[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/00 (2006.01)
H04L 12/56 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200510135736.0

[43] 公开日 2007 年 2 月 7 日

[11] 公开号 CN 1909443A

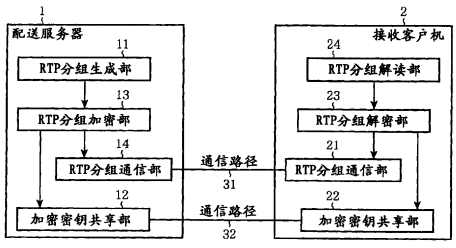
[22] 申请日 2005.12.29
[21] 申请号 200510135736.0
[30] 优先权
[32] 2005. 8. 2 [33] JP [31] 2005 - 224434
[71] 申请人 三菱电机株式会社
地址 日本东京
[72] 发明人 平松隆宏 阿倍博信 山田耕一 横里纯一
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 曲 瑞
权利要求书 3 页 说明书 11 页 附图 2 页

[54] 发明名称

数据配送装置和数据通信系统

[57] 摘要

本发明提供了一种进行安全性高的数据通信的数据配送装置和数据通信系统。其中，RTP 分组生成部(11)通过分割数据来生成分组，在标题中附加用于识别所生成的分组的信息。RTP 分组加密单元(13)将生成的分组内部的数据划分成规定的块，使用加密密钥共享部(12)所共享的加密密钥对每个块加密数据，并且，在加密最开始的块时，使用包含在标题中的、用于识别分组的信息作为初始向量来进行加密，在加密以后的每一个块时，以利用前一个块的加密结果的加密方式来进行加密。



1、一种数据配送装置，其特征在于，具备:

分组生成单元，通过分割数据来生成分组，并在标题中附加用于识别所生成的分组的信息;

加密密钥共享单元，与数据接收装置之间共享加密密钥;

分组加密单元，将由上述分组生成单元生成的分组内部的数据划分成规定的块，使用上述加密密钥共享单元所共享的加密密钥对每个块加密数据，并且，在加密最开始的块时，使用包含在标题中的、用于识别上述分组的信息作为初始向量来进行加密，在加密以后的每一个块时，以利用前一个块的加密结果的加密方式来进行加密；和

分组通信单元，经由通信路径将由该分组加密单元加密后的分组配送到上述数据接收装置。

2、根据权利要求 1 所述的数据配送装置，其特征在于:

上述分组加密单元使用密码块链接（CBC）模式作为加密方式。

3、根据权利要求 1 所述的数据配送装置，其特征在于:

上述分组生成单元生成互联网协议（IP）分组，上述分组加密单元使用包含在 IP 标题中的标识符（ID）作为上述初始向量。

4、根据权利要求 1 所述的数据配送装置，其特征在于:

上述分组生成单元生成用户数据报协议（UDP）分组，上述分组加密单元使用包含在 UDP 标题中的 ID 作为上述初始向量。

5、根据权利要求 1 所述的数据配送装置，其特征在于:

上述分组生成单元生成实时传输协议（RTP）分组，上述分组加密单元使用包含在 RTP 标题中的顺序号作为上述初始向量。

6、根据权利要求 5 所述的数据配送装置，其特征在于:

上述分组加密单元使用对上述顺序号进行加密后得到的值作为上述初始向量，在加密上述顺序号时，利用使用了与上述数据接收装置之间共享的规定初始向量的上述加密方式以及上述加密密钥来进行加密。

7、根据权利要求 5 所述的数据配送装置，其特征在于：

上述分组加密单元使用扩展顺序号作为上述初始向量，上述扩展顺序号联结了计数器的值和上述顺序号，上述计数器对包含在上述 RTP 标题中的顺序号超过值的上限后进行循环的次数进行计数。

8、根据权利要求 7 所述的数据配送装置，其特征在于：

上述分组加密单元使用对上述扩展顺序号进行加密后得到的值作为上述初始向量，在加密上述扩展顺序号时，利用使用了与上述数据接收装置之间共享的规定初始向量的上述加密方式以及上述加密密钥来进行加密。

9、根据权利要求 7 或 8 所述的数据配送装置，其特征在于：

上述分组加密单元使用随机设定的值作为上述计数器的初始值，并与上述数据接收装置之间共享该值。

10、根据权利要求 7 所述的数据配送装置，其特征在于：

上述分组加密单元使用上述扩展顺序号以及包含在 RTP 标题中的、表示时刻信息的时间标记作为上述初始向量。

11、根据权利要求 10 所述的数据配送装置，其特征在于：

上述分组加密单元使用对上述扩展顺序号以及上述时间标记进行加密后得到的值作为上述初始向量，在加密上述扩展顺序号以及时间标记时，利用使用了与上述数据接收装置之间共享的规定初始向量的上述加密方式以及上述加密密钥来进行加密。

12、一种数据通信系统，具备配送数据的数据配送装置和接收所配送的数据的数据接收装置，该数据通信系统的特征在于：

上述数据配送装置具备：

分组生成单元，通过分割数据来生成分组，并在标题中附加用于识别所生成的分组的信息；

第 1 加密密钥共享单元，与上述数据接收装置之间共享加密密钥；

分组加密单元，将由上述分组生成单元生成的分组内部的数据划分成规定的块，使用上述第 1 加密密钥共享单元所共享的加密密钥对每个块加密数据，并且，在加密最开始的块时，使用包含在标题中的、

用于识别上述分组的信息作为初始向量来进行加密，在加密以后的每一个块时，以利用前一个块的加密结果的加密方式来进行加密；和

第 1 分组通信单元，经由通信路径将由该分组加密单元加密后的分组配送到上述数据接收装置，

上述数据接收装置具备：

第 2 分组通信单元，接收由上述第 1 分组通信单元配送的数据；

第 2 加密密钥共享单元，与上述数据配送装置之间共享加密密钥；

分组解密单元，使用上述第 2 加密密钥共享单元所共享的加密密钥，对由上述第 2 分组通信单元接收到的分组进行解密；和

数据恢复单元，从由该分组解密单元解密后的分组中恢复数据。

数据配送装置和数据通信系统

技术领域

本发明涉及一种配送图像或声音等数据的数据配送装置、以及具备该数据配送装置和接收所配送的数据的数据接收装置的数据通信系统。

背景技术

在作为现有技术的非专利文献 1 中，提供了一种在 IP（互联网协议，Internet Protocol）网络上配送以图像或声音为代表的实时数据的机构。在 IP 网络上是将数据变成分组后进行传送，但不能保证将分组可靠地配送到目的地，也不能保证可在接收侧按配送侧进行配送的顺序来接收。

在需要上述保证的情况下，通常利用 TCP（传输控制协议，Transport Control Protocol）协议，但由于 TCP 协议通过再次发送来补偿分组的丢失，所以不适合要求实时性的用途。在要求实时性的用途中利用 UDP（用户数据报协议，User Datagram Protocol），但 UDP 与 IP 同样，不保证分组的可靠配送或按顺序的配送。

在图像或声音等实时数据的传送中，由于重视实时性、不允许再次发送的时间，所以即使数据丢失时也不进行再次发送。但是，在接收侧使用电传的数据时，必须按照配送分组的顺序重新排列。

在非专利文献 1 所记载的 RTP（实时传输协议，Realtime Transport Protocol）中，忽视了分组的丢失，但在标题中包含表示分组配送顺序的 16 位的顺序号，以便在接收侧可按照配送顺序容易地重新排列分组。另外，同样地，通过在标题中包含表示时刻信息的时间标记，可以在配送侧和接收侧之间取得时刻同步。

另外，在作为现有技术的非专利文献 2 中，提供了一种对 RTP

分组中除了标题以外的有效负荷部分进行加密的装置。这里，使用加密密钥和 RTP 标题中包含的顺序号等信息，并利用 AES（改进的加密标准，Advanced Encryption Standard）计数模式来生成加密密钥流，并通过计算其与有效负荷部分的异或来进行加密。

非专利文献 1: IETF Standard RFC 1889 RTP: A Transport Protocol for Real-Time Applications Jan.1996

非专利文献 2: IETF Standard RFC 3711 The Secure Real-time Transport Protocol (SRTP) Mar.2004

在上述非专利文献 2 的 RTP 分组的加密中，使用块密码，但实际上用作生成加密密钥流的流密码。在流密码中使用相同的加密密钥流的情况下，具有容易被解读的弱点等，因而存在安全性低的问题。

另外，由于计数模式是比较新的加密模式，所以存在的问题是，现存的加密硬件有可能不支持、不能使用通用的加密硬件。

发明内容

本发明为解决上述问题而作出，其目的在于提供一种数据配送装置和数据通信系统，在不保证可靠地传送数据的通信路径中，可使用通用的加密硬件，来进行安全性高的数据通信。

本发明的数据配送装置具备：分组生成单元，通过分割数据来生成分组，并在标题中附加用于识别所生成的分组的信息；加密密钥共享单元，与数据接收装置之间共享加密密钥；分组加密单元，将由上述分组生成单元生成的分组内部的数据划分成规定的块，使用上述加密密钥共享单元所共享的加密密钥对每个块加密数据，并且，在加密最开始的块时，使用包含在标题中的、用于识别上述分组的信息作为初始向量来进行加密，在加密以后的每一个块时，以利用前一个块的加密结果的加密方式来进行加密；和分组通信单元，经由通信路径将由该分组加密单元加密后的分组配送到上述数据接收装置。

通过本发明，可取得使用通用的加密硬件来进行安全性高的数据通信的效果。

附图说明

图 1 是表示本发明实施方式 1 的数据通信系统的结构的框图。

图 2 是说明本发明实施方式 2 的数据通信系统中的配送服务器的 RTP 分组加密部的 CBC 模式的动作的图。

图 3 是说明本发明实施方式 3 的数据通信系统中的配送服务器的 RTP 分组加密部的 CBC 模式的动作的图。

图 4 是说明本发明实施方式 5 的数据通信系统中的配送服务器的 RTP 分组加密部的 CBC 模式的动作的图。

具体实施方式

(实施方式 1)

图 1 是表示本发明实施方式 1 的数据通信系统的结构的框图。该数据通信系统具备: 按照 RTP 配送图像·声音等数据的配送服务器(数据配送装置)1; 和接收由配送服务器 1 配送的图像·声音等数据的接收客户机(数据接收装置)2。

在图 1 中, 配送服务器 1 具备: RTP 分组生成部(分组生成单元)11、加密密钥共享部(加密密钥共享单元、第 1 加密密钥共享单元)12、RTP 分组加密部(分组加密单元)13 及 RTP 分组通信部(分组通信单元、第 1 分组通信单元)14。另外, 接收客户机 2 具备: RTP 分组通信部(第 2 分组通信单元)21、加密密钥共享部(第 2 加密密钥共享单元)22、RTP 分组解密部(分组解密单元)23 及数据恢复部(数据恢复单元)24。由通信路径 31 连接配送服务器 1 的 RTP 分组通信部 14 和接收客户机 2 的 RTP 分组通信部 21, 由通信路径 32 连接加密密钥共享部 12 和加密密钥共享部 22。

在图 1 的配送服务器 1 中, RTP 分组生成部 11 分割未图示的图像或声音等数据, 生成 RTP 分组, 在 RTP 标题中附加作为用于识别所生成的分组的信息的顺序号或表示时刻信息的时间标记等。加密密钥共享部 12 与接收客户机 2 之间共享加密密钥。

RTP 分组加密部 13 将由 RTP 分组生成部 11 生成的分组内部的

数据划分成规定的块，使用加密密钥共享单元 12 所共享的加密密钥对每个块加密数据，并且，在加密最开始的块时，使用包含在 RTP 标题中的、作为用于识别分组的信息的顺序号作为初始向量来进行加密，在加密以后的每一个块时，以利用前一个块的加密结果的加密方式来进行加密。RTP 分组通信部 14 经由通信路径 31 将由 RTP 分组加密部 13 加密后的 RTP 分组配送到接收客户机 2。

另外，在图 1 的接收客户机 2 中，RTP 分组通信部 21 经由通信路径 31 接收从配送服务器 1 配送的被加密的 RTP 分组。加密密钥共享部 22 与配送服务器 1 之间共享加密密钥。RTP 分组解密部 23 使用加密密钥共享部 22 所共享的加密密钥，对由 RTP 分组通信部 21 接收的 RTP 分组进行解密。RTP 分组解读部 24 从由 RTP 分组解密部 23 解密后的 RTP 分组中恢复原来的图像或声音等数据。

通信路径 31 传送 RTP 分组，该通信路径 31 例如是因特网等 IP 网络。通信路径 32 是传送加密密钥信息的通信路径，可以是与通信路径 31 相同的通信路径，也可以是虽然类似、但是另外的通信路径，也可以是完全不同的通信路径。

下面说明动作。

首先，配送服务器 1 和接收客户机 2 在开始基于 RTP 协议的数据通信之前，通过由相互的加密密钥共享部 12 与加密密钥共享部 22 经由通信路径 32 通信，在不被配送服务器 1 及接收客户机 2 以外的第三方知道其内容的情况下，秘密地共享加密密钥（未图示）。对于共享该加密密钥的手段，这里不作规定，但例如可使用 SSL（安全套接层，Secure Socket Layer），也可使用 MIKEY（多媒体互联网键控，？Multimedia Internet KEYing），也可利用其它手段。另外，加密密钥的生成可在配送服务器 1 侧进行，也可在接收客户机 2 侧进行。

在配送服务器 1 中，RTP 分组生成部 11 分割未图示的所要配送的图像或声音等数据，使其具有固定长度或可变长度的分组大小。要分割的分组大小可根据所要配送的数据的特性来确定，也可根据通信路径 31 的特性来确定，还可根据其它理由来确定。例如，在配送图像

数据时，可以在 1 个 RTP 分组中存储 1 帧的图像数据，在利用 IP 网作为通信路径 31 时，可以分割成 IP 分组的大小是利用通常的 IP 网进行通信时的标准的 1500 字节，也可以按其它大小来进行分割。

RTP 分组由 RTP 标题和 RTP 有效负荷构成，RTP 分组生成部 11 在 RTP 有效负荷中存储在上述过程中分割后的所要配送的数据，并在 RTP 有效负荷之前附加包含 16 位的顺序号等的 RTP 标题。

RTP 分组加密部 13 将由 RTP 分组生成部 11 生成的 RTP 分组中的 RTP 有效负荷划分成规定的块，使用加密密钥共享部 12 与接收客户机 2 共享的加密密钥，利用 DES（数据加密标准，Data Encryption Standard）或 AES（改进的加密标准，Advanced Encryption Standard）等公共加密密钥加密方式中、被分类成块加密的加密方式对每个块进行加密。为确保安全性，RTP 分组加密部 13 使用使前一个块的加密结果反映到下一个块的加密中的、例如 CBC（密码块链接，Cipher Block Chaining）模式的加密方式，作为块加密的加密模式。

为了进行以 CBC 模式加密后的数据的通信，在接收侧的接收客户机 2 中进行正常解密、无误地传送全部的块是必要条件。在 IP 网络等以分组为单位进行通信的通信路径 31 中，由于数据的丢失以分组为单位发生，所以在 1 个分组丢失时，为了不使接收侧无法对其后的分组进行解密处理，不能使用前一分组的最后的加密结果作为加密时的初始向量。

因此，在该实施方式 1 中，RTP 分组加密部 13 使用将顺序号填充至达到初始向量的长度后得到的值作为初始向量。由于包含在 RTP 标题中的顺序号是针对每个分组变化的值，并且包含在未加密的 RTP 标题中，所以必定在配送侧和接收侧共享。RTP 分组通信部 14 通过通信路径 31，将由 RTP 分组加密部 13 加密的 RTP 分组配送到接收客户机 2 的 RTP 分组通信部 21。

在接收客户机 2 中，RTP 分组通信部 21 向 RTP 分组解密部 23 输出所接收的、被加密的 RTP 分组。RTP 分组解密部 23 从加密密钥共享部 22 获取与配送服务器 1 之间共享的加密密钥，使用加密密钥和

包含在 RTP 标题中的顺序号，对 RTP 有效负荷进行解密。将解密后的 RTP 分组输出到数据恢复部 24。数据恢复部 24 从由 RTP 分组解密部 23 解密后的 RTP 分组中恢复原来的数据，将数据输出到必需的、未图示的处理部。所谓未图示的处理部，例如，在所配送的数据是图像时为图像解密部及图像显示部，在所配送的数据是声音时为声音解密部及声音再现部。

在该实施方式 1 中，RTP 分组生成部（分组生成单元）11 生成 RTP 分组，RTP 分组加密部（分组加密单元）13 使用包含在 RTP 标题中的顺序号作为初始向量来进行加密，但也可以由分组生成单元生成 IP 分组，由分组加密单元使用包含在 IP 标题中的 ID（标识符）作为初始向量来进行加密，还可以由分组生成单元生成 UDP 分组，由分组加密单元使用包含在 UDP 标题中的 ID（标识符）作为初始向量来进行加密。

如上所述，根据本发明实施方式 1，RTP 分组加密部 12 将由 RTP 分组生成部 11 生成的分组内部的数据划分成规定的块，使用加密密钥共享单元 12 所共享的加密密钥对每个块加密数据，并且，在加密最开始的块时，使用包含在 RTP 标题中的、作为用于识别分组的信息的顺序号作为初始向量来进行加密，在加密以后的每一个块时，以利用前一个块的加密结果的 CBC 模式的加密方式来进行加密，从而可得到的效果是，在 IP 网络等不保证可靠地传送数据的通信路径 31 中，可利用通用的加密硬件来进行安全性高的数据通信。

（实施方式 2）

表示本发明实施方式 2 的数据通信系统的结构的框图与上述实施方式 1 的图 1 相同。在上述实施方式 1 中，利用包含在 RTP 标题中的顺序号作为初始向量，但在本发明实施方式 2 中，使用对顺序号进行加密后得到的值作为初始向量。

图 2 是说明本发明实施方式 2 的数据通信系统中的配送服务器的 RTP 分组加密部的 CBC 模式的动作的图。在图 2 中，明文块 41 是按块大小来划分 RTP 有效负荷后形成的最开始的明文块，明文块 42 是

按块大小来划分RTP有效负荷后形成的第2个明文块。密码块43是对明文块41进行加密后的结果，密码块44是对明文块42进行加密后的结果。异或计算部45a、45b、45c用于计算2个输入的异或，在图中为了方便说明图示了3个，但也可以由1个硬件构成。加密部46a、46b、46c使用加密密钥共享部12所共享的加密密钥进行加密，在图中为了方便说明图示了3个，但也可以由1个硬件构成。

另外，在图2中，顺序号47是将包含在RTP标题中的顺序号填充至达到与明文块41或明文块42相同大小后得到的值。初始向量48是配送服务器1和接收客户机2中共享的规定值的初始向量。密码块49是对顺序号47与初始向量48的异或计算结果进行加密后的结果，相当于在上述实施方式1中使用的初始向量。即，在本实施方式2中，使用对顺序号47进行加密后得到的值作为初始向量。

下面说明动作。

首先，异或计算部45a计算顺序号47与规定值的初始向量48的异或后输出到加密部46a。加密部46a使用加密密钥共享部12所共享的加密密钥进行加密，输出密码块49。

其后的异或计算部45b的处理与将密码块49视为初始向量时的、通常的CBC模式相同。异或计算部45b计算明文块41与密码块49的异或后，输出到加密部46b。加密部46b使用加密密钥共享部12所共享的加密密钥进行加密，输出密码块43。接着，异或计算部45c计算明文块42与密码块43的异或，输出到加密部46c。加密部46c使用加密密钥共享部12所共享的加密密钥进行加密，输出密码块44。

RTP分组加密部13连续进行这样的处理，直到对未图示的RTP有效负荷进行划分后形成的最后一个明文块为止，从而输出从密码块49开始到未图示的最后一个密码块为止的密码块。除了其中的密码块49之外，RTP分组加密部13联结全部的密码块，并存储在RTP有效负荷中。

接收客户机2的RTP分组解密部23通过进行与配送服务器1的

RTP 分组加密部 13 相反的处理，得到联结了从明文块 41 开始到未图示的最后一个明文块为止的明文块的明文数据。

这里，作为规定值的初始向量 48，必定可以使用值 0，也必定可以使用除 0 以外的固定值，还可以在配送服务器 1 和接收客户机 2 之间秘密地共享与加密密钥同样地随机确定的值。

在本实施方式 2 中，在使用值 0 或固定值作为初始向量 48 时，可以使在配送服务器 1 和接收客户机 2 之间秘密共享的值仅为加密密钥，而且，与上述实施方式 1 相比，可提高安全性。另外，在秘密共享随机值作为初始向量 48 时，可进一步提高安全性。在任意一种情况下，从图 2 可知，即使通过实施方式 2 追加处理，由于进行与通常的 CBC 模式相同的处理，所以可使用基于通用的 CBC 模式的加密硬件。

如上所述，根据本实施方式 2，可取得与上述实施方式 1 相同的效果，并且，由于 RTP 分组加密部 13 使用对顺序号进行加密后得到的值作为初始向量来进行加密，还得到可进一步提高安全性的效果。

（实施方式 3）

表示本发明实施方式 3 的数据通信系统的结构的框图与上述实施方式 1 的图 1 相同。在本实施方式 3 中，RTP 分组加密部 13 使用对顺序号进行扩展后形成的扩展顺序号作为初始向量来进行加密。

图 3 是说明本发明实施方式 3 的数据通信系统中的配送服务器的 RTP 分组加密部的 CBC 模式的动作的图。在图 3 中，扩展顺序号 50 是将包含在标题 RTP 中的 16 位顺序号扩展到任意长度后形成的，其他的符号 41～49 与图 2 相同。

由于 RTP 的顺序号是 16 位的值，所以在配送了顺序号为 65535 的分组后，顺序号循环为 0。利用任意位数的计数器对循环的次数进行计数，将联结了该计数器的值和顺序号的值用作扩展顺序号 50。通过适当设定该计数器的位数，可将在 2 个以上的 RTP 分组的加密中使用同一初始向量的可能性降低到可忽视的程度。

下面说明动作。

异或计算部 45 a 计算扩展顺序号 50 与规定值的初始向量 48 的异

或后输出到加密部 46a。加密部 46a 使用加密密钥共享部 12 所共享的加密密钥进行加密，输出密码块 49。其后的处理与上述实施方式 2 相同，为通常的 CBC 模式。

另外，就该计数器的值而言，有必要在配送服务器 1 及接收客户机 2 之间共享，但也可通过存储在 RTP 分组的扩展标题中来配送，也可在配送服务器 1 及接收客户机 2 中分别独立地设置该计数器，并且分别独立地计数。

这里，为说明本发明实施方式 3 的效果，考虑存在可更换在通信路径 31 上传送的数据的、未图示的第三方的情况。

在上述实施方式 1 及上述实施方式 2 的数据通信系统中，在未图示的第三方更换了配送服务器 1 所配送的数据的情况下，接收客户机 2 有时不能识别出数据被更换。即，第三方记录 16 位顺序号循环一次期间的所有 RTP 分组，将第二次循环以后的 RTP 分组更换成所记录的第一次循环的 RTP 分组后配送。在接收客户机 2 的 RTP 分组解密部 23 中，如果顺序号 47、初始向量 48 以及未图示的加密密钥一致，则可正常解密，所以不能检测出被更换的情况。另一方面，在本实施方式 3 中，通过扩展顺序号，在实际应用时顺序号不循环，从而可防止如上所述的攻击。

如上所述，根据本实施方式 3，可得到与上述实施方式 2 相同的效果，并且，密码块 49 的值更加难以猜测，从而可防止如上所述的攻击，因而与上述实施方式 2 相比，可得到可进一步提高安全性的效果。

另外，在本实施方式 3 中，对扩展顺序号 50 进行加密，但与上述实施方式 1 相同，也可不进行加密。

（实施方式 4）

表示本发明实施方式 4 的数据通信系统的结构的框图与上述实施方式 1 的图 1 相同。另外，说明配送服务器的 RTP 分组加密部的 CBC 模式的动作的图与上述实施方式 3 的图 3 相同。在本实施方式 4 中，对于上述实施方式 3 的扩展顺序号，使用随机设定的值作为上述计数器的初始值，在配送服务器 1 和接收客户机 2 之间秘密共享该值，并

独立地计数。

如上所述，根据本实施方式4，可得到与上述实施方式3相同的效果，并且通过使扩展顺序号的一部分为秘密，即使在假设利用相同的密钥进行多个数据配送的情况下，也可得到如上述实施方式3所述的、防止介于通信路径上的第三方的攻击的效果。

（实施方式5）

表示本发明实施方式5的数据通信系统的结构的框图与上述实施方式1的图1相同。在本实施方式5中，其特征在于：除上述实施方式1～上述实施方式4中使用的顺序号47或扩展顺序号50之外，还利用包含在RTP标题中、表示时刻信息的时间标记。

图4是说明本发明实施方式5的数据通信系统中的配送服务器的RTP分组加密部的CBC模式的动作的图。在图4中，异或计算部45d计算2个输入的异或，加密部46d使用未图示的加密密钥进行加密，时间标记51表示时刻信息、并包含在RTP标题中，密码块52是对时间标记51与规定的初始向量48的异或进行加密的结果。其他的符号41～50与图3相同。

下面说明动作。

异或计算部45d计算时间标记51与规定的初始向量48的异或，输出到加密部46d。加密部46d使用加密密钥共享部12所共享的加密密钥进行加密，输出密码块52。以后的动作与图3相同。

如上所述，根据本实施方式5，可得到与上述实施方式3相同的效果，并且通过使用表示时刻信息的时间标记51作为加密时使用的值，可得到的效果是，可进一步提高安全性，并且，可使用以通用的CBC模式进行加密的硬件。

另外，在本实施方式5中，采用图4的结构，利用扩展顺序号50和时间标记51来进行加密，但也可采用上述实施方式3的图3的结构，将扩展顺序号50替换成联结了顺序号47和时间标记51的扩展顺序号，并以初始向量48的异或的加密结果作为密码块49。

另外，在本实施方式5中，利用扩展顺序号50和时间标记51来

加密数据，但也可利用顺序号 47 和时间标记 51 来加密数据。

并且，在本实施方式 5 中，对扩展顺序号 50 和时间标记 51 进行加密，但也可以与上述实施方式 1 相同，不进行加密。

图1

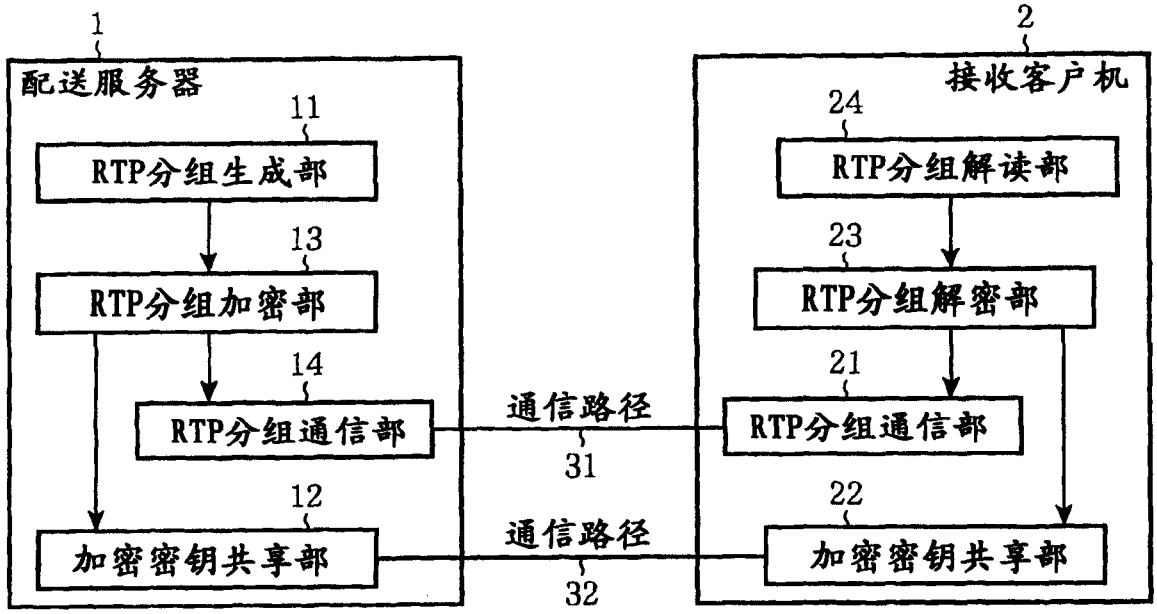

1
配送服务器
11
RTP分组生成部
13
RTP分组加密部
14
RTP分组通信部
12
加密密钥共享部
通信路径
31
通信路径
32
2
接收客户机
24
RTP分组解读部
23
RTP分组解密部
21
RTP分组通信部
22
加密密钥共享部

图2

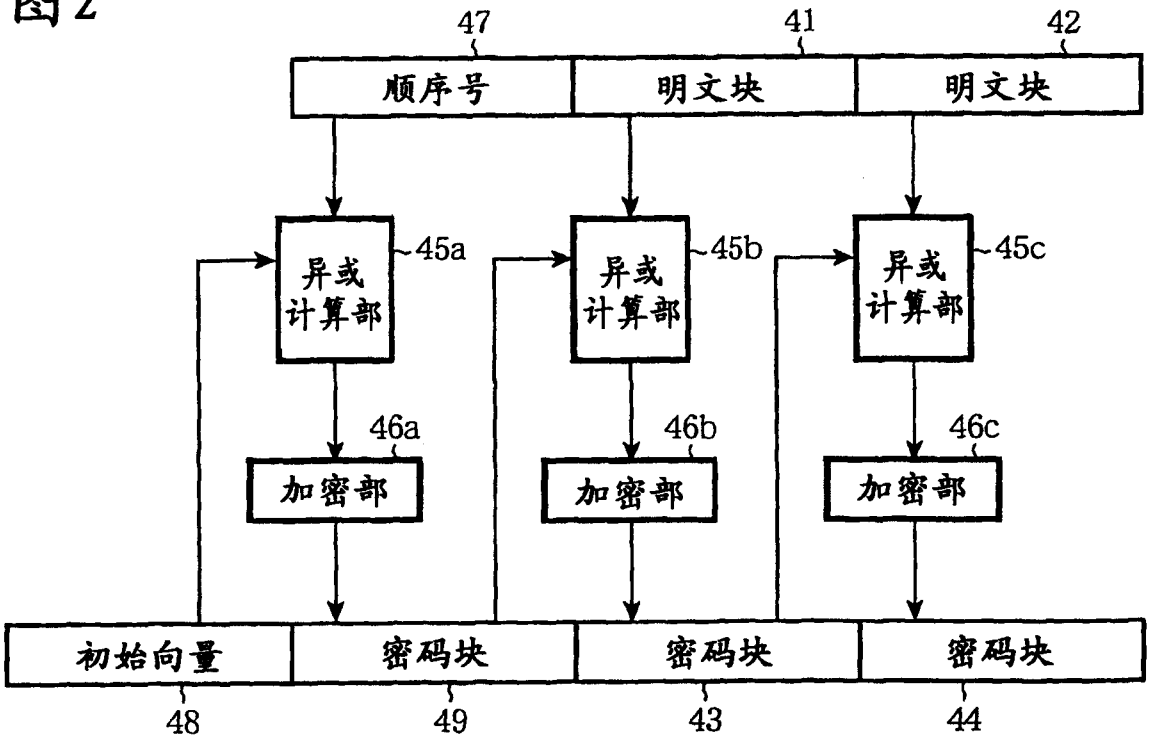

47
41
42
顺序号
明文块
明文块
异或计算部
45a
异或计算部
45b
异或计算部
45c
46a
加密部
46b
加密部
46c
加密部
初始向量
密码块
密码块
密码块
48
49
43
44

图 3

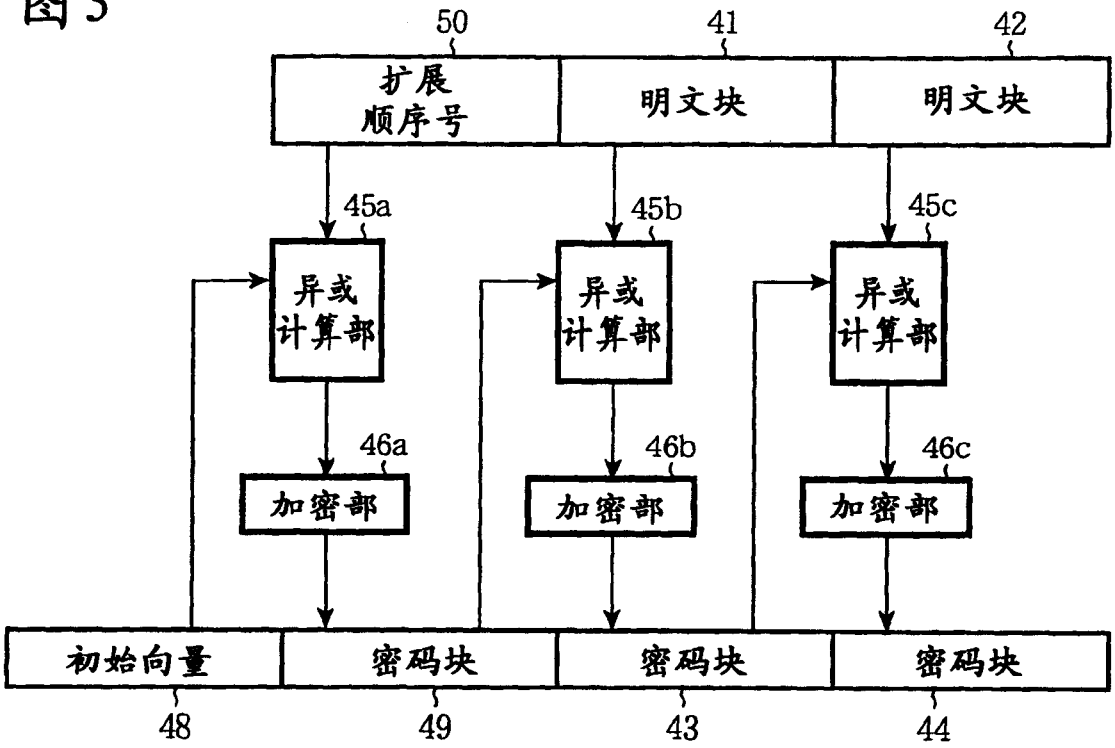
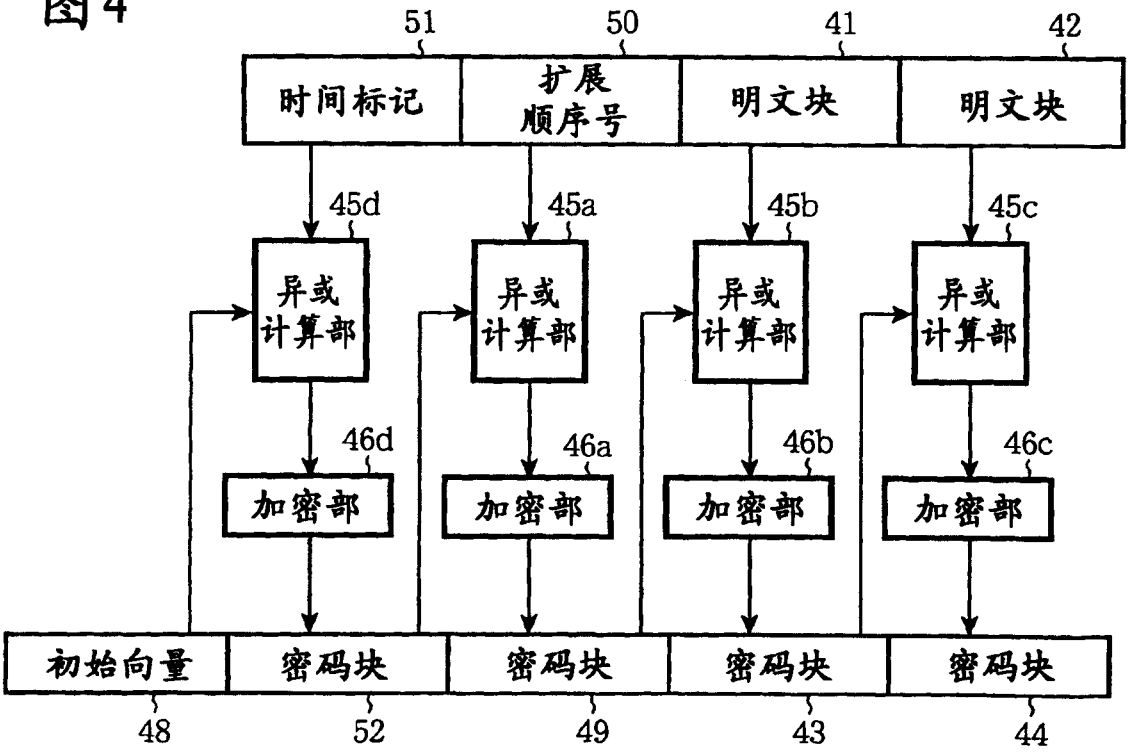

50
41
42
扩展
顺序号
明文块
明文块
45a
45b
45c
异或
计算部
异或
计算部
异或
计算部
46a
46b
46c
加密部
加密部
加密部
初始向量
密码块
密码块
密码块
48
49
43
44

图 4


51
50
41
42
时间标记
扩展
顺序号
明文块
明文块
45d
45a
45b
45c
异或
计算部
异或
计算部
异或
计算部
异或
计算部
46d
46a
46b
46c
加密部
加密部
加密部
加密部
初始向量
密码块
密码块
密码块
密码块
48
52
49
43
44