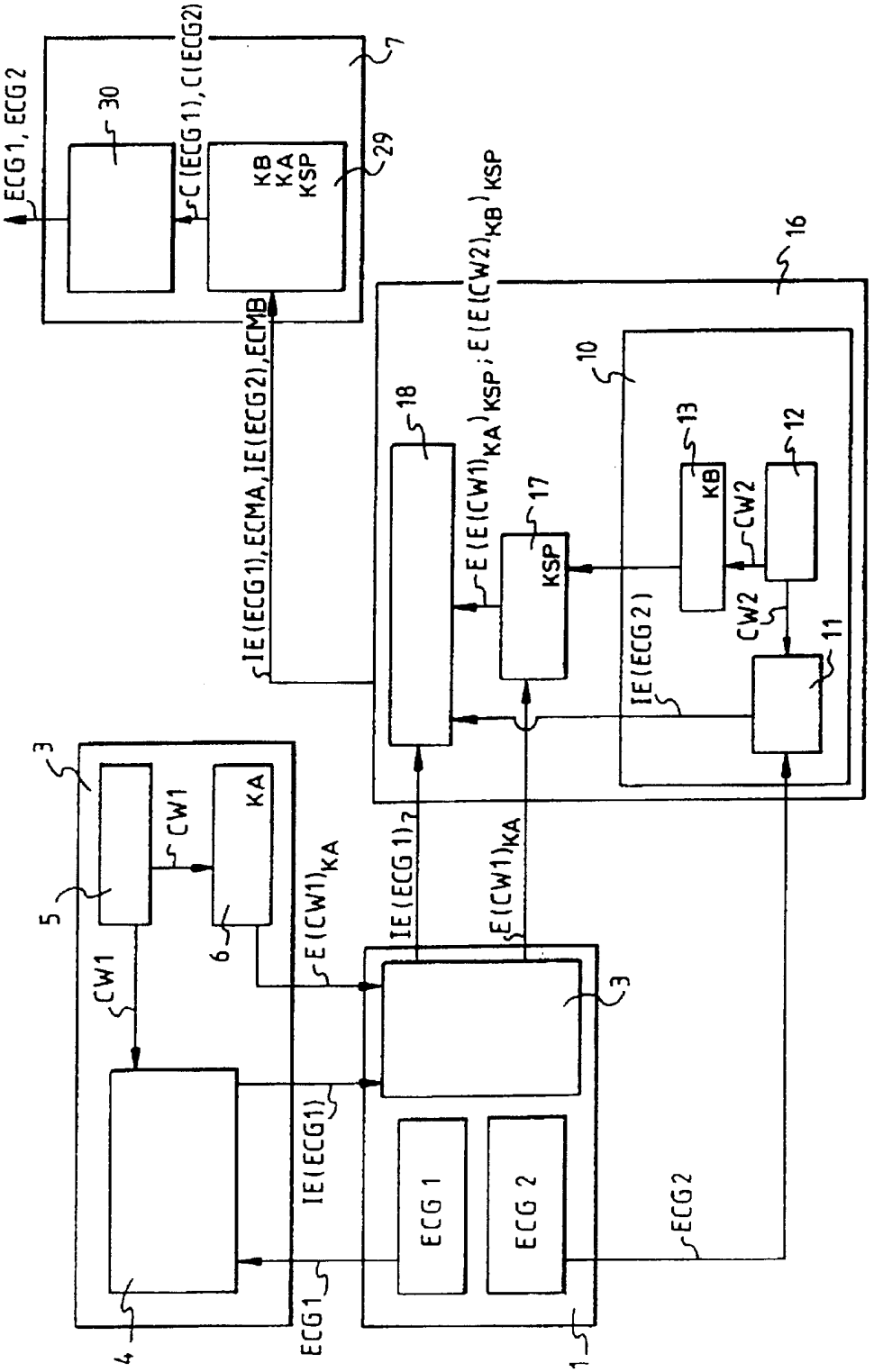

ECG1, ECG2
30
C(ECG1), C(ECG2)
KB
KA
KSP
29
7
IE(ECG1), ECMA, IE(ECG2), ECMB
16
18
E(E(CW1)KA)KSP; E(E(CW2)KB)KSP
10
17
KSP
13
KB
12
CW2
CW2
11
IE(ECG2)
3
5
CW1
KA
6
CW1
E(CW1)KA
IE(ECG1)
E(CW1)KA
IE(ECG1)
ECG 1
ECG 2
ECG2
4
ECG1
1

图 8