



## (12) 发明专利

(10) 授权公告号 CN 1825850 B

(45) 授权公告日 2011.06.08

(21) 申请号 200510136887.8

EP 0739106 A1, 1996.10.23, 全文.

(22) 申请日 1999.06.07

US 5495533 A, 1996.02.27, 说明书第8栏第  
69行至第9栏第58行, 附图8.

## (30) 优先权数据

39808/98 1998.09.24 KR

审查员 魏玲

39809/98 1998.09.24 KR

## (62) 分案原申请数据

99110955.4 1999.06.07

## (73) 专利权人 三星电子株式会社

地址 韩国京畿道

## (72) 发明人 姜恩成 边珍荣

## (74) 专利代理机构 北京市柳沈律师事务所

11105

代理人 邵亚丽 李晓舒

## (51) Int. Cl.

H04L 29/06 (2006.01)

## (56) 对比文件

EP 0843449 A2, 1998.05.20, 全文.

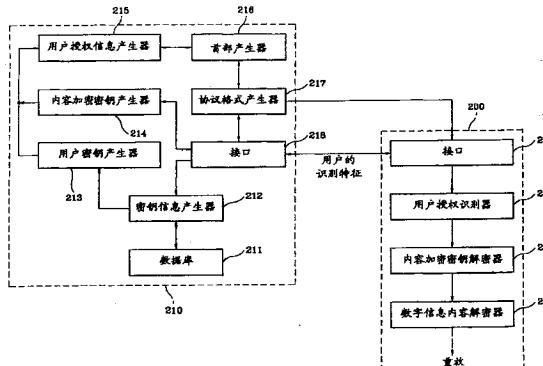
权利要求书 1 页 说明书 13 页 附图 17 页

## (54) 发明名称

数字信息内容的保密分配系统

## (57) 摘要

一种数字密码机和加密方法,其以数字格式加密和发送通过使用密钥信息,用户密钥和内容加密密钥的数字信息内容发送系统的用户所请求的特定的信息项,以便通过使用密钥信息和用户授权信息来解密和重放用户终端上的加密数字信息。每个登记的预订用户具有唯一的密钥信息。通过将该密钥信息应用到一个密钥产生算法产生用户密钥。利用该用户密钥加密当该登记的用户访问该服务器时建立的内容加密密钥。通过在一个加密算法中使用该内容加密密钥加密该数字信息。



1. 一种在一个具有用于有条件地访问数字信息的终端单元的传输系统中为用于传输数字信息的业务服务器的协议格式加密同时也保持传输安全的设备，包括：

接口，用于接收从终端单元收到的识别特征；

密钥信息产生器，用于通过使用随机数产生密钥信息，所述密钥信息对应于用户的识别特征；

用户密钥产生器，通过将密钥信息加入密钥产生算法产生用户密钥；

内容加密密钥产生器，用于产生内容加密密钥；

用户授权信息产生器，通过首先使用用户密钥加密内容加密密钥并接着使用用户密钥和加密的内容加密密钥来产生用户的授权密钥信息；

首部产生器，通过使用该用户的授权信息产生用于版权保护协议的首部；以及

协议格式产生器，通过将加密的数字信息加到首部产生版权保护协议格式。

2. 一种用于在具有提供数字信息的业务服务器的传输系统中为用来接收数字信息的终端单元解码一个协议格式同时也保持传输安全性的设备，

所述业务服务器包括：

接口，用于接收从终端单元收到的识别特征；

密钥信息产生器，用于通过使用随机数产生密钥信息，所述密钥信息对应于用户的识别特征；

用户密钥产生器，通过将密钥信息加入密钥产生算法产生用户密钥；

内容加密密钥产生器，用于产生内容加密密钥；

用户授权信息产生器，通过首先使用用户密钥加密内容加密密钥并接着使用用户密钥和加密的内容加密密钥来产生用户的授权密钥信息；

首部产生器，通过使用该用户的授权信息产生用于版权保护协议的首部；以及

协议格式产生器，通过将加密的数字信息加到首部产生版权保护协议格式；以及

所述设备包括：

一个接口，用于接收所述密钥信息和所述版权保护协议格式；

用户授权识别器，对照所述用户密钥来分析所述用户授权信息以确定所述用户是否被授权接收所述加密数字信息；

内容加密密钥解密器，利用所述用户密钥来解密在版权保护协议格式中传输的内容加密密钥；以及

数字内容解容器，使用解密的内容加密密钥来解密所述加密数字信息。

## 数字信息内容的保密分配系统

[0001] 本申请是申请日为 1999 年 6 月 7 日、申请号为 99110955.4、题为“数字信息内容的保密分配系统”的发明专利申请的分案申请。

### 技术领域

[0002] 本发明一般涉及加密方法和加密设备，具体地涉及在数字信息的发送和重放中密钥产生和使用的方法和设备。

### 背景技术

[0003] 最近，随着由诸如广播和新闻等各种媒体所提供的信息的大量涌现，已经由信息提供者建立起致力于提供能覆盖所有媒体的综合信息的一种环境。其他用户则希望从一个特定的信息提供者 (IP) 处由可得到的整个信息领域中选择性地接收特定项目的数字信息。因此，已经由信息提供者形成了一个数字信息内容发送系统，该系统是通过信息提供者将各种类型的信息转换成数字的形式并存储这种数字信息和存储关于通过网络从信息提供者预订这个数字信息系统的用户的信息而形成的。数字信息发送系统赋与容易下载数字信息内容能力的应用程序。用户可以通过使用这个应用程序通过网络访问该数字信息系统以得到全部所需的信息。

[0004] 该数字信息可以有偿或免费地提供给用户。在付费提供数字信息的情况下，经发送系统提供该数字信息的服务器设置了该业务费。该业务服务器根据当该数字信息下载到用户时请求的信息量收取用户费用。例如 MPEG 软件协议，将音频文件压缩为它们原始规模的一部分，但是在音频声音的质量上几乎没有可察觉的影响。现在因特网站广泛使用了 MPEG 软件协议以便提供数字化的音乐，但是记录的该软件协议被公用，使在没有音乐家同意的情况下发送录制的数字化音乐版本。当用户通过一个网络商业性地连接到一个提供数字信息的服务器时，一些用户能够无意地或非法地复制该数字信息，关于演奏音乐的音乐家和运行该数字信息发送系统的服务器的提供者二者在经济上遭受损害的事实最近已经由 InterdepoSIT 和法国程序保护机构，欧洲作业协会和专业信息技术的成员，从专利，商标和版权杂志，(Pateut Trademark & Copyright journal) 第 57 卷，第 1416 号，第 385 页 (1999 年 3 月 11 日) 上注意到，现在，提供者和音乐家除了通过采取民事和刑事诉讼致力于控制未经授权的数字信息的发送接收来寻求合理赔偿外别无它法。因此，在限制由未经授权的实体访问该信息和防止未经授权的用户使用其可能从信息提供者非法获得任何信息的同时，需要一种技术用来保护可靠的收益支承数字信息的传输。这通过限制未授权的用户解密他们试图通过该系统得到的任何信息的能力完成。

### 发明内容

[0005] 因此，本发明的一个目的是提供关于数字信息内容的保密分配 (securedistribution) 系统的改进。

[0006] 本发明的另一个目的是提供通过使用多重密钥能够加密和发送从发送系统接收

的数字信息的数字加密方法和设备。

[0007] 本发明的再一个目的是提供在发送数字信息给用户期间产生和使用多重密钥的数字加密方法和设备。

[0008] 本发明的又一个目的是提供在发送数字信息给用户期间按照多重密钥的产生和使用的一种使用用户信息的数字加密方法和设备。

[0009] 本发明还有另一个目的是提供一种数字加密方法和设备, 使用多重密钥加密和发送从发送系统得到的数与信息并使用多个密钥在用户终端解密和重放该数字信息, 其中之一密钥是多重密钥共有的。

[0010] 本发明的另外一个目的是提供通过使用密钥信息, 用户密钥, 和内容加密密钥能够加密和发送从发送系统获得的数字信息, 和通过使用该密钥信息和用户授权信息在用户的终端上能够解密和播放该数字信息的数字加密方法和设备。

[0011] 本发明的再一个目的是提供加密, 传输和接收协议格式以便能够加密, 传输和解密从发送系统接收的数字信息。

[0012] 本发明的再另外一个是提供加密, 传输和接收协议格式, 通过使用多重密钥加密该数字信息, 和通过使用多个密钥在用户终端上解密和重放该数字信息, 以便能够加密和传输从发送系统接收的数字信息其中该多个密钥之一是多重密钥所共有的。

[0013] 本发明的又另一个目的是提供加密, 传输和接收协议格式, 通过使用密钥信息, 用户密钥, 和内容加密密钥能够加密和传输从发送系统接收的数字信息, 和通过使用该密钥信息和用户授权信息在用户的终端上解密和重放该数字信息。

[0014] 本发明还有一个目的是提供用于发送信息到已经请求该信息的用户终端的更安全的密码机和方法。

[0015] 本发明还有又一个目的是提供一种方法, 它可靠地限制登记的用户的能力以便该用户以一种容易使用的形式传送那个信息给另一个实体, 该登记的用户已经合法地从一个信息提供者得到信息。

[0016] 这些和其他目的可以利用一个加密处理和设备得到其使用户能够请求将数字信息发送给该用户的终端单元。但是, 在发送请求的项目之前, 用户必须利用控制数字信息发送的服务器登记包括用户识别特征的用户会员资格信息。该服务器产生与从该终端单元接收的该用户的识别特征一致的加密密钥信息。响应用户对于数字信息的请求该服务器提供, 和该终端单元下载并存储由该终端单元接收的加密密钥信息。该服务器利用该加密密钥信息加密该数字信息, 和终端单元通过使用结合该加密密钥信息的一个解密算法解密从该服务器接收的数字信息并且重放该解密信息。

[0017] 本发明的一个实施例提供的一种协议格式具有:一个首部字段和一个加密数字信息字段以便保持数字信息的版权保护。该服务器使用一个协议格式产生器, 产生版权保护协议格式和产生利用相应于该用户识别特征的一个密钥产生算法加密内容加密密钥的一个用户密钥。该协议格式产生器通过使用该用户密钥产生保护协议首部格式, 其产生一个内容加密密钥。该协议格式产生器将已经利用该内容加密密钥加密的加密数字信息加到首部以便形成版权保护协议格式。该终端单元利用该密钥信息和一个解密算法解密该用户的密钥和该内容加密密钥, 并且它利用该内容加密密钥解密该版权保护协议格式。

[0018] 本发明提供一种用于加密和解密数字信息内容的设备, 该用于加密和解密数字信

息内容的设备包括：一具有解密算法的终端单元，用于发送用户的识别特征；用于接收和存储密钥信息；用于接收包括加密的数字信息内容的协议格式；和用于通过使用所述解密算法和所述密钥信息解密所述协议格式；和一具有加密算法的业务服务器，用于产生相应于从所述终端单元发送的所述识别特征的所述密钥信息；用于发送所述密钥信息给所述终端单元；用于通过使用所述密钥信息和所述加密算法加密所述数字信息内容；和用于发送包括所述加密数字信息内容和首部的所述协议格式给所述终端单元。

[0019] 本发明提供的一种协议格式设备，该协议格式设备包括：一协议格式编码器，用于编码首部和数字信息内容为版权保护协议格式，其中所述首部包括有关解密和说明所述数字信息内容的信息；和一协议格式解码器，用于解码所述协议格式和根据从所述协议格式编码器接收的所述首部的所述信息来解密所述数字信息内容。

[0020] 本发明提供的一种具有解密算法的版权保护的协议格式解码器包括：一用于接收包括加密数字信息内容的版权保护协议的装置和一用于通过使用解密算法和密钥信息解密版权保护协议的装置，以重放加密数字信息内容。

[0021] 本发明提供的一种保护版权的协议，该保护版权的协议格式包括：一加密的数字信息内容；和一具有解密所述加密的数字信息内容的信息的首部。

[0022] 本发明提供的一种用于加密数字信息内容的方法，该用于加密数字信息内容的方法包括步骤：输入用户识别特征，用于登记；确定所述用户是否登记；当确定未登记所述用户时，将所述用户的所述识别特征的信息存储在成员资格登记上；发送密钥信息给所述用户；响应来自所述用户的请求信号通过使用内容加密密钥加密所述数字信息内容；和发送所述加密数字信息内容。

## 附图说明

[0023] 通过结合附图参照下列详细描述，本发明的特征和许多附带的优点会更清楚，同时本发明的特征和优点会变得更好理解，附图中相同的标号表示相同或相似的部件，其中：

- [0024] 图 1 是说明根据本发明原理构造的数字密码机的一个实施例的示意方框图；
- [0025] 图 2 是说明图 1 所示的终端单元的一个实施例的示意方框图；
- [0026] 图 3 是说明图 1 所示的数字密码机的另一个实施例的示意方框图；
- [0027] 图 4 是说明图 1 所示的终端单元的另一个实施例的示意方框图；
- [0028] 图 5 是说明图 1 所示的数字密码机的实施例的更多细节的示意方框图；
- [0029] 图 6 是说明图 3 所示的数字密码机的实施例的更多细节的示意方框图；
- [0030] 图 7 是说明当应用到图 3 所示的实施例的一个业务服务器的操作流程图；
- [0031] 图 8 是说明应用到图 3 所示的实施例的一个主机服务器的操作流程图；
- [0032] 图 9 是说明根据本发明原理在协议格式编码器和协议格式解码器之间的操作关系的示意方框图；
- [0033] 图 10 是可以应用到本发明的实践的一个协议格式的说明；
- [0034] 图 11 是可以应用到本发明的实践的一个协议格式的另一个实施例的说明；
- [0035] 图 12 是可以应用到图 10 和图 11 所示的协议格式的首部字段的说明；
- [0036] 图 13 是可以应用到图 10 和图 11 所示的协议格式的首部字段的另一个实施例的

说明；

- [0037] 图 14 是适合于图 12 和图 13 所示的首部字段的一个未加密首部字段的说明；
- [0038] 图 15 说明适合于用做图 12 和图 13 所示的首部字段的一个未加密首部字段的另一个实施例；
- [0039] 图 16 说明适合于应用到图 14 和图 15 所示的未加密首部字段的用户授权信息的格式；
- [0040] 图 17 说明可以应用到图 12 和 13 所示的首部字段的首部字段的细节；
- [0041] 图 18 说明产生在本发明的实践中的协议的一个处理的流程图；
- [0042] 图 19 说明在图 18 所示的处理中产生首部的一个处理的流程图；
- [0043] 图 20 说明在图 19 所示的处理中产生用户授权信息的一个处理的流程图；
- [0044] 图 21A 和 21B 说明在本发明的实践中解密和播放数字信息的一个处理的流程图；
- [0045] 图 22 是说明适合于广播由图 1 和图 3 所示的实施例发送的数字信息的播放机的一个实施例的方框图；和
- [0046] 图 23A 和 23B 说明在本发明的实践中解密数字信息的另一个处理的流程图。

### 具体实施方式

[0047] 本发明的实施例提供使用密钥以便加密和解密数字信息例如录制的音乐和音频和视频资料。本发明的实施例可以使用三个密钥以便加密和解密数字信息。

[0048] 用户密钥是在主机服务器上产生的密钥信息当用户已经请求数字信息和未利用主机服务器登记时在业务服务器请求的时刻产生。如果一个特定的数字信息内容发送系统将该主机服务器与该业务服务器 (service server) 结合，则该密钥信息也可以由该业务服务器产生。用户密钥信息用于产生加密、解密处理的一个内容加密密钥。另外，该用户密钥信息用于确认该用户是否被授权下载和在该用户的终端单元上重放加密的数字信息。该用户密钥信息最好由使用随机数产生并且形成对用户可以是唯一的一对一的对应。其一旦产生，该用户密钥信息与该用户的特征信息一起存储在主机服务器的数据库中。该用户密钥信息的大小最好是 128 字节。

[0049] 用户的密钥用于加密和解密首部中的内容加密密钥。该用户的密钥通过将该用户密钥信息应用于密钥生成算法产生，并且该用户密钥用于产生和确认该用户的授权信息。该用户的授权信息包括由使用该密钥信息与该用户密钥一起产生的一个散列值。当该用户密钥的散列值与首部中的该用户的授权信息中的散列值相同时，该用户被授权重放加密的数字信息。

[0050] 总之，用户的密钥由使用用户密钥信息产生。用户的密钥用于加密首部中的用户授权信息中包括的输出内容加密密钥和解密该加密的输入内容加密密钥，以便解密和播放加密的数字信息。该散列值具有有利特性，总是从相同的输入提供相同的输出，不用总是允许输入从该输出导出。

[0051] 内容加密密钥还用于加密数字信息的一部分和首部。密钥最好使用随机数产生和它的大小最好是 8 字节的倍数。在本发明的实现中，内容加密密钥最好是 8 字节。本发明的一个特征是不会产生具有相同内容的两个内容加密密钥。例如，内容加密密钥可以根据当用户访问业务服务器时的时间产生。因此，同一用户将接收不同的内容加密密钥，每个内

容加密密钥对应于一个不同的用户访问时间。内容加密密钥只有在用户访问该系统时保持有效和在访问后无效。

[0052] 除加密由信息提供者提供的数字信息的算法,和使授权用户解密从信息提供者得到的信息的算法外,本发明提供使用多个其他算法。这些算法包括密钥产生算法,数字信息内容 (digital content) 加密和解密算法,和散列算法。

[0053] 这些算法的第一个算法,密钥产生算法,通过使用来自主机服务器的密钥信息产生用户密钥。在那些系统中,主机服务器与业务服务器是分开的,密钥产生算法包括在业务服务器中。

[0054] 第二个算法,数字信息内容加密算法,也包括在业务服务器中并且由业务服务器使用以便产生首部信息来加密由用户已经请求的数字信息。

[0055] 第三个算法,散列算法,用于通过使用业务服务器中用户的密钥产生用户的授权信息,和用于确定关于该用户是否被授权接收该用户通过该系统已经向信息提供者请求的数字信息。

[0056] 由用户请求的数字信息在这个说明书中有时指数字信息内容 (digital content)。简要地,数字信息是数据,诸如已经变成存储在一个单独文件中的数字信息的音乐或文学作品。利用网络通信的应用程序的帮助。用户可以选择已经存储在文件中的数字信息,并且接着使用用于重放数字信息的个人或便携计算机访问和读或听该数字信息。该数字信息包括已经由信息提供者变换为数字数据并以文件形式诸如杂志,书,字典,图或说明以及歌曲文件形式存储的所有信息。

[0057] 图 1 和 2 是表示根据本发明原理构造的数字信息内容加密和解密设备的一个实施例的示意方框图。终端单元 10 发送用户的识别特征和接收并存储由业务服务器 12 产生的与由用户终端单元 10 提供的识别特征一致的密钥信息。密钥信息与协议格式和由用户请求的加密数字信息一起从业务服务器 12 接收。终端单元 10 通过使用存储的密钥信息和解密算法解密和重放该数字信息。

[0058] 业务服务器 12 产生具有用户授权信息的首部包括了已经利用用户的密钥加密后的内容加密密钥。业务服务器 12 接着将加密的数字信息加到首部以便产生版权保护的协议格式。版权保护的协议格式通过该网络发送到用户终端单元 10。

[0059] 如图 2 所示,终端单元 10 可以利用配备了一个常规通信设备和用于重放该数字信息的一个外设或内部设备 11b 的一个个人计算机 PC 11a 来构造。计算机 11a 和重放设备 11b 可以具有多个解密算法。终端单元 10 可以是连接到因特网的一个个人计算机 (PC) 或一个便携式计算机 11a,或可以是配备了通信程序和通信设备的任意类型的设备,该通信设备能够连接到因特网。可以结合到终端单元 10 的计算机 11a 的通信设备的例子是数字电视机,蜂窝电话机或 Web 可视电话 (web videophones)。例如,当计算机 11a 配备一个网络访问程序时,终端单元 10 可以或连接到一个公共交换电话网或一个无线网。

[0060] PC 11a 从业务服务器 12 接收该密钥信息和在存储器中存储该密钥信息。PC 11a 还接收包括加密的数字信息的协议格式并在一个长期存储媒体例如硬盘 (例如,HDD) 中存储该数字信息。计算机 11a 还通过使用存储的密钥信息产生用户的密钥,通过使用产生的用户密钥解密该内容加密密钥,通过使用解密的内容加密密钥解密已加密的数字信息。因此,解密的数字信息可以通过独立于任何其他内部或外围的重放设备 11b 的或计算机 11a

的一个视频显示器或一个音频设备重放。

[0061] 重放设备 11b 从 PC 11a 接收密钥信息和加密的数字信息内容并通过使用存储的解密算法解密该加密的数字信息内容。重放设备 11b 根据它的存储媒体类型可以或是便携的或固定的。

[0062] 业务服务器 12 基于从终端单元 10 发送的用户识别特征产生密钥信息，存储该密钥信息和识别特征，并当该用户请求该密钥信息时发送该密钥信息给终端单元 10 的计算机 11a。业务服务器 12 响应该用户的请求产生内容加密密钥，它使用用户的密钥信息产生用户的密钥，并且从使用用户的密钥和该用户密钥的散列值加密后的内容加密密钥中产生用户的授权信息。业务服务器 12 还将已经由加密算法加密的数字信息加到包括该用户的授权信息的首部以便形成版权保护协议格式，并且接着发送该版权保护协议格式给终端单元 10。

[0063] 业务批准代理服务器 14 从业务服务器 12 接收一个涉及数字信息费的信号该费用用于从业务服务器 12 下载该数字信息内容，并且通过累积登记用户的这些费用收取用户费用。

[0064] 定义用户的优选的识别特征可以是用户的社会安全号 (social security number)，用户的驾照号或用户的居住登记号，可以使用任何特征组但是趋向于以驾照号 (driver license number) 的方式唯一识别该用户。

[0065] 图 3 是表示适于本发明的实现的另一个实施例的示意方框图。涉及终端单元 20，重放设备 21b 和业务批准代理服务器 24 的说明将因为这些部分在图 1 和 2 的每个实施例中已在前面描述过而省略。优选地，业务服务器，主机服务器和终端单元是利用基于微处理器的计算机和伴随它们的操作和数据存储器实现的。

[0066] 业务服务器 22 发送一个请求信号给主机服务器 23，该请求信号请求对应于由用户终端单元 20 发送的识别特征的密钥信息。为响应请求信号的接收，主机服务器 23 发送该密钥信息给业务服务器，并且接着该密钥信息发送给终端单元 20。业务服务器 22 还响应用户的请求发送该密钥信息给终端单元 20。业务服务器 22 产生一个内容加密密钥响应该用户的请求，使用该密钥信息产生用户密钥，并且从通过使用用户的密钥和该用户密钥的散列值加密的内容加密密钥中产生用户授权信息。业务服务器 22 将由加密算法加密的数字信息加到包括该用户授权信息的首部以便形成版权保护协议格式，并且接着发送该版权保护协议格式给终端单元 20。

[0067] 主机服务器 23 产生对应于从业务服务器 22 发送的识别特征的密钥信息并且将该密钥信息与该识别特征存储在一起，并且接着发送该密钥信息给业务服务器 22 响应由业务服务器 22 产生的请求信号。

[0068] 在图 1，图 2 和图 3 的实施例中，业务服务器 12 和 22 可以给用户提供数字信息菜单或表它们是经业务服务器 12, 22 从信息提供者得到的。这使用户容易地选择用户想要的数字信息。例如，如果数字信息是音乐，则该内容表例如可以是歌曲名或歌唱家名或作曲家名。

[0069] 图 5 是表示图 1 的数字密码机的详细功能结构的方框图，具有示出的业务服务器和终端单元之间的功能结构和相互关系。终端单元 200 的功能结构为一个接口 201，一个用户授权识别器 202，一个内容加密密钥解密器 203，和一个数字信息内容解密器 204。接口

201接收根据用户的识别特征由业务服务器210已经产生的密钥信息。用户授权识别器202在读出从业务服务器210接收的版权保护协议的首部之后得到用户的密钥，并且接着通过利用已经产生的用户密钥分析该用户的授权信息确定该用户是否授权以便接收数字信息。内容加密密钥解密器203通过使用由用户授权识别器202提供的用户密钥来解密该内容加密密钥。数字信息内容解密器204通过使用由内容加密密钥解密器203解密的内容加密密钥来解密利用版权保护协议接收的加密的数字信息。

[0070] 业务服务器210可以构造为一个接口218，密钥信息产生器212，用户密钥产生器213，内容加密密钥产生器214，用户授权信息产生器215，首部产生器216，和协议格式产生器217。接口218接收从终端单元200收到的识别特征。密钥信息产生器212确定由接口218接收的识别特征是否存在于用户登记的识别特征组中该特征组存储在数据库211，并且接着产生该密钥信息。用户密钥产生器213通过将密钥信息加入密钥产生算法产生用户密钥。内容加密密钥产生器214当用户通过接口218访问业务服务器210和请求数字信息的某些项时产生内容加密密钥。用户授权信息产生器215通过使用由用户密钥产生器213产生的用户密钥加密内容加密密钥和接着使用用户的密钥和加密的内容加密密钥产生用户的授权密钥信息。首部产生器216通过使用该用户的授权信息和加密必需的另外信息产生一个用于版权保护协议的首部。协议格式产生器217通过将加密的数字信息加到由首部产生器216产生的首部产生版权保护协议格式。

[0071] 由图5功能性的说明数字信息内容密码机的操作该操作提供在用户将他的，或她的识别特征和请求一起发送时从业务服务器210接收数字信息，该识别特征由业务服务器210通过接口218接收和加到密钥信息产生器212。密钥信息产生器212对一个识别特征的相同组是否存在于在数据库211的存储器内用户登记的识别特征中进行确定。根据确定的结果，密钥信息产生器212还产生相应于识别特征的新的密钥信息和将新的密钥信息加到用户密钥产生器213或将已经从数据库211读出的用户登记的密钥信息发送给用户密钥产生器213。

[0072] 用户密钥产生器213通过将该密钥信息加到密钥产生算法来产生用户的密钥，并且接着将该用户的密钥提供给用户授权信息产生器215。内容加密密钥产生器214产生内容加密密钥响应通过接口218输入的用户访问信号，并且将该内容加密密钥输入到用户授权信息产生器215。用户授权信息产生器215通过将该用户的密钥加到该散列算法例如通过计算确定一个散列值，接着通过使用该用户的密钥加密内容加密密钥。用户授权信息产生器215从一组散列值和加密的内容加密密钥中产生用户授权信息。由产生器215提供的用户的授权信息被加到首部产生器216。首部产生器216将该用户授权信息加到首部，并接着将首部提供给协议格式产生器217，协议格式产生器217通过将加密的数字信息加到首部形成版权保护协议格式并且接着发送该版权保护协议格式给用户的终端单元200。

[0073] 图6是表示图3的数字密码机的详细功能结构的方框图，示意性地示出业务服务器110，主机服务器120和终端单元100的功能结构和相互关系。密钥信息产生器121和数据库122属于主机服务器120。而且，用户密钥产生器111，接口116，内容加密密钥产生器112，用户授权信息产生器113，首部产生器114，和协议格式产生器115属于业务服务器110。这些部件的功能操作与关于图5表示的实施例的讨论中的描述相同。

[0074] 前面段落中对本发明的说明主要是通过参照个人计算机的用户进行的。但是讨论

的原理可以应用到配备有通信程序和解密算法的任意类性的设备。

[0075] 图 7 是说明当数字信息提供给以前未登记在由业务服务器 22 保留的用户数据库中的用户时,图 3 所示的业务服务器 22 的操作的流程图。业务服务器 22 可以利用网络访问程序从终端单元 20 访问。当用户发送他的或她的识别特征时,业务服务器 22 通过将那些识别特征与由数据库保留的登记用户的识别特征作比较来识别那个用户是否登记。如果这个用户被确定是登记了的,则密钥信息产生器不产生另外的密钥信息。但是,如果确定那些识别特征不存在于主机服务器 22 的数据库,则业务服务器 22 将识别该用户作为一个新的成员用户和开始进行执行这个用户的成员资格登记。如果该用户完成成员资格登记处理,则业务服务器 22 从主机服务器 23 接收密钥信息和接着在步骤 S510 发送该密钥信息给终端单元 20 响应该用户的请求。响应于该识别特征而产生的这个密钥信息将保持法律效力,除非该用户请求消除他的成员资格。

[0076] 在步骤 S510 之后的步骤 S520 业务服务器 22 确定用于下载数字信息内容的用户请求信号是否已经从终端单元 20 接收到。如果在步骤 S520 确定下载的请求信号已经接收到,则在步骤 S530 期间,业务服务器 22 通过使用该密钥信息产生用户的密钥,通过使用该用户的密钥加密内容加密密钥,和接着通过使用该用户的密钥和加密的内容加密密钥建立首部。在步骤 S530,业务服务器 22 还通过将加密的数字信息内容加到首部产生版权保护协议格式和发送该协议格式给用户的终端单元 20。在发送数字信息内容给用户以后,在步骤 S540 期间,业务服务器 22 发送由用户在得到数字信息过程中招致的费用的业务费信息给业务批准代理服务器 (service sanctionagent server) 24 以便将费用信息加到用户的存储费信息业务的帐上。业务批准代理服务器 24 接着收取用户由使用系统以便得到发送给他的终端单元 20 的数字信息招致的数字信息内容费。

[0077] 图 8 是说明图 3 所示的主机服务器的操作的流程图。在步骤 S610,主机服务器 23 确定识别特征是否已经从终端单元 20 接收到。当主机服务器 23 确定识别特征已经接收到时,在步骤 S620,将那些识别特征与存储在主机服务器 23 的数据库中的识别特征作比较以便确定一个相同的识别特征组是否存在于数据库中。在步骤 S620 之后,如果已经确定一个相同的识别特征组已经存在于数据库中,则在步骤 S630 期间,将利用那些识别特征所存储的相应的密钥信息发送给业务服务器 22。如果确定没有相同的识别特征组以前已经被存储在数据库中,则在步骤 S640 产生新用户的密钥信息和,在步骤 S650,将其与新用户的识别特征一起存储。

[0078] 典型地,当如图 3 和 4 所示,该密码被配置给单独的业务服务器 22 和主机服务器 23 时,由业务服务器 22 执行步骤 S510 和由主机服务器 23 通过 S650 执行步骤 S610。如图 1 和 2 所示,当仅提供一个单独的业务服务器 12 时,业务服务器 12 完整地执行这些步骤以便产生相应于用户识别特征的密钥信息和接着发送产生的密钥信息给用户的终端单元 20;因为从图 7 和 8 可以容易地推导出该处理,所述对这些步骤不再作具体描述。

[0079] 当一起提供了密钥信息和由用户请求的数字信息时,终端单元 10,20 通过存储的解密算法解密密钥信息和数字信息并同时,输出解密的数字信息或给外部或给内部音频输出设备(例如,扬声器或耳机)以便给用户提供可听到的解密数字信息。因此,当出现数字信息从终端单元 10,20 非法拷贝到一些其他终端单元时,在那些密钥信息没有被存储的其他终端单元内将不能处理数字信息从而防止了加密的数字信息被重放和听到。

[0080] 当一个登记的用户想将由该用户从业务服务器 10, 20 得到的数字信息提供给另一个人时, 那个其他人的识别特征与该登记用户的识别特征被存储在一起。在那种情况下, 利用以前的识别特征以及其他人的识别特征解密和重放加密的数字信息。所提供的数字信息的交换导致的费用将由利用业务服务器 22 登记的用户来付。

[0081] 在功能方面, 这个数字信息内容密码机 (cryptograph) 用作本发明实现中的加密和解密设备, 该密码机可以概括地分成加密数字信息的设备和解密加密的数字信息的设备。

[0082] 图 9 是表示根据本发明原理的数字密码机功能的功能结构的示意方框图。本发明的数字密码机可以归结为操作地连接到协议格式解码器 31 的协议格式编码器 30。协议格式编码器 30 产生包括加密数字信息的版权保护协议格式和包括与其在一起的加密和解密数字信息必需的信息的首部。协议格式解码器 31 根据保护协议格式的首部信息解密和重放从协议格式编码器 30 的版权保护协议格式中接收的加密数字信息。

[0083] 更具体地, 协议格式编码器 30 通过使用依据用户的识别特征产生的密钥信息和密钥产生算法来产生用户密钥。接着, 协议格式编码器 30 通过使用用户的密钥和该用户密钥的一个散列值将具有加密内容加密密钥的用户授权信息加到首部而产生该首部, 协议格式编码器 30 还通过将已经利用内容加密密钥加密的数字信息加到该首部而产生版权保护协议格式。

[0084] 协议格式解码器 31 接收由协议格式编码器 30 发送的版权保护协议格式, 通过使用该密钥信息产生用户密钥, 并且解码器当协议格式编码器 30 已经识别出授权终端单元的用户时在通过使用该用户的密钥解密内容加密密钥之后通过使用该内容加密密钥解密该加密的数字信息内容。作为一个利用由业务服务器, 或主机服务器保存的数据库登记的用户, 该用户是否被授权的表示是通过采用该用户的密钥, 由协议格式解码器得到的用户授权信息提供的以便确定该用户是否被授权接收、解码和使用该数字信息。

[0085] 现在参考图 10 到图 16, 详细描述协议格式处理系统的操作。当用户选择他或她想得到的数字信息时, 本发明的数字密码机将该数字信息安排为在下面段落中更详细描述的协议格式, 并且接着将该协议格式发送给用户的终端单元。

[0086] 图 10 是应用本发明实现的一个协议格式的说明。由一个业务服务器发送的用于保护数字信息版权的一个协议的格式, 它可以安排为具有: 包括一个用于加密数字信息的信息和说明该数字信息的资料的首部, 和一个加密的数字信息字段。现在再参照图 5, 为理解首部记录结构, 由用户请求的数字信息的首部是由用户密钥和内容加密密钥部分加密的以便防止在没有密钥信息的情况下, 例如当加密的数字信息由另一个实体得到时重放数字信息。

[0087] 图 11 是利用包括可以随意增加的附加字段的版权保护协议格式, 说明对于由图 10 所示的可选的协议格式的另一个实施例。一个表示加密数字信息大小的字段可以插入首部和加密的数字信息内容字段之间; 优选地加密数字信息的大小与未加密数字信息内容字段的大小相同。另外, 一个附加信息字段可以加到加密数字信息内容字段的尾端以便为方便和容易由用户理解而定义该加密数字信息。例如, 如果数字信息是一个音乐歌曲, 该附加信息可以是各种相关的信息, 例如音乐家的姓名, 歌曲的标题, 演奏时间, 唱片集标题 (title of album), 唱片集出版者, 歌曲的出版日期, 和如果数字信息是音乐电视, 则该附

加信息可以包括相关的电影的名称。可以顺序安排附加信息字段与首部和数据依次安排，所以格式可以扩展，而不管版权保护协议内包括的数字信息的附加项目数。

[0088] 图 12 具体说明适合于图 10 和 11 的首部字段，具有：一个版权支持信息字段，一个未加密首部字段和一个加密首部字段。该版权支持信息字段包括一个版权支持代码，该代码表示由数字信息内容提供者提供的数字信息是否支持该版权。如果版权支持代码存在于版权支持信息字段，则识别出提供给用户的数字信息符合于加密的数字信息，并且接着由用户解密重放。另外，如果版权支持代码不存在于版权支持信息字段，则识别出该数字信息不符合于未加密的数字信息（例如，由于数字信息接收者的未登记状态）和终止解密处理以使数字信息只在没有解密的情况下重放（即，在它的加密状态例如噪声重放）。

[0089] 图 13 说明图 12 可选的首部字段的另一个实施例。图 13 的首部字段相应于图 11 说明的协议格式的任意附加的字段。一个偏址字段 (offset field) 和表示未加密首部大小的一个字段可以插入版权支持信息字段和未加密首部字段之间。偏址字段提供关于附加信息字段的位置的信息；这使附加信息字段能够在没有首部分析的情况下被访问。而且，在加密首部字段之前按顺序提供表示加密首部大小的字段。

[0090] 图 14 说明适合于由图 12 和 13 所示的可选方案的首部字段的一个未加密首部字段的格式。可以安排未加密首部字段具有：一个版权库版本字段，表示数字变换格式类型的一个数字变换格式字段，表示关于密钥产生算法的信息的一个密钥产生算法字段，表示关于数字信息内容加密算法信息的一个数字信息内容加密算法字段，在用户终端单元的计算机上表示用户授权信息的字段，和在重放设备上表示用户授权信息的字段。数字变换格式字段表示使用哪种变换技术将数字信息内容变换成数字信号。该变换方法的典型例子是 MP3 和 AAC。加密算法字段可以包括：一个散列算法代码，密钥加密算法代码，原始向量 (IV) 大小，和用于加密数字信息内容的原始向量信息。在用户终端单元的计算机上表示用户授权信息的字段和在重放设备上表示用户授权信息的字段是首部最重要的部分；它们用于识别用户的授权以便使用数字信息和按照比例增加共享加密数字信息的人数。

[0091] 图 15 说明对于图 14 所示的可任选的未加密首部字段的另一个实施例。这个未加密首部字段可以任意包括增加的附加字段，例如信息提供者的标识符和共享数字信息的用户数。表示信息提供者代码的字段可以插入数字信息内容变换格式字段和密钥产生算法字段之间。可以将表示在终端单元共享计算机的用户数的一个字段，和表示共享重放设备的用户数的一个字段加到数字信息内容加密算法字段的后端。

[0092] 图 16 说明适合于图 14 和 15 所示的未加密首部字段的用户授权信息字段的详细结构。在终端单元的计算机上以及在重放设备上的用户授权信息字段可以安排为具有：一个第一字段，它表示由散列算法产生的散列值大小；一个第二字段，表示用户密钥的散列值；一个第三字段，表示由密钥加密算法建立的加密内容加密密钥的产生值大小；和一个第四字段，表示加密内容加密密钥的产生值。

[0093] 图 17 说明适合用于图 12 和 13 所示的首部字段的加密首部的安排的细节。加密首部字段可以安排为具有：一个第一字段，表示提供给用户的数字信息内容的基本处理单元；一个第二字段，表示加密字节数；和一个第三字段，表示加密数字信息内容的重复周期。数字信息的基本处理单元和由加密数字信息产生的加密字节数可以由信息提供者指定；但是，基本处理单元和加密字节数很可能由基本算法通过参照终端单元的处理速度和通过参

照基于终端单元用于微处理器存储数据的存储器被设置为基本值。

[0094] 图 18 是说明在本发明实现期间产生保护协议格式的一个方法的流程图。当从用户接收数字信息内容请求信号时, 内容加密密钥在步骤 S110 产生。接着, 确定当该内容加密密钥在步骤 S120 产生时, 由数字信息内容提供者确定的首部产生算法是否存在。如果在步骤 S120 期间确定首部产生算法是业务服务器可用的, 则在步骤 S130 利用由数字信息内容提供者确定的首部产生算法产生首部。如果建立首部产生算法的该确定对于业务服务器是不可用的, 则在步骤 S190 利用一个基本值建立首部。

[0095] 在或步骤 S130 或 S190 建立首部之后, 在步骤 S140 期间加密由用户请求的该数字信息和接着在步骤 S150 期间将加密的数字信息加到在或步骤 S130 或 S190 期间产生的首部。当附加信息提供给用户时, 在步骤 S160 进行确定关于与首部组合的数字信息的附加信息是否存在。在步骤 S160 期间, 如果确定附加信息存在, 则附加信息字段在步骤 S170 期间和在步骤 S180 期间产生, 并加到加密数字信息内容的后端以便形成版权保护协议格式。接着将版权保护协议格式发送给早先对数字信息作出请求的用户。当该信息提供者愿意对用户作出关于数字信息内容的一些附加说明时, 附加信息由信息提供者任意加到数字信息中。可以由业务提供者选择地增加附加信息处理步骤 220。

[0096] 图 19 是说明产生应用到图 18 的首部的方法的流程图。

[0097] 描述提供的数字信息内容是否在版权的保护之下的该版权支持信息字段, 和表示未加密首部大小的字段均被产生和加到首部 (S210)。未加密首部字段也被产生和加到首部 (S220), 该字段包括: 版本信息, 音乐类型, 支持版权的业务提供者的代码, 散列算法, 密钥产生算法, 和数字信息内容加密算法。

[0098] 如果数字信息内容的附加信息字段存在, 则关于附加信息字段的开始点信息也可以加到首部。

[0099] 在步骤 S230, 构造首部部分的一部分, 使用用户具有的密钥信息产生用户授权信息和将产生的用户授权信息加到首部 (S240)。步骤 S240 之后, 产生加密的首部信息 (S250)。

[0100] 首部信息包括: 数字信息内容加密必需的信息例如加密块的大小, 加密周期和加密帧单元等。还产生首部信息以便包括通过将整个首部应用到散列算法得到的散列值, 利用该值可以确定首部信息的改变。

[0101] 加密在步骤 S250 产生的首部信息 (S260) 和接着将关于加密首部的信息和该加密首部的大小加到首部 (S270), 以便产生被加到发送给用户的加密数字信息内容的前端的首部。

[0102] 在由数字信息内容提供者提供的加密算法存在的情况下 (S260), 利用加密算法和内容加密密钥加密首部信息。否则通过基本算法和内容加密密钥加密首部信息。

[0103] 图 20 是说明产生应用到图 19 的用户授权信息的方法的流程图, 用于更详细地描述在图 19 的步骤 S230 上产生加密密钥信息的方法。

[0104] 确定密钥信息或内容加密密钥是否存在 (S310)。当在步骤 S310 确定密钥信息和内容加密密钥存在时 (S320), 通过将该密钥信息应用到密钥产生算法产生用户密钥。

[0105] 通过将在步骤 S320 产生的用户密钥应用到散列算法计算散列值 (330), 并且接着使用密钥加密算法和产生的用户密钥来加密内容加密密钥 (S3400)。在确定步骤 S310 时,

当确定密钥信息或内容加密密钥不存在时,利用错误消息的输出终止处理。

[0106] 图 21 是说明根据本发明解密和重放加密的数字信息内容的方法的流程图。

[0107] 首先,确定密钥信息或从数字信息内容提供者接收的数字信息内容是否存在(S410)。当确定数字信息内容或密钥信息存在时(S415),读出数字信息内容的首部,和当该数字信息内容和该密钥信息不存在时,识别该处理出现错误和终止该处理。

[0108] 确定在步骤 S415 读出的首部是否包括版权支持代码,就是说,数字信息内容是否支持版权(S420)。

[0109] 如果确定该版权支持代码存在,则识别为数字信息内容受到版权保护并且将读出的未加密的首部信息存储在存储器中作为一个预定的变量(S425)。

[0110] 如果确定版权支持代码不存在,即,数字信息内容不受到版权保护,在解密处理中将该数字信息内容识别为错误。接着解密处理不再执行和不通过解密处理解码和输出接收的数字信息内容。

[0111] 当确定数字信息内容由版权支持时,使用密钥信息产生用户密钥和接着计算产生的用户密钥的散列值(S430)。

[0112] 确定计算的用户密钥的散列值是否与该首部中用户密钥的散列值相同(S435)。

[0113] 当确定计算的用户密钥的散列值与首部中的用户密钥的散列值相符时,识别用户是被授权的并且使用该用户密钥解密内容加密密钥(S440)。使用解密的内容加密密钥解密加密的首部(S445)。通过将整个首部应用到散列算法计算用于确定整个首部变化的参考值的整个首部的散列值(S450)。

[0114] 在确定步骤 S435,当确定计算的用户密钥的散列值与首部中用户密钥的散列值不相同时,输出例如“没有授权”的消息和终止整个数字信息内容的解密处理。

[0115] 根据整个首部的散列值确定首部的变化(S455)。在确定首部没有改变的情况下,解密加密的数字信息内容(S460)。

[0116] 确定附加信息是否存在(S465)。如果确定附加信息不存在则重放数字信息内容(S470)。并且当确定附加信息存在时处理附加的信息接着进行重放(S475)。

[0117] 当在步骤 S455 确定首部被改变时,识别该用户没有授权,以便终止解密处理,对该用户不重放该数字信息内容(S490)。

[0118] 图 22 示意说明应用到图 1 和图 3 的重放设备的结构。

[0119] 存储器 300 包括:用于整个系统的一个驱动算法和用于解密加密的数字信息内容的多个算法。存储器 300 在其中存储接收的密钥信息和数字信息内容数据以响应该写信号和输出存储的密钥信息和数字信息内容数据以响应该读信号。存储器 300 优选是一个快闪存储器(flash memory)。

[0120] 微计算机 320 接收该密钥信息和数字信息内容数据以便将其存储到存储器 300,通过存储在存储器 300 中的算法解密加密的数字信息内容并且接着根据从用户密钥输入设备 330 输入的密钥信号输出它们。同时,它控制显示器 340 显示设备的目前状态。

[0121] 当输入的数字信息内容被加密时,微计算机 320 根据该算法使用存储在存储器 300 中的密钥信息通过首部的用户授权信息产生用户密钥,该算法也存储在存储器 300 中。而且,微计算机 320 使用产生的用户密钥来解密包括在首部的用户授权信息中的内容加密密钥。使用解密的内容加密密钥解密加密的数字信息内容以便输出。

[0122] 当接收到未加密数字信息内容时,微计算机 320 在不解密它们的情况下重放和输出数字信息内容。解码器 350 解码从微计算机 320 输出的数字信息内容以便输出音频信号。解码器 350 优选是 MPEG 解码器。

[0123] 图 23 说明如图 22 所示在从 PC 输入加密的数字信息内容到重放设备的情况下解密加密的数字信息内容的方法的流程图。微计算机 320 确定密钥信息是否从 PC 输入 (S510) 并且当确定该密钥信息输入时在存储器 300 中存储输入的密钥信息 (S520)。

[0124] 在存储器 300 中存储该密钥信息以后,微计算机 320 确定加密的数字信息内容是否从 PC 输入 (S515)。当在步骤 S520 确定输入了加密的数字信息内容时,微计算机 320 在存储器 300 中存储该数字信息内容并且接着在发送处理完成以后根据存储在存储器 300 中的解密算法从数字信息内容中读出首部 (S525)。当确定没有输入加密的数字信息内容时,将它们识别为一个错误 (S580) 并且终止解密处理。

[0125] 下一步,微计算机 320 确定版权支持代码是否存在与读出的数字信息内容的首部 (S530)。如果确定版权支持代码存在,则识别该数字信息内容受到版权的保护和将读出的未加密的首部信息存储在存储器 300 中作为一个预定的变量 (S535)。当确定数字信息内容受到版权保护时,微计算机 320 使用该密钥信息和密钥产生算法来产生用户密钥。微计算机 320 利用存储在存储器 300 中的散列算法计算产生的用户密钥的散列值 (S540)。

[0126] 下一步,微计算机 320 确定计算的用户密钥的散列值是否与该首部的用户授权信息中的用户密钥的散列值相同 (S545)。当确定计算的用户密钥的散列值与首部中用户密钥的散列值相符时,识别用户是被授权的并且使用用户密钥解密内容加密密钥 (S550)。使用解密的内容加密密钥来解密加密的首部 (S555)。

[0127] 在确定步骤 S545,当确定计算的用户密钥的散列值与首部中用户密钥的散列值不相同时,输出一个“未授权”的消息并终止解密处理。根据整个首部的散列值进行确定整个首部是否改变以便确定用户是否被授权解密和重放该数字信息内容 (S455)。通过将整个首部应用到散列算法计算散列值 (S560)。

[0128] 根据在步骤 S560 计算的整个首部的散列值是否与存储在首部中的整个首部的散列值相同确定整个首部的改变 (S565)。

[0129] 在确定首部没有改变的情况下,即,在步骤 S560 计算的整个首部的散列值与存储在首部中的整个首部的散列值相同的情况下,解密加密的数字信息内容 (S570)。处理附加信息并且接着在附加信息不存在的情况下重放 (S575)。

[0130] 当在步骤 S565 确定首部改变时,即,计算的整个首部的散列值与存储在首部中的整个首部的散列值不相同,识别为用户没有授权从而终止解密处理,对用户不重放数字信息内容 (S585)。

[0131] 本发明在没有使用解码算法和密钥信息的情况下可不重放提供的加密数字信息。因此,当数字信息非法拷贝时,它可以不重放。这样就阻碍了非法拷贝,分配,出版和未授权的分配,并且使由非法拷贝和未授权分配引起的数字信息的信息提供者遭受严重损失的危险最小化。并且,这个系统鼓励了用户经过合法途径获得信息。

[0132] 虽然已经结合当前被认为是最实际的和优选的实施例描述了本发明,但是应该理解本发明不限于公开的实施例,而,相反,本发明将覆盖包括在本发明权利要求书中的精神和范围内的种种改进和等同物。

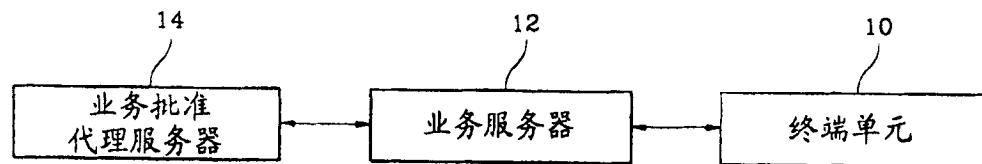


图 1

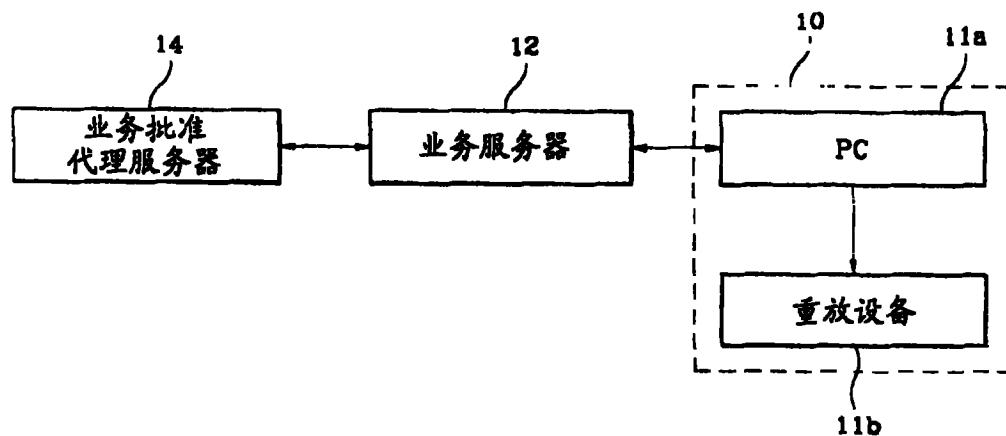


图 2

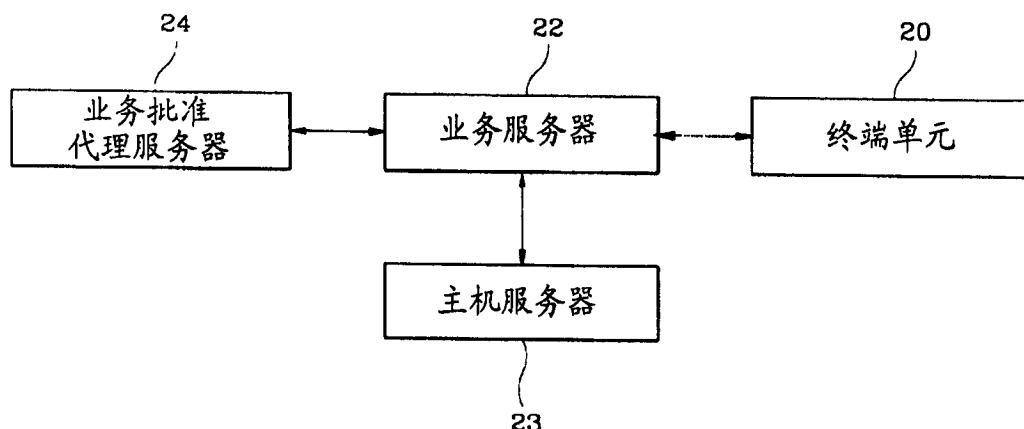


图 3

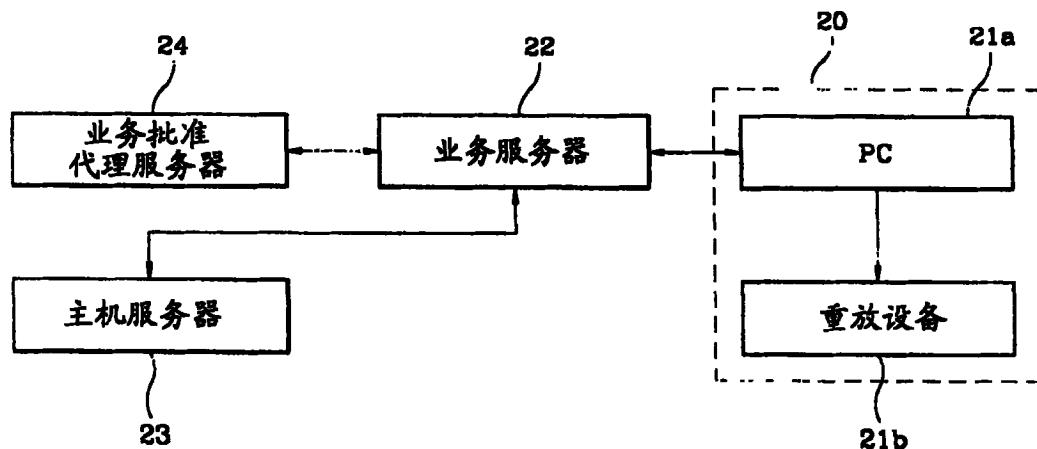


图 4

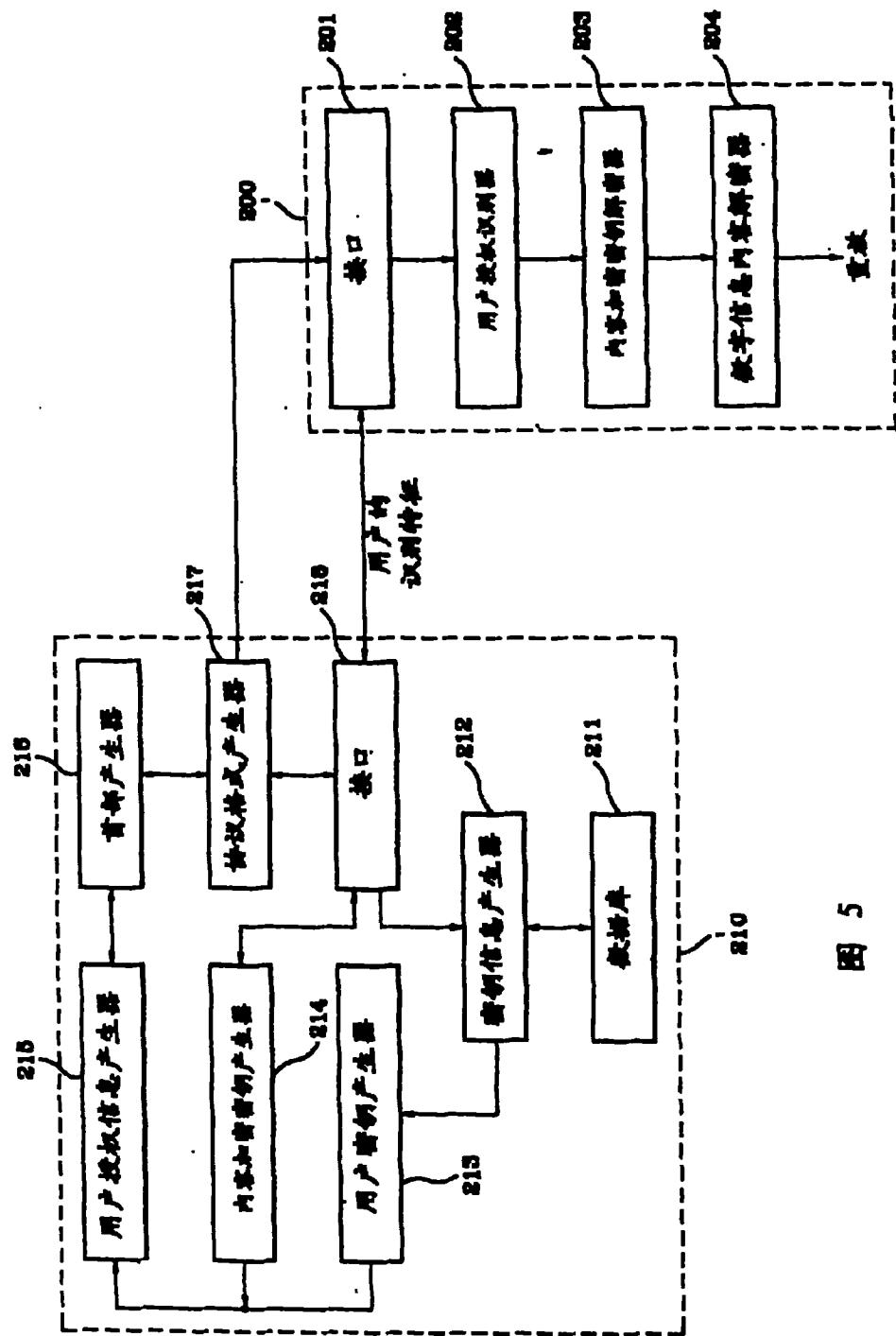


图 5

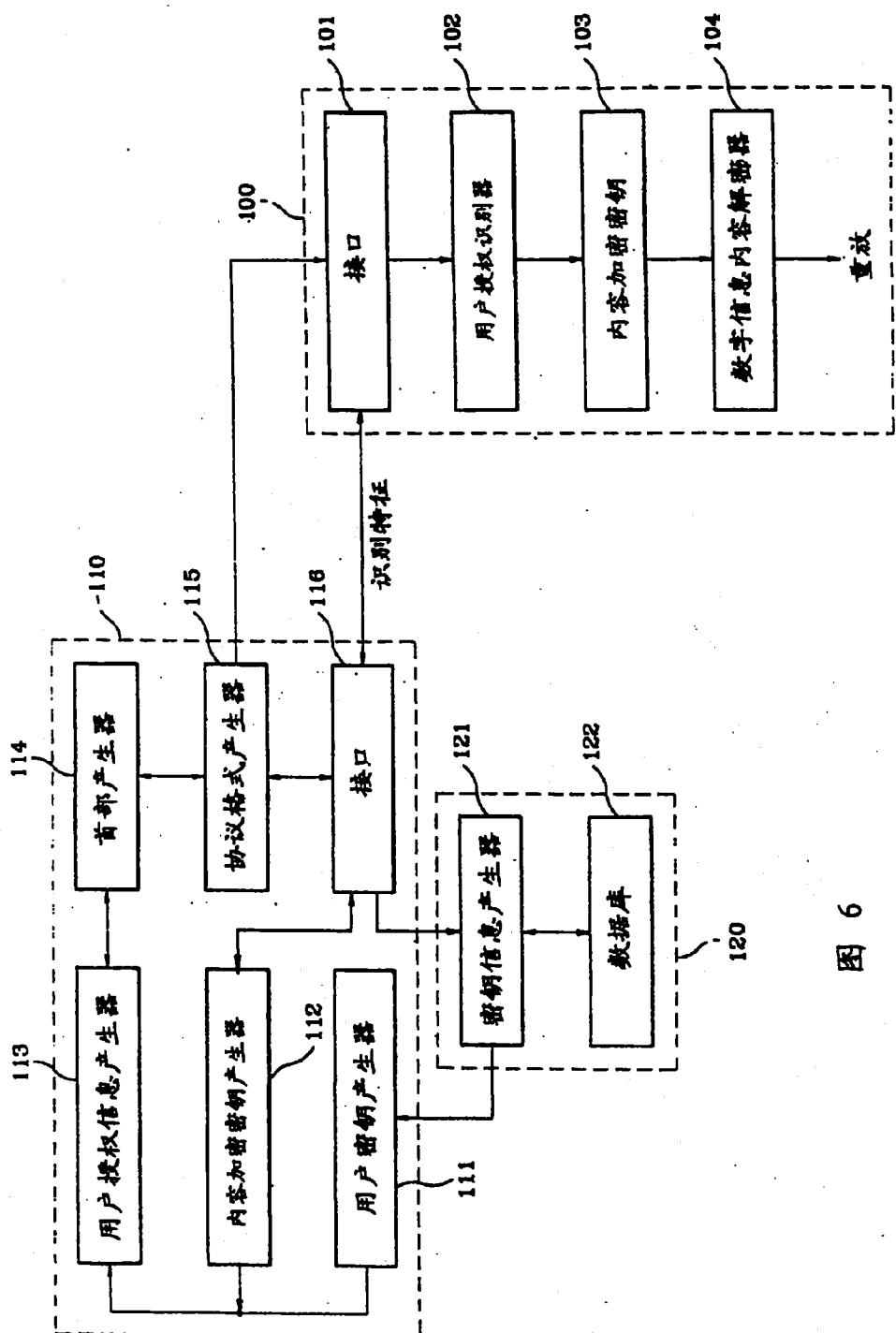


图 6

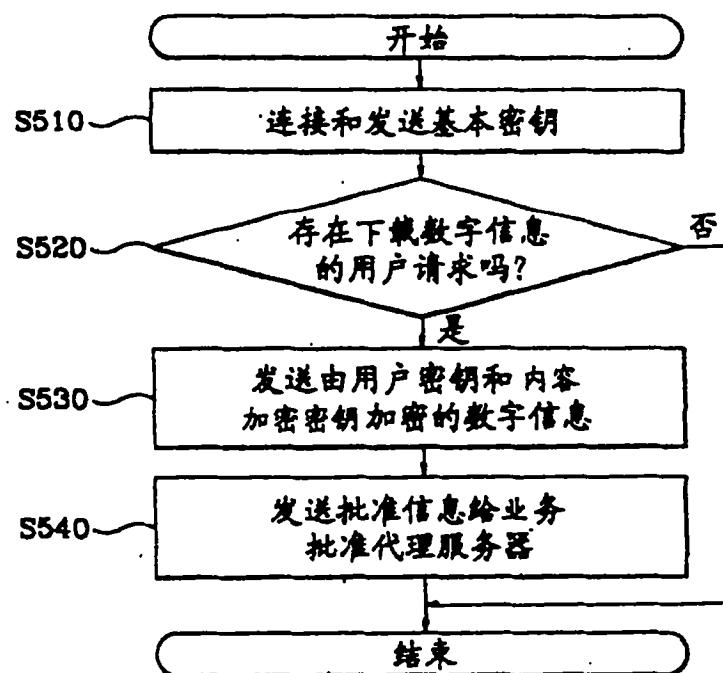


图 7

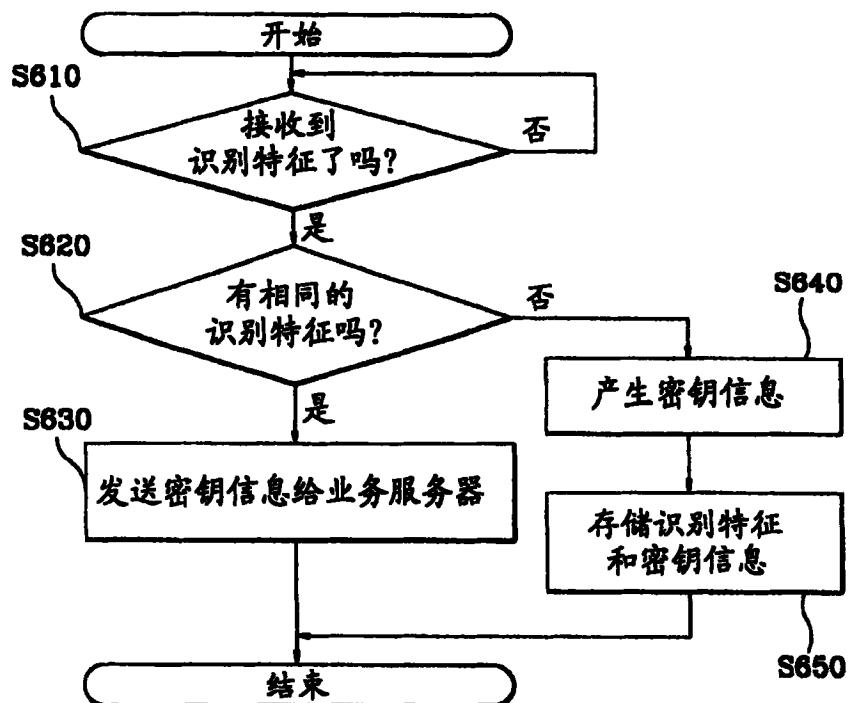


图 8

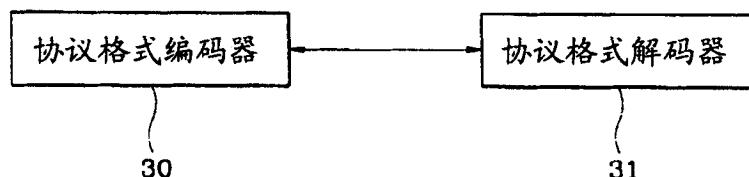


图 9

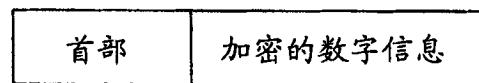


图 10

首部	加密数字信息 内容的大小	加密的数字信息	附加信息
----	-----------------	---------	------

图 11

版权支持信息	未加密的首部	加密的首部
--------	--------	-------

图 12

版权支 持信息	偏址	未加密首 部的大小	未加密的首部	加密首 部的大小	加密首部	附加信息
------------	----	--------------	--------	-------------	------	------

图 13

版权库版本	关于数字信息内容 变换格式的信息	密钥产 生算法	数字信息内 容加密算法	在PC上的用户 授权信息	在重放设备上 的用户授权信息
-------	---------------------	------------	----------------	-----------------	-------------------

图 14

版权库 版本	数字信息内 容变换格式	数字信息内 容提供者代码	密钥产 生算法	数字信息内 容加密算法	共享PC的 用户数	共享重放设 备的用户数	PC上的用户 授权信息	重放设备上的 用户授权信息
-----------	----------------	-----------------	------------	----------------	--------------	----------------	----------------	------------------

图 15

散列值 的大小	散列值	加密的内容加密 密钥的结果值大小	加密的内容加密 密钥的结果值
------------	-----	---------------------	-------------------

图 16

数字信息内容 的基本处理单元	加密大小	加密的周期
-------------------	------	-------

图 17

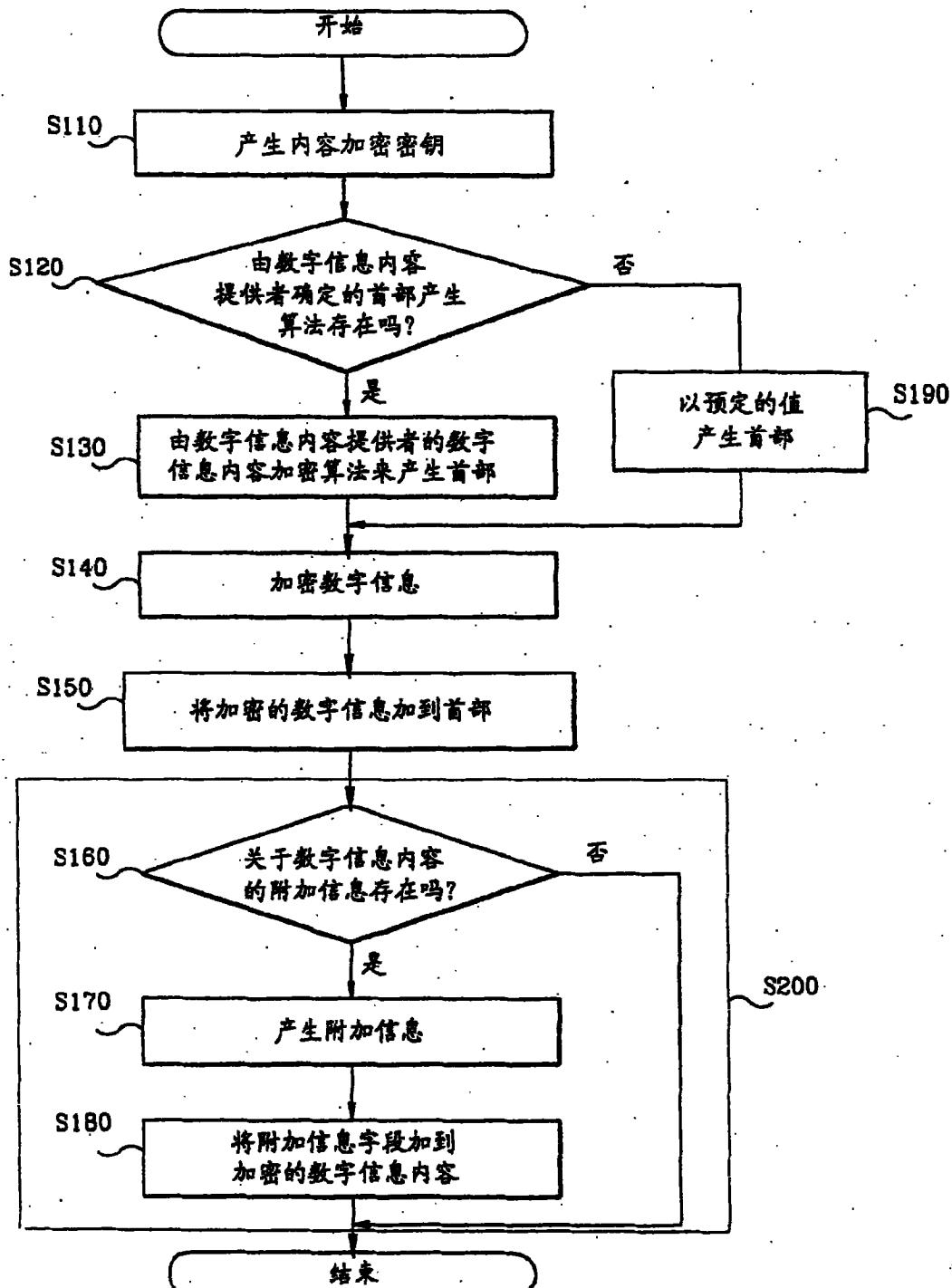


图 18

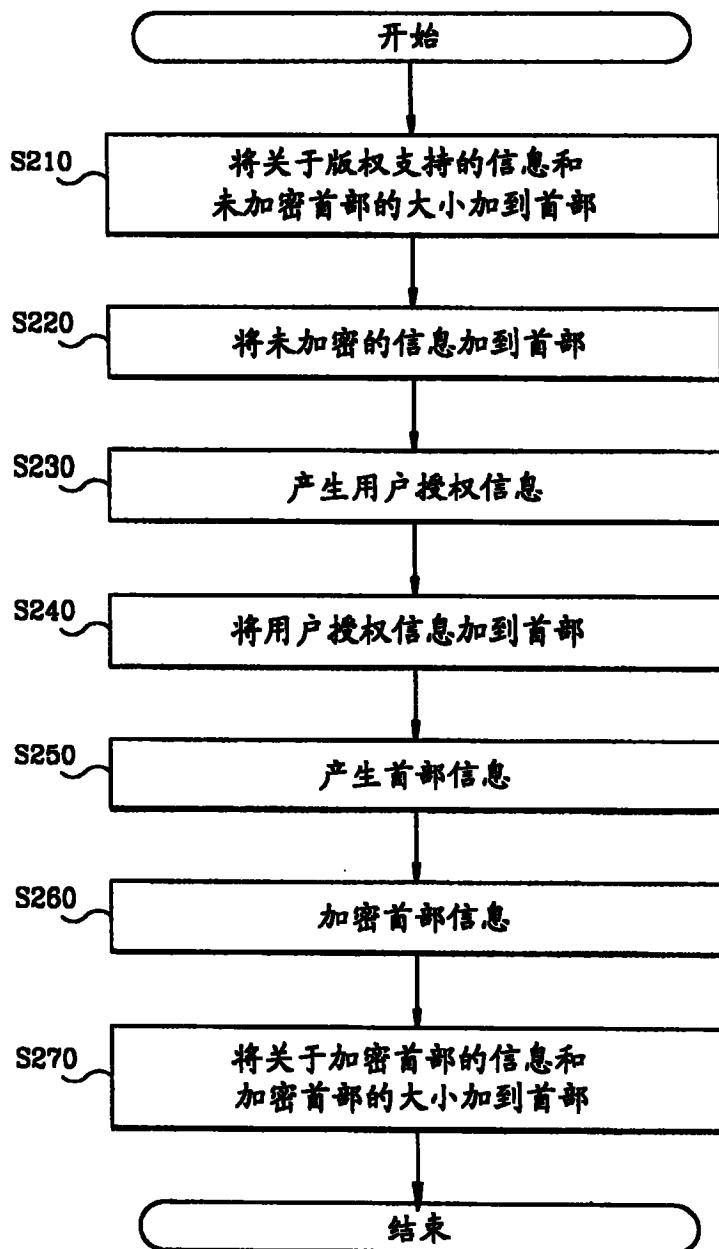


图 19

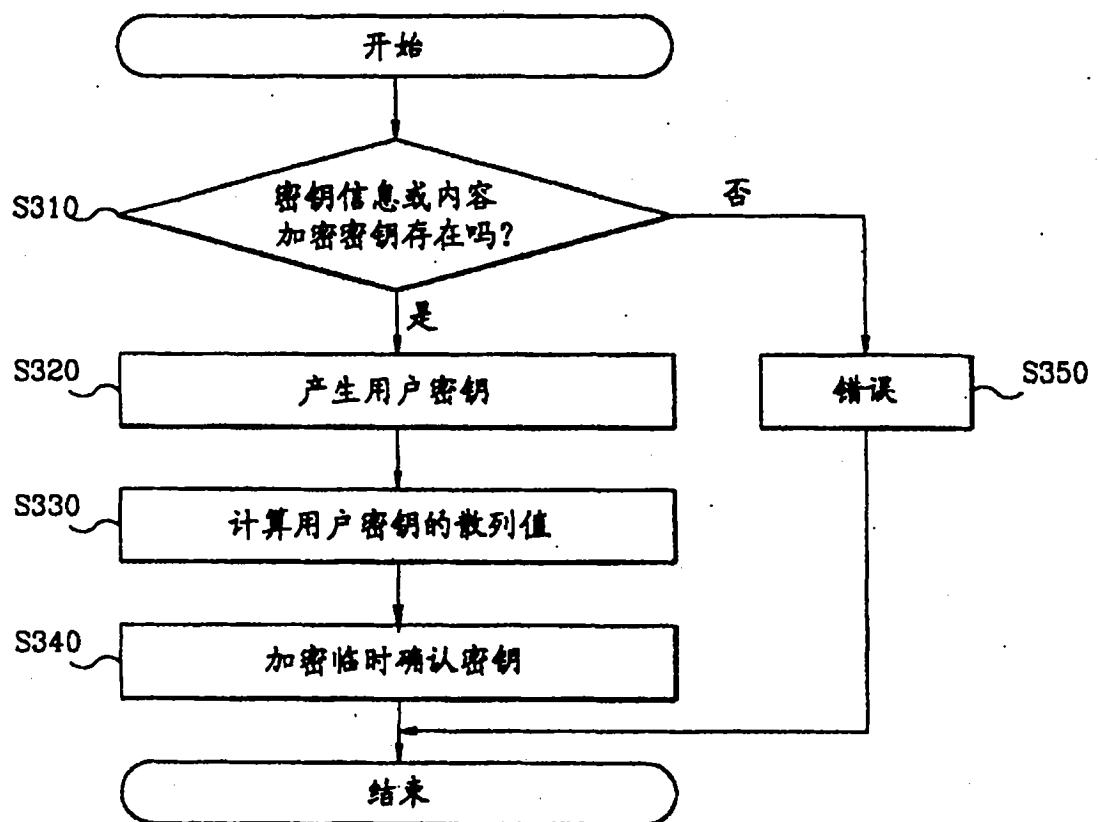


图 20

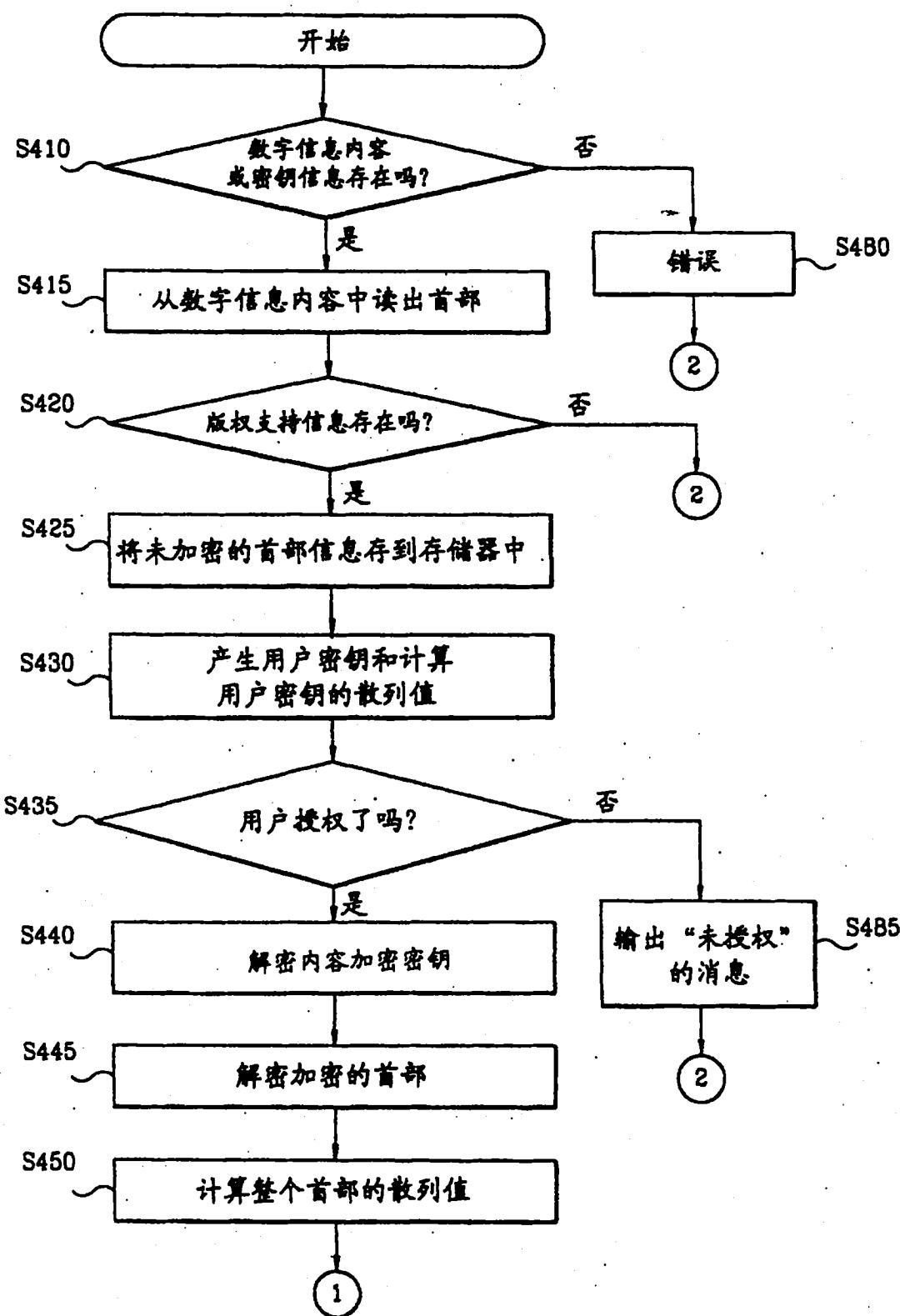


图 21A

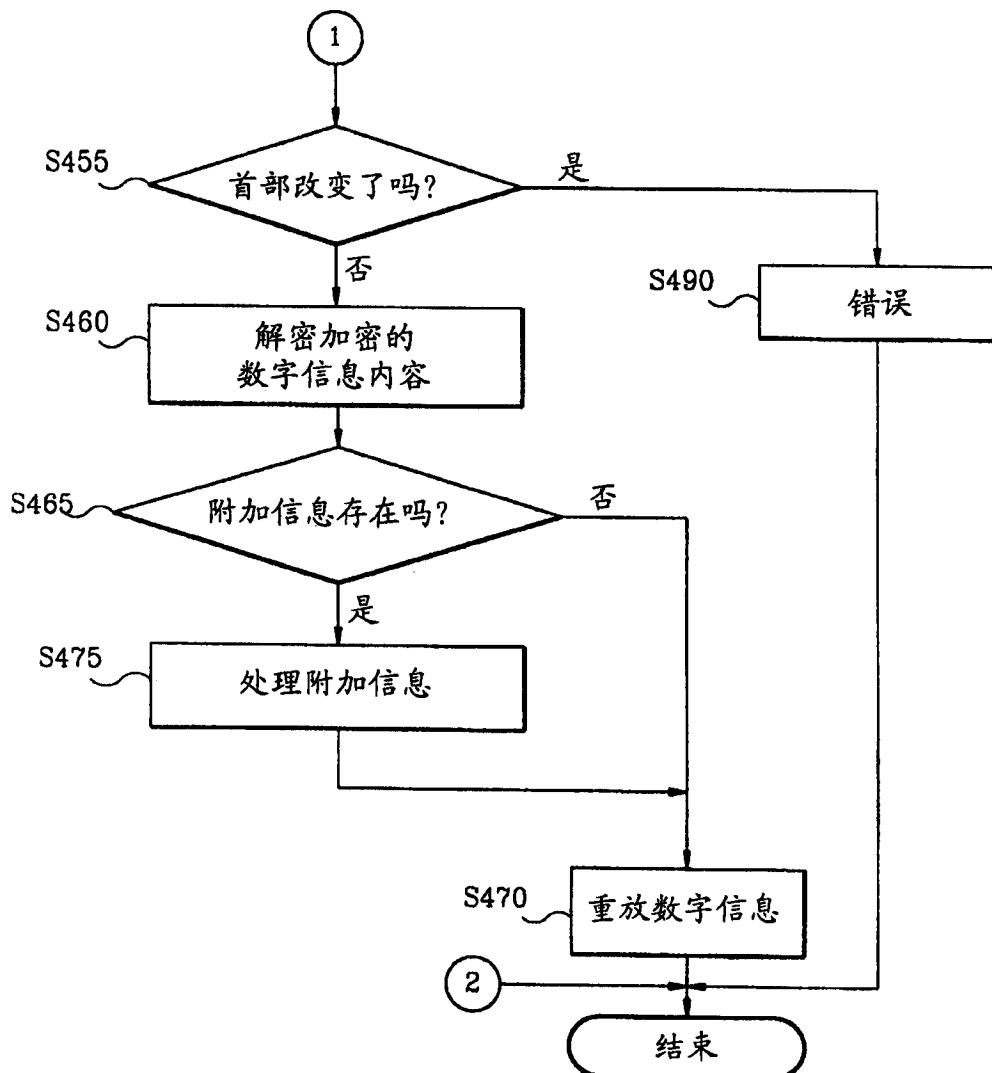


图 21B

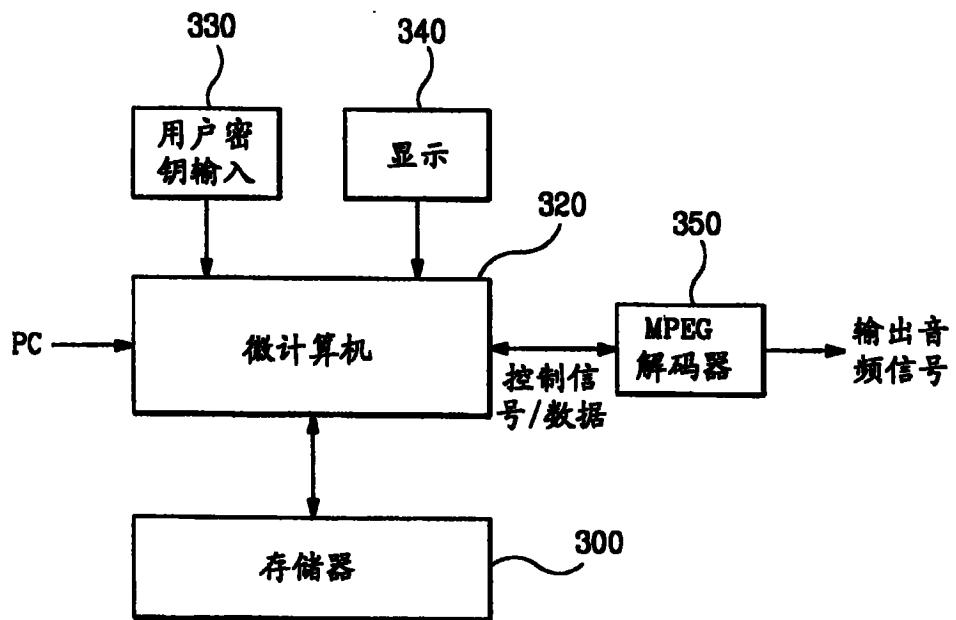


图 22

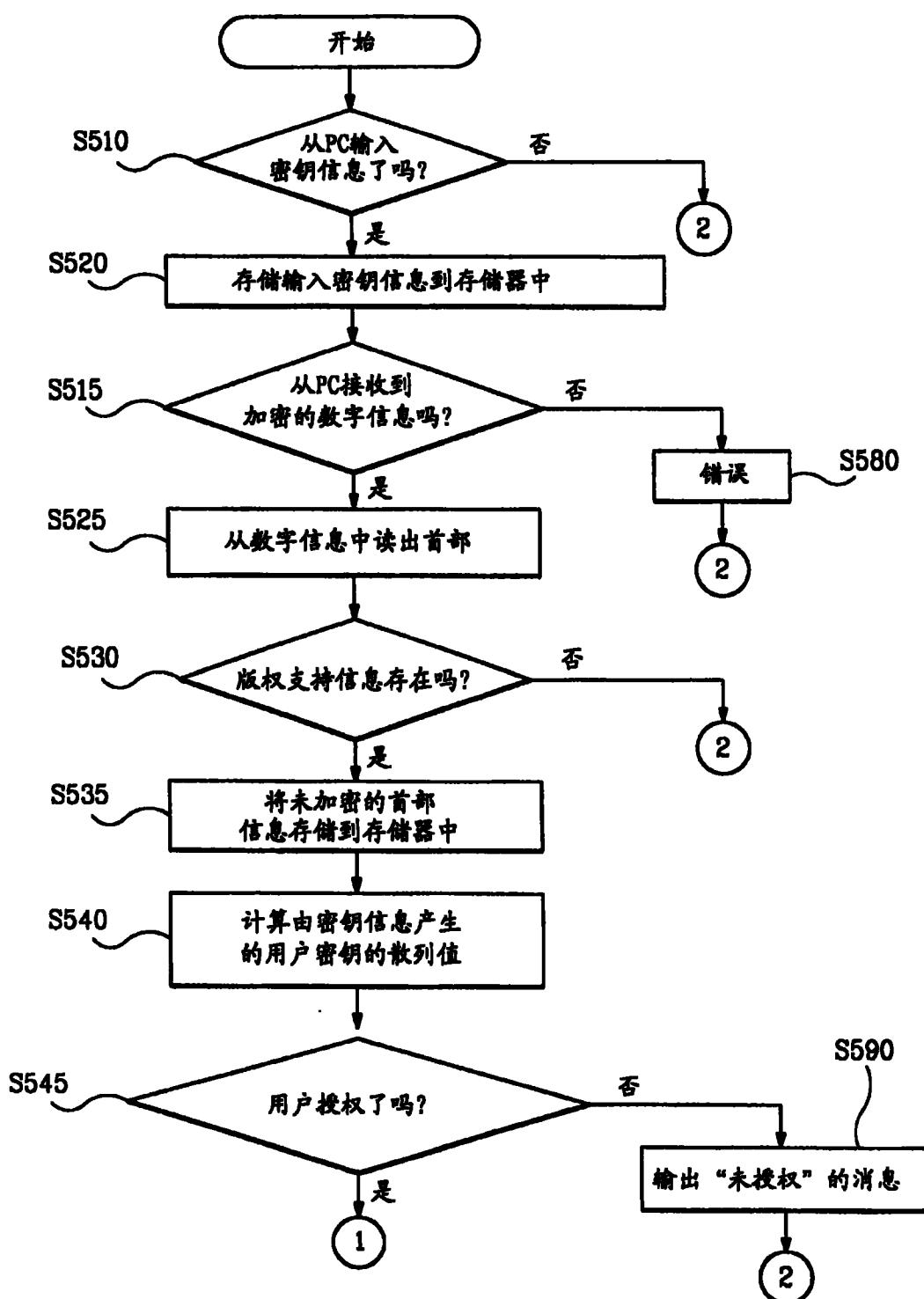


图 23A

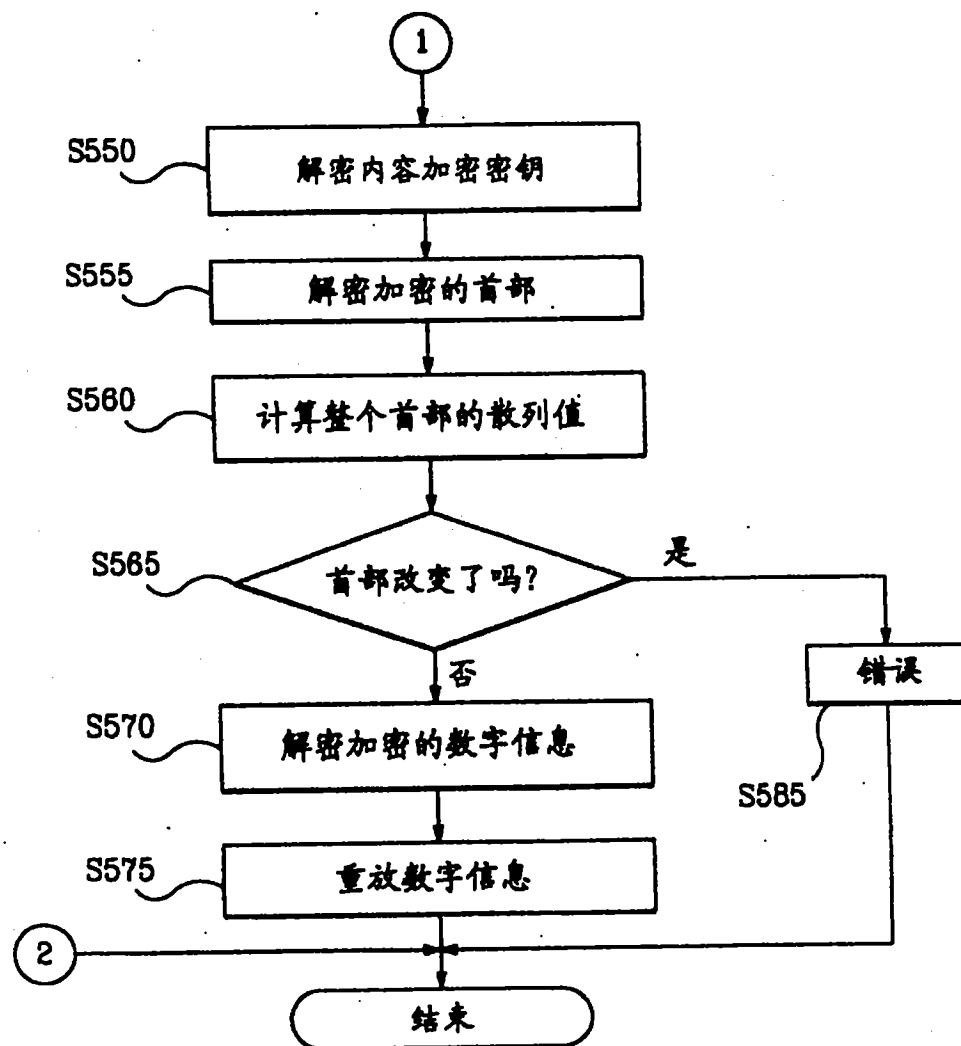


图 23B