(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102481956 A
(43)申请公布日 2012.05.30

(21)申请号 201080038458.6

(22)申请日 2010.08.30

(30)优先权数据
10-2009-0081278 2009.08.31 KR

(85)PCT申请进入国家阶段日
2012.02.29

(86)PCT申请的申请数据
PCT/KR2010/005844 2010.08.30

(87)PCT申请的公布数据
WO2011/025331 KO 2011.03.03

(71)申请人 安纳斯塔锡斯株式会社
地址 韩国首尔市

(72)发明人 李东勋 金允圭 金凡韩

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 臧建明

(51)Int.Cl.
B62D 41/00(2006.01)
G01D 9/00(2006.01)

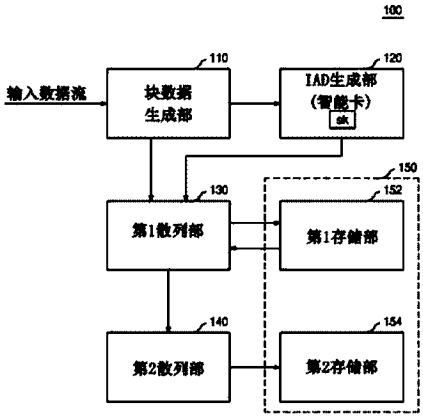
权利要求书 2 页 说明书 8 页 附图 4 页

(54)发明名称

实时车辆数据完整性保障装置和方法及车辆用黑匣子系统

(57)摘要

本发明涉及一种车辆用黑匣子技术，本发明将输入数据流生成块数据，执行基于签名密钥的签名及重叠散列，从而提供实时保障存储于黑匣子的车辆数据完整性的优点。另外，每个车辆用黑匣子拥有具有可靠性的唯一的签名密钥，从而提供支持防止否认功能的优点。而且，通过生成完整性验证数据的固有的算法，提供即使在发生车辆数据的错误的情况下也支持错误恢复功能的优点。



CN 102481956 A

1. 一种实时车辆数据完整性保障装置，其特征在于，包括；

块数据生成部，把关于车辆传感信息的输入数据流分割成预定的大小的块数据；

IAD 生成部，针对所述输入数据流的最初块数据，执行基于签名密钥 (signing key) 的签名，生成初始认证数据 (Initial Authentication Data ;IAD)；

第 1 散列部，依次生成关于分割的各个所述块数据的第 1 散列值，其中，通过将当前块数据的值与关于前一块数据的第 1 散列值相连接进行散列，生成关于所述当前块数据的第 1 散列值；

第 2 散列部，通过对关于所述当前块数据的第 1 散列值进行散列，生成第 2 散列值，将所述第 2 散列值输出为关于所述当前块数据的完整性验证数据；

其中，所述第 1 散列部利用所述 IAD 值作为关于所述最初块数据的第 1 散列值。

2. 根据权利要求 1 所述的实时车辆数据完整性保障装置，其特征在于，

所述 IAD 生成部利用由第三方信任机构 (Third Trust Party) 发放的签名密钥生成所述 IAD。

3. 根据权利要求 2 所述的实时车辆数据完整性保障装置，其特征在于，

所述 IAD 生成部由内置所述签名密钥并保障所述签名密钥的安全性的智能卡 (Smart Card) 构成。

4. 根据权利要求 3 所述的实时车辆数据完整性保障装置，其特征在于，

所述 IAD 生成部包括存储所述签名密钥及生成的所述 IAD 的存储器部。

5. 根据权利要求 1 所述的实时车辆数据完整性保障装置，其特征在于，

所述实时车辆数据完整性保障装置还包括存储由所述第 1 散列部生成的第 1 散列值的第 1 存储部，

所述第 1 散列部利用所述第 1 存储部存储的关于前一块数据的第 1 散列值，生成关于当前块数据的第 1 散列值。

6. 根据权利要求 5 所述的实时车辆数据完整性保障装置，其特征在于，

所述第 1 存储部将所述 IAD 值存储为关于所述最初块数据的第 1 散列值。

7. 根据权利要求 6 所述的实时车辆数据完整性保障装置，其特征在于，

所述第 1 存储部在存储关于所述当前块数据的第 1 散列值的情况下，删除关于所述前一块数据的第 1 散列值。

8. 根据权利要求 1 所述的实时车辆数据完整性保障装置，其特征在于，

所述实时车辆数据完整性保障装置还包括存储关于由所述第 2 散列部输出的各个块数据的完整性验证数据的第 2 存储部。

9. 一种实时车辆数据完整性保障方法，收集及存储车辆传感信息相关车辆数据的车辆用黑匣子实时保障所述车辆数据的完整性，该方法包括；

块数据生成步骤，将关于车辆传感信息的输入数据流分割成预定的大小的块数据；

IAD 生成步骤，针对所述输入数据流的最初块数据，利用签名密钥 (signing key) 进行签名，生成初始认证数据 (Initial Authentication Data ;IAD)；

第 1 散列步骤，依次生成关于所述分割的各个块数据的第 1 散列值，其中，通过将当前块数据的值与关于前一块数据的第 1 散列值相连接进行散列，生成关于所述当前块数据的第 1 散列值；

第 2 散列步骤，通过对关于所述当前块数据的第 1 散列值进行散列，生成第 2 散列值，而且将所述第 2 散列值输出为关于所述当前块数据的完整性验证数据；

其中，所述第 1 散列步骤是利用所述 IAD 值作为关于所述最初块数据的第 1 散列值的步骤。

10. 根据权利要求 9 所述的实时车辆数据完整性保障方法，其特征在于，

所述 IAD 生成步骤是利用由第三方信任机构 (Third Trust Party) 发放的签名密钥生成所述 IAD 的步骤。

11. 根据权利要求 9 所述的实时车辆数据完整性保障方法，其特征在于，

所述实时车辆数据完整性保障方法还包括存储由所述第 1 散列步骤生成的第 1 散列值的第 1 存储步骤，

所述第 1 散列步骤是利用由所述第 1 存储步骤存储的关于前一块数据的第 1 散列值，生成关于当前块数据的第 1 散列值的步骤。

12. 根据权利要求 11 所述的实时车辆数据完整性保障方法，其特征在于，

所述第 1 存储步骤是把所述 IAD 值存储为关于所述最初块数据的第 1 散列值的步骤。

13. 根据权利要求 12 所述的实时车辆数据完整性保障方法，其特征在于，

所述第 1 存储步骤是在存储关于所述当前块数据的第 1 散列值的情况下，删除关于所述前一块数据的第 1 散列值的步骤。

14. 根据权利要求 9 所述的实时车辆数据完整性保障方法，其特征在于，

所述实时车辆数据完整性保障方法还包括存储关于由所述第 2 散列步骤输出的各个块数据的完整性验证数据的第 2 存储步骤。

15. 一种计算机可判读记录介质，记录了以计算机运行权利要求 9 至 14 项中任意一项的方法所需的程序。

实时车辆数据完整性保障装置和方法及车辆用黑匣子系统

技术领域

[0001] 本发明涉及一种车辆用黑匣子技术，更详细地说，涉及不仅保障实时存储于黑匣子的车辆数据的完整性，而且支持防止否认及错误恢复功能的车辆数据完整性保障装置及方法和利用其的车辆用黑匣子系统。

背景技术

[0002] 本来，所谓黑匣子 (Black Box) 是指飞行记录装置 (Flight Data Recorder ;FDR) 乃至飞行影像存储装置 (Airborne Video Recorder ;AVR)。这种黑匣子记录飞行中飞机的高度、温度、运行状态、驾驶室内部声音、与控制塔的通信内容等，用于在发生飞机事故时查明事故原因、再现事故当时情况的目的。

[0003] 但是，由于最近汽车普遍率急剧增高，随之而来的汽车事故率也急剧增加，因此，对车辆用黑匣子 (Vehicle Black Box 或 Event Data Recorder) 的关注和研究、开发呈现迅速增加的趋势。

[0004] 实际上，市场上的车辆用黑匣子年销售业绩 2008 年约为 66000 台 (约 120 亿韩元)，2009 年今年预计将增加到约 10 万台 (约 200 亿韩元) 以上。另外，在韩国，建设交通部、技术标准院、远程自动技术协会正在制定车辆用黑匣子相关标准，预计以商业用车辆为中心实现车辆用黑匣子安装义务化的法案将于 2011 年立法。

[0005] 这种趋势是世界性的，例如就美国而言，联邦交通部 (DOT ;Depart of Transportation) 2004 年发布黑匣子标准案，高速公路安全协会 (NHTSA ;National Highway Traffic Safety Administration) 发布推荐自 2008 年 9 月起在本国进口轻型汽车上加装车辆用黑匣子的劝告案，美国汽车工程师协会 (SAE ;Society of Automotive Engineers) 和美国电气与电子工程师协会 (IEEE ;Institute of Electrical and Electronics Engineers) 发布了车辆用黑匣子标准案。另外，就欧洲而言，联合国欧洲经济委员会 (UNECE ;United Nations Economic Commission for Europe) 正在作为强制条款的相互进出口限制中制订车辆用黑匣子标准化工作，欧盟 (EU ;European Union) 确定了自 2009 年起要求对 EU 成员国内所有车辆加装黑匣子的法案。另外，就日本而言，自 2008 年起开始对一部分车型义务安装黑匣子，就中国而言，2008 年已经实行所有车辆义务安装数字行驶记录装置。

[0006] 随着这种世界性趋势，对黑匣子中存储的数据的安全问题的关心也越来越高。因为黑匣子中存储的数据如果能够被黑客轻易伪造乃至变造，那么，由于对数据歪曲的忧虑，造成数据可靠性下降，无法承认法律证据效力等，无法达成黑匣子技术的目的。

[0007] 但是，原有的车辆用黑匣子技术只将重点放在收集、存储车辆的内部、外部传感数据，或通过黑匣子中存储的数据再现事故情况。即，原有技术存在面对黑客对黑匣子数据的伪造、变造非常薄弱的问题。

[0008] 特别是就黑匣子中存储的车辆数据而言，由于实时收集及存储的特性，为防止车辆数据的伪造、变造，要求实时保障数据完整性 (Data Integrity) 的技术。但是，原有技术

存在尚未提出能够实时保障车辆数据完整性的解决方案的问题。

[0009] 而且，原有技术存在无法提供关于黑匣子中存储的数据的防止否认(Non-repudiation)、错误恢复(Error Recovery)功能等问题。

发明内容

[0010] 技术问题

[0011] 本发明要解决的第一技术课题是提供一种不仅实时保障存储于黑匣子中的车辆数据的完整性，而且，支持防止否认及错误恢复功能的车辆数据完整性保障装置。

[0012] 本发明要解决的第二技术课题是提供一种不仅实时保障存储于黑匣子中的车辆数据的完整性，而且，支持防止否认及错误恢复功能的车辆数据完整性保障方法。

[0013] 本发明要解决的第三技术课题是提供一种利用了所述车辆数据完整性保障装置及方法的车辆用黑匣子系统。

[0014] 技术方案

[0015] 为解决如上所述的第一技术课题，本发明提供一种实时车辆数据完整性保障装置，包括：块数据生成部，把关于车辆传感信息的输入数据流分割成预定的大小的块数据；IAD 生成部，针对所述输入数据流的最初块数据，执行基于签名密钥(signing key)的签名，生成初始认证数据(Initial Authentication Data；IAD)；第 1 散列部，依次生成关于分割的各个所述块数据的第 1 散列值，其中，通过将当前块数据的值与关于前一块数据的第 1 散列值相连接进行散列，生成关于所述当前块数据的第 1 散列值；第 2 散列部，通过对关于所述当前块数据的第 1 散列值进行散列，生成第 2 散列值，将所述第 2 散列值输出为关于所述当前块数据的完整性验证数据。其中，所述第 1 散列部利用所述 IAD 值作为关于所述最初块数据的第 1 散列值。

[0016] 根据本发明一实施例，所述 IAD 生成部利用由第三方信任机构(Third Trust Party)发放的签名密钥生成所述 IAD。

[0017] 根据本发明一实施例，所述 IAD 生成部由内置所述签名密钥并保障所述签名密钥的安全性的智能卡(Smart Card)构成。

[0018] 根据本发明一实施例，所述 IAD 生成部包括存储所述签名密钥及生成的所述 IAD 的存储器部。

[0019] 根据本发明一实施例，所述实时车辆数据完整性保障装置还包括存储由所述第 1 散列部生成的第 1 散列值的第 1 存储部，所述第 1 散列部利用所述第 1 存储部存储的关于前一块数据的第 1 散列值，生成关于当前块数据的第 1 散列值。

[0020] 根据本发明一实施例，所述第 1 存储部将所述 IAD 值存储为关于所述最初块数据的第 1 散列值。

[0021] 根据本发明的一实施例，所述第 1 存储部在存储关于所述当前块数据的第 1 散列值的情况下，删除关于所述前一块数据的第 1 散列值。

[0022] 根据本发明的一实施例，所述实时车辆数据完整性保障装置还包括存储关于由所述第 2 散列部输出的各个块数据的完整性验证数据的第 2 存储部。

[0023] 为解决如上所述的第二技术课题，本发明提供一种实时车辆数据完整性保障方法，收集及存储车辆传感信息相关车辆数据的车辆用黑匣子实时保障所述车辆数据的完整

性，该方法包括 ；块数据生成步骤，将关于车辆传感信息的输入数据流分割成预定的大小的块数据 ；IAD 生成步骤，针对所述输入数据流的最初块数据，利用签名密钥进行签名，生成初始认证数据 (IAD) ；第 1 散列步骤，依次生成关于所述分割的各个块数据的第 1 散列值，其中，通过将当前块数据的值与关于前一块数据的第 1 散列值相连接进行散列，生成关于所述当前块数据的第 1 散列值 ；第 2 散列步骤，通过对关于所述当前块数据的第 1 散列值进行散列，生成第 2 散列值，而且将所述第 2 散列值输出为关于所述当前块数据的完整性验证数据。其中，所述第 1 散列步骤是利用所述 IAD 值作为关于所述最初块数据的第 1 散列值的步骤。

[0024] 为解决如上所述的第三技术课题，本发明提供一种收集及存储关于车辆的传感信息的车辆数据的车辆用黑匣子系统，包括 ：块数据生成部，把关于车辆传感信息的输入数据流分割成预定的大小的块数据 ；IAD 生成部，针对所述输入数据流的最初块数据，执行基于签名密钥的签名，生成初始认证数据 (IAD) ；第 1 散列部，依次生成关于所述分割的各个块数据的第 1 散列值，而且是通过将当前块数据的值与关于前一块数据的第 1 散列值相连接进行散列，生成关于所述当前块数据的第 1 散列值 ；第 2 散列部，通过对关于所述当前块数据的第 1 散列值进行散列，生成第 2 散列值，将所述第 2 散列值输出为关于所述当前块数据的完整性验证数据。其中，所述第 1 散列部利用所述 IAD 值作为关于所述最初块数据的第 1 散列值。

[0025] 根据本发明一个实施例，所述 IAD 生成部由内置由第三方信任机构发放的签名密钥并保障所述签名密钥的安全性的智能卡体现。

[0026] 根据本发明一实施例，所述车辆用黑匣子系统还包括存储关于由所述第 2 散列部输出的各个块数据的完整性验证数据的数据存储部。

[0027] 根据本发明一实施例，所述数据存储部还存储对应于所述完整性验证数据的所述块数据。

[0028] 发明效果

[0029] 本发明将输入数据流生成块数据，执行基于签名密钥的签名及重叠式散列，从而提供实时保障黑匣子中存储的车辆数据完整性的优点。

[0030] 另外，每个车辆用黑匣子拥有具有可靠性的唯一的签名密钥，从而提供支持防止否认功能的优点。

[0031] 而且，通过生成完整性验证数据的固有的算法，提供即使在车辆数据发生错误的情况下也支持错误恢复功能的优点。

附图说明

[0032] 图 1 为显示根据本发明一实施例的实时车辆数据完整性保障装置的框图 ；

[0033] 图 2 为显示根据本发明一实施例的实时车辆数据完整性保障方法的流程图 ；

[0034] 图 3 为显示根据本发明一实施例生成的块数据及完整性验证数据的附图 ；

[0035] 图 4 为显示根据本发明一个实施例生成的演算值的附图 ；

[0036] 图 5 为显示执行一次散列并生成完整性验证数据情况下的演算值的附图 ；

[0037] 图 6 为显示根据本发明一个实施例的车辆用黑匣子系统的框图。

[0038] 最佳实施方式

[0039] 本发明包括：块数据生成部，把关于车辆传感信息的输入数据流分割成预定的大小的块数据；IAD 生成部，针对所述输入数据流的最初块数据，执行基于签名密钥 (signing key) 的签名，生成初始认证数据 (Initial Authentication Data；IAD)；第 1 散列部，依次生成关于所述分割的各个块数据的第 1 散列值，而且是通过将当前块数据的值与关于前一块数据的第 1 散列值相连接进行散列，生成关于所述当前块数据的第 1 散列值；第 2 散列部，通过对关于所述当前块数据的第 1 散列值进行散列，生成第 2 散列值，将所述第 2 散列值输出为关于所述当前块数据的完整性验证数据；而且，所述第 1 散列部利用所述 IAD 值作为关于所述最初块数据的第 1 散列值。

[0040] 本发明包括：块数据生成步骤，将关于车辆传感信息的输入数据流分割成预定的大小的块数据；IAD 生成步骤，针对所述输入数据流的最初块数据，利用签名密钥进行签名，生成初始认证数据 IAD；第 1 散列步骤，依次生成关于所述分割的各个块数据的第 1 散列值，而且是通过将当前块数据的值与关于前一块数据的第 1 散列值相连接进行散列，生成关于所述当前块数据的第 1 散列值；第 2 散列步骤，通过对所述关于当前块数据的第 1 散列值进行散列，生成第 2 散列值，将所述第 2 散列值输出为关于所述当前块数据的完整性验证数据；而且，所述第 1 散列步骤是利用所述 IAD 值作为关于所述最初块数据的第 1 散列值的步骤。

具体实施方式

[0041] 下面，为了明确本发明的技术课题的技术方案，参照附图对本发明的优选实施例进行详细说明。不过，在说明本发明的过程中，当对相关公知技术的说明反而会混淆本发明的要旨时，省略其相关说明。另外，后述的术语是考虑到在本发明中的功能而定义的术语，可能会因使用者、运用者等的意图或惯例等而异。因此，其定义应以本说明书中的全面内容为基础加以决定。

[0042] 图 1 为显示根据本发明一实施例的实时车辆数据完整性保障装置的框图。

[0043] 图 2 为显示根据本发明一实施例的实时车辆数据完整性保障方法的流程图。

[0044] 如图 1 及图 2 所示，所述实时车辆数据完整性保障装置 100 包括块数据生成部 110、IAD 生成部 120、第 1 散列部 130 及第 2 散列部 140，还可以包括数据存储部 150。

[0045] 首先，在步骤 S210 中，所述块数据生成部 110 将关于车辆传感信息的输入数据流分割成预定的大小的块数据。这是基于为了实时处理关于车辆传感信息的输入数据流的技术考虑。

[0046] 然后，在步骤 S220 中，所述 IAD 生成部 120 针对所述输入数据流的最初块数据，利用签名密钥 (signing key；sk) 执行签名，生成初始认证数据 (Initial Authentication Data；IAD)。在一个实施例中，所述 IAD 生成部 120 可以由内置所述签名密钥 sk 并保障所述签名密钥 sk 的安全性的智能卡 (Smart Card) 体现。这种智能卡埋设有搭载了 IC 存储器和中央处理装置 CPU 的半导体芯片，因此具有加密处理、接入对象的认证、记忆数据的管理等安全功能出色、稳定性高、不能伪造的特征。此时，所述智能卡 120 可在购买具备所述完整性保障装置 100 的黑匣子时或车辆登记时，从第三方信任机构 (TTP；Third Trust Party) 获得发放，例如从政府机关获得发放。所述签名密钥 sk 唯一地分配给所述完整性保障装置 100 乃至具备其的黑匣子，发放所述智能卡 120 时，可一同从所述第三方信任机构获得发

放。在一个实施例中，在所述完整性保障装置100乃至具备其的黑匣子中具备通信模块（未图示），可以从所述第三方信任机构获得发放所述签名密钥sk。另外，所述IAD生成部120包括存储所述发放的签名密钥sk及所述生成的IAD的具有安全性的存储器部（例如，智能卡的IC存储器）。

[0047] 然后，在步骤S230至步骤S260中，所述第1散列部130依次生成关于所述分割的各个块数据的第1散列值，而且是通过将当前块数据的值与关于前一块数据的第1散列值相连接进行散列，dj生成关于所述当前块数据的第1散列值。为此，所述完整性保障装置100还可以包括存储由所述第1散列部130生成的第1散列值的第1存储部152。

[0048] 需要注意的是，所述第1散列部130在输入了所述最初块数据的情况下，将用由所述IAD生成部120生成的所述IAD的值代替用作关于所述最初块数据的第1散列值。其理由是因为，就所述最初块数据而言，不存在前一块数据。

[0049] 更具体地涉及，在步骤S230中，所述第1散列部130在输入了所述最初块数据的情况下，在步骤S240中，把所述IAD值作为关于所述最初块数据的第1散列值存储于所述第1存储部152。而且，在步骤S230中，所述第1散列部130在输入了第二个之后的块数据的情况下，在步骤S250中通过将当前输入的块数据值与关于前一块数据的第1散列值相连接(concatenation)进行散列(hashing)，生成关于所述当前块数据的第1散列值。

[0050] 而且，所述第1散列部130将关于所述当前块数据的第1散列值存储于所述第1存储部152，在生成关于下一块数据的第1散列值时，用作关于所述前一块数据的第1散列值。此时，在步骤S230中，所述第1存储部152在存储了关于当前块数据的第1散列值的情况下，删除所述第1存储部152中存储的关于前一块数据的第1散列值S260。例如，在生成了关于第二块数据的第1散列值或将关于第二块数据的第1散列值存储于所述第1存储部152的情况下，把关于前一块数据，即，把作为关于最初块数据的第1散列值的所述IAD值从所述第1存储部152中删除。另外，在生成了关于第三块数据的第1散列值或将关于第三块数据的第1散列值存储于所述第1存储部152的情况下，把关于第二块数据的第1散列值从所述第1存储部152中删除。由于诸如所述第1存储部152的存储器或数据存储空间一般容易被黑客访问，因此所述作法是基于为了使所述IAD等重要信息不会不必要地泄漏的技术考虑。

[0051] 然后，在步骤S270中，所述第2散列部140通过对关于所述当前块数据的第1散列值再次进行散列，生成第2散列值，将所述第2散列值输出为关于所述当前块数据的完整性验证数据。此时，在步骤S280中，所述完整性保障装置100还可以包括第2存储部154，可以存储关于由所述第2散列部140输出的各个块数据的完整性验证数据。

[0052] 所述完整性保障装置100在输入了下一块数据的情况S290下，反复所述步骤S250至所述步骤S280。

[0053] 在图1中，所述第1存储部152及所述第2存储部154独立体现，根据实施例，也可以由单一的存储部150体现。

[0054] 在图3中，显示了根据本发明一个实施例生成的块数据及完整性验证数据。

[0055] 如图3所示，本发明将关于车辆传感信息的输入数据流300分割成预定大小的块数据(Block Data ;BD_n)，生成对应于所述分割的各个块数据BD_n的附加数据(Additional Data ;AD_n)310，即，完整性验证数据AD_n。

[0056] 在图 4 中，显示了根据本发明的一个实施例生成的演算值。

[0057] 如图 4 所示，根据本发明的一个实施例生成的所述完整性验证数据 AD_n 由如下步骤生成。

[0058] 1、最初块数据 BD_1 通过所述 IAD 生成部（例如，智能卡 120）的输入而进入，被利用所述签名密钥 sk 签名并输出。所述签名值 $Sign_{sk}(BD_1)$ 定义为 IAD(Initial Authentication Data)。

[0059] 2、IAD 存储于所述 IAD 生成部 120 的具有安全性的存储器。

[0060] 3、作为关于所述 BD_1 的第 1 散列值 h_1，利用所述 IAD 值，作为关于所述 BD_1 的完整性验证数据 AD_1，存储关于所述 BD_1 的第 2 散列值 h_1'，即，对所述 IAD 进行散列的值 h(IAD)。

[0061] 4、作为关于第二块数据 BD_2 的第 1 散列值 h_2，存储将所述 IAD 与 BD_2 相连接进行散列的值 $h(IAD||BD_2)$。

[0062] 5、所述 IAD 在所述 h_2 生成后，被从存储部删除。

[0063] 6、作为关于所述 BD_2 的第 2 散列值 h_2'，存储对所述 h_2 进行散列的值 $h(h_2)$。

[0064] 7、即，作为关于所述 BD_2 的完整性验证数据 AD_2，存储所述 h_2'。

[0065] 8、作为关于第三块数据 BD_3 的第 1 散列值 h_3，存储将所述 h_2 及 BD_3 相连接进行散列的值 $h(h_2||BD_3)$。

[0066] 9、所述 h_2 在所述 h_3 生成后，被从存储部删除。

[0067] 10、作为关于所述 BD_3 的第 2 散列值 h_3'，存储对所述 h_3 进行散列的值 $h(h_3)$。

[0068] 11、即，作为关于所述 BD_3 的完整性验证数据 AD_3，存储所述 h_3'。

[0069] 12、利用所述 8 至 11 的过程，继续生成及存储关于块数据 BD_n 的完整性验证数据 AD_n。

[0070] 在本发明中，为生成各个完整性验证数据 AD_n 而执行两次散列，这是基于提供更安全、高效的实时数据完整性保障技术所需的技术考虑。

[0071] 在图 5 中，显示了执行一次散列并生成完整性验证数据情况下的演算值。

[0072] 如图 5 所示，在只通过一次散列生成完整性验证数据 AD_n 的情况下，例如，在将 h_2 存储为关于第二块数据 BD_2 的完整性验证数据 AD_2 的情况下，黑客虽然无法生成至所述 AD_2，但从关于第三块数据 BD_3 的完整性验证数据 AD_3 起，前一块数据的第 1 散列值 h_{n-1} 暴露，例如，h_2 暴露，发生使黑客可以生成的问题。

[0073] 另一方面，如果将所述 IAD 级联于所述 BD_2 之后的块数据 BD_n，从逻辑上，只通过一次散列也可以保障数据完整性。但是，在这种情况下，就产生了在存储部的存储器上继续暴露所述 IAD 的结果，发生使黑客可以仿造乃至变造 AD_n 值的问题。

[0074] 因此，本发明为防止所述问题，在生成各个完整性验证数据 AD_n 方面，通过执行两次散列，保障数据完整性。其中，需要注意的是，在实际体现方面，散列函数可以高速演算，几乎不影响演算性能。

[0075] 在图 6 中，以框图显示了本发明一个实施例的车辆用黑匣子系统。

[0076] 如图 6 所示，所述车辆用黑匣子系统 600 可以包括传感车辆内部和外部的多种信息的传感器部 610 以及收集并存储由所述传感器部 610 传感的信息的黑匣子 630。

[0077] 所述传感器部 610 可以包括用于传感车辆内部和外部的多种信息的各种传感器。例如，可以包括拍摄车辆周围影像的影像传感器 612、记录车辆内部 / 外部声音的音频传感

器 614、感知车辆行驶速度变化 / 转动等的加速度传感器 616 及角速度传感器 618、感知车辆是否碰撞的冲击传感器 620 等。

[0078] 所述黑匣子 630 可以包括把由所述传感器部 610 感知的传感信号转换为数字形态的数据流的输入接口 632、实时保障输入数据的完整性的完整性保障部 100 以及存储数据的数据存储部 634。

[0079] 所述完整性保障部 100 的详细构成要素及动作参照所述关于本发明的实时车辆数据完整性保障装置 100 的说明。

[0080] 如上所述，所述完整性保障部 100 的所述 IAD 生成部 120 可以由内置由第三方信任机构 (TTP) 发放的签名密钥 sk 并保障所述签名密钥 sk 的安全性的智能卡 (Smart Card) 构成。此时，由所述智能卡 120 生成的签名值 IAD 只能从所述完整性保障部 100 内获得，即使是车辆持有人，也无法随意获得。因此，只有发放所述签名密钥 sk 的所述第三方信任机构 (TTP) 才拥有对应于所述签名密钥 sk 的签名验证用公共密钥 (pk)，只有所述第三方信任机构 (TTP) 才能执行数据完整性验证。例如，所述第三方信任机构 (TTP) 从所述智能卡导出所述 IAD 值后，利用对应于所述签名密钥 sk 的所述公共密钥 (pk) 执行签名验证，所述签名验证通过后，按照与所述签名所述完整性验证数据 AD_n 生成过程相同的顺序，执行对所述块数据 BD_n 的散列，通过比较生成的值 AD_n' 是否与所述完整性验证数据 AD_n 的值一致，可以验证生成的数据的完整性。

[0081] 所述数据存储部 634 将所述块数据 BD_n 存储为对应于所述完整性验证数据 AD_n 的源数据。在一个实施例中，所述完整性保障部 100 的所述第 1 存储部 152、所述第 2 存储部 154 或所述第 1 及第 2 存储部 152，154 两者可以整合于所述数据存储部 634，由单一的存储部体现。另外，在一个实施例中，考虑所述数据存储部 634 的存储容量，可以利用先入先出方式限制所述数据存储部 634 中存储的数据的量。即，可以在删除久远的存储数据的同时，存储新输入的数据。此时，所述数据存储部 634 在由所述传感器部 610 感知的传感信息表示事故、被盗、故障等车辆危急情况的情况下，可以体现为，在相应情况下存储的数据与存储时刻无关地一直保存。

[0082] 另外，在一个实施例中，所述完整性保障部 100 可以在控制车辆用黑匣子的黑匣子的电子控制装置 (Electronic Control Unit ;ECU，未图示) 上，利用系统芯片 (system on chip) 技术加以体现，使所述黑匣子的电子控制装置能够实时保障所述车辆用黑匣子中存储的车辆数据的完整性。如果利用单一的微处理器芯片体现本发明，具有可以减小各种系统的大小、可以简化组装过程、可以节省制造费用等优点。

[0083] 另外，根据实施例，本发明可以在可由计算机判读的记录介质中，以计算机可以读取的程序代码体现。在本发明通过软件运行时，本发明的构成要素是运行所需作业的代码段。另外，程序或代码段可以存储于计算机的处理器可判读介质，或者通过传输介质或通信网，利用与载波结合的计算机数据信号进行传输。

[0084] 计算机可判读记录介质包括存储可由计算机系统读取的数据的所有种类的记录装置。例如，计算机可判读记录介质可以包括 ROM、RAM、CD-ROM、磁带、软盘、光数据存储装置等。另外，计算机可判读记录介质可以分布于通过网络连接的计算机系统，以分布方式存储、运行计算机可读取的代码。

[0085] 下面分析本发明的显著效果。

[0086] 本发明保障关于车辆用黑匣子中存储的数据的实时完整性。即，在图 4 中，所述 AD_1 是对利用所述签名密钥 sk 生成的签名值 IAD 进行散列的值，因此，黑客无法获知所述智能卡 120 中存储的所述签名密钥 sk 及所述 IAD，无法生成所述 AD_1。所述 IAD 值只有第三方信任机构 (TTP) 可以导出。另外，由于无法生成所述 IAD，所以无法生成所述 h_2 及 h_2'，这意味着 AD_2 也无法生成。另外，由于无法生成所述 h_2，所以无法生成 h_3 及 h_3'，这意味着 AD_3 也无法生成。同理，使黑客无法生成以后的 AD_n。另外，由于散列函数的特性，因而无法获知作为 h_n' 的预映射 (Pre-image) 值的 h_n 值，所以也不能伪造中间值。

[0087] 另外，本发明由于使各个黑匣子系统拥有唯一的签名密钥，因而支持防止否认功能。

[0088] 另外，本发明在所述完整性验证数据 AD_n 存储后，即使在因外部冲击、电信号错误、传输障碍等发生错误的情况下，也支持错误恢复功能。即，即使在 AD_{n-1} 值中发生错误而无法验证 AD_n 的完整性的情况下，也可以获知 IAD 值，因此，其余所有块的完整性可以验证。

[0089] 而且，本发明在所述块数据 BD_n 存储后，即使在发生错误的情况下，如果输入数据流是关于视频数据的数据流，则支持部分的错误恢复。即，应对当在特定块数据 BD_n 中发生错误时，无法进行与此后块数据相关的完整性验证的情况，针对所述视频数据的每个 I- 数据帧 (Intra frame) 进行签名。如此生成的签名值独立于完整性验证数据 AD_n 进行存储。所述 I- 数据帧之后可以进行译码，转换为图片，所以，即使在所述视频数据中发生错误，也可以针对每秒的停止影像图片验证完整性。

[0090] 如上所述，本发明提供不仅实时保障存储于黑匣子的车辆数据的完整性，而且支持防止否认及错误恢复功能的优点。

[0091] 以上参照实施例，对本发明进行了说明。但是，所属技术领域的技术人员可以理解 :在不脱离本发明本质性的技术思想的范围内，本发明可以由变形的形态体现。因此，公开的实施例并非用于限定，而是应从详细的角度加以考虑。即，本发明的真正的技术范围出现于附带的所述权利要求书中，在与之均等的范围内的所有差异应解释为包含于本发明。

[0092] 工业应用性

[0093] 本发明可由车辆用黑匣子的一个模块体现。

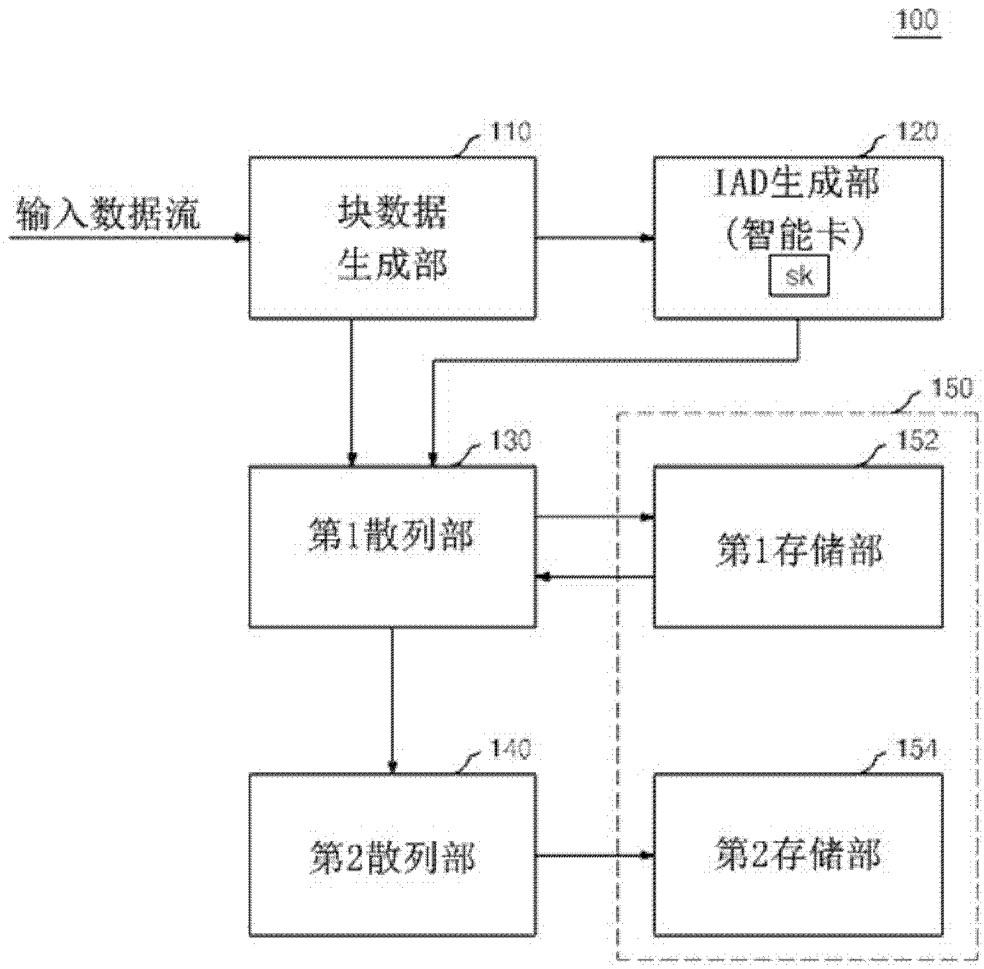

100
110
120
输入数据流
块数据
生成部
IAD生成部
(智能卡)
sk
150
130
152
第1散列部
第1存储部
140
154
第2散列部
第2存储部

图 1

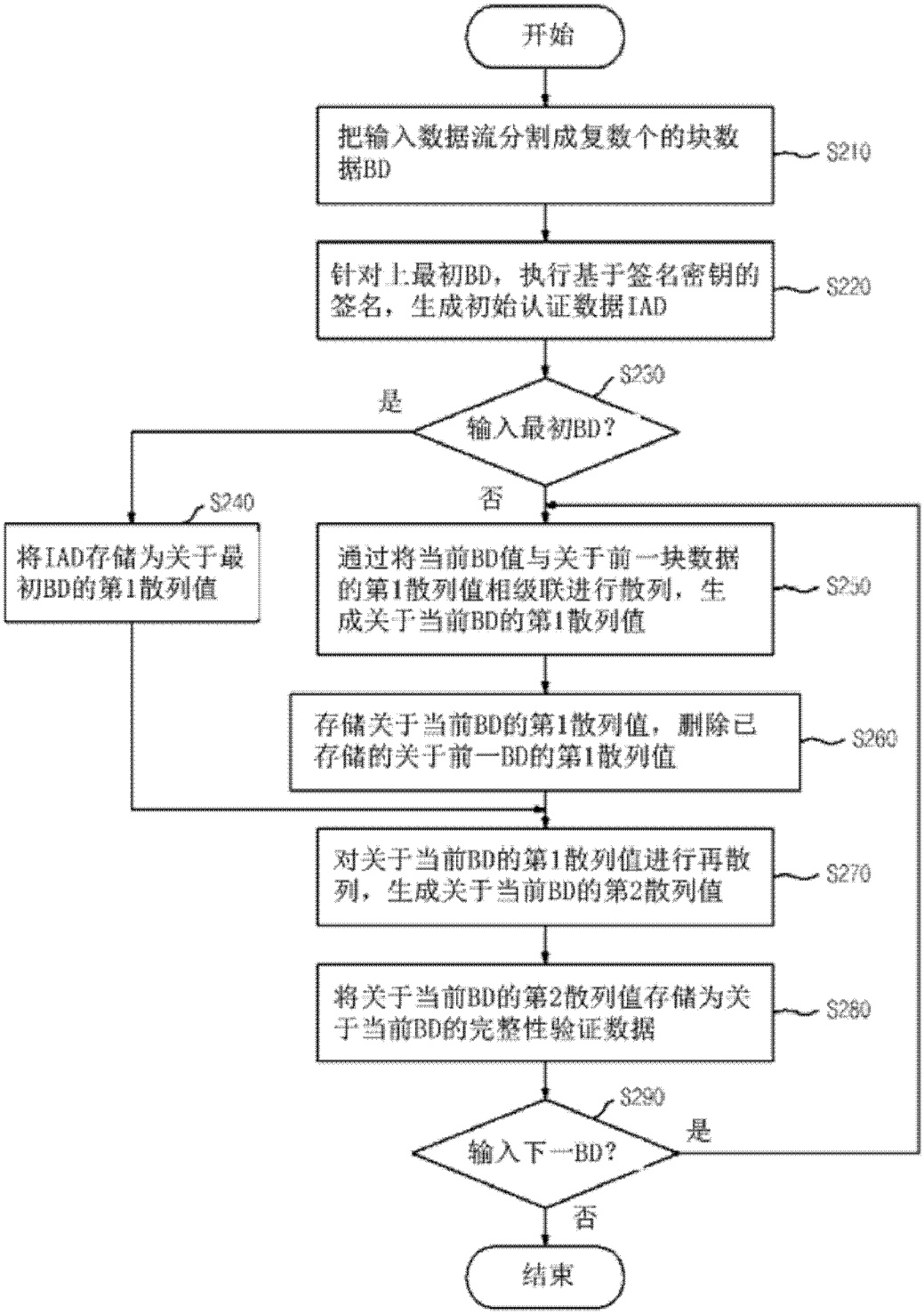

开始
把输入数据流分割成复数个的块数据BD
S210
针对上最初BD，执行基于签名密钥的签名，生成初始认证数据IAD
S220
S230
输入最初BD?
是
否
S240
将IAD存储为关于最初BD的第1散列值
通过将当前BD值与关于前一块数据的第1散列值相级联进行散列，生成关于当前BD的第1散列值
S250
存储关于当前BD的第1散列值，删除已存储的关于前一BD的第1散列值
S260
对关于当前BD的第1散列值进行再散列，生成关于当前BD的第2散列值
S270
将关于当前BD的第2散列值存储为关于当前BD的完整性验证数据
S280
S290
输入下一BD?
是
否
结束

图 2

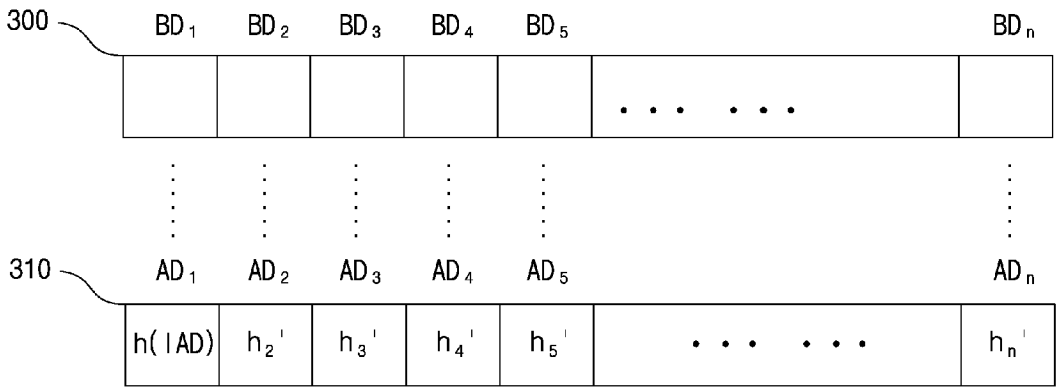


图 3

$IAD = Sign_{SK}(BD_1)$

块数据(BD_n)	第1散列值(h_n)	第2散列值(h_n')	完整性验证数据(AD_n)
BD_1	$h_1 = IAD$	$h_1' = h(h_1)$	$AD_1 = h(IAD)$
BD_2	$h_2 = h(IAD \| BD_2)$	$h_2' = h(h_2)$	$AD_2 = h_2'$
BD_3	$h_3 = h(h_2 \| BD_3)$	$h_3' = h(h_3)$	$AD_3 = h_3'$
BD_4	$h_4 = h(h_3 \| BD_4)$	$h_4' = h(h_4)$	$AD_4 = h_4'$
⋮	⋮	⋮	⋮
BD_n	$h_n = h(h_{n-1} \| BD_n)$	$h_n' = h(h_n)$	$AD_n = h_n'$

图 4

$IAD = Sign_{SK}(BD_1)$

块数据(BD_n)	第1散列值(h_n)	完整性验证数据(ADn)
BD_1	$h_1 = IAD$	$AD_1 = h(IAD)$
BD_2	$h_2 = h(IAD \| BD_2)$	$AD_2 = h_2$
BD_3	$h_3 = h(h_2 \| BD_3)$	$AD_3 = h_3$
BD_4	$h_4 = h(h_3 \| BD_4)$	$AD_4 = h_4$
⋮	⋮	⋮
BD_n	$h_n = h(h_{n-1} \| BD_n)$	$AD_n = h_n$

图 5

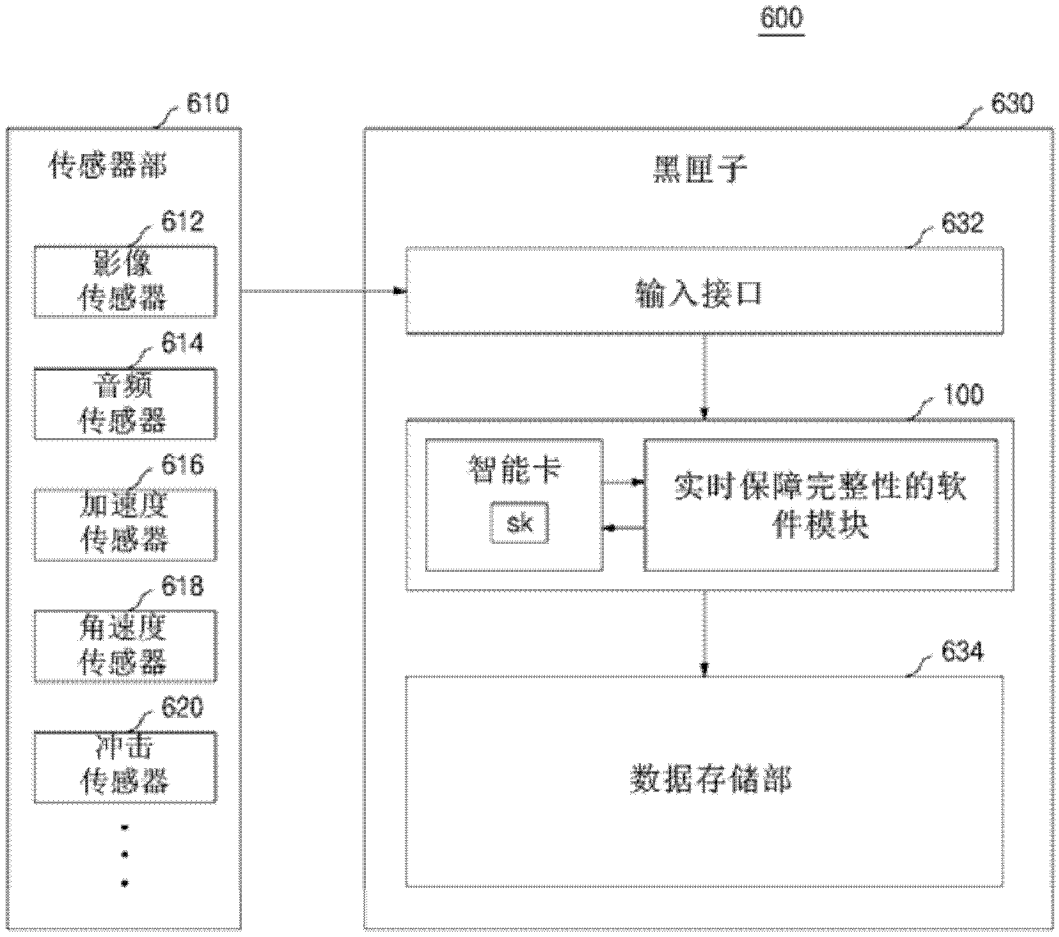

600
610
传感器部
612
影像
传感器
614
音频
传感器
616
加速度
传感器
618
角速度
传感器
620
冲击
传感器
630
黑匣子
632
输入接口
100
智能卡
sk
实时保障完整性的软
件模块
634
数据存储部

图 6