

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 9/30 (2006.01)  
H04L 29/06 (2006.01)  
H04L 12/28 (2006.01)



# [12] 发明专利申请公布说明书

[21] 申请号 200710184948.7

[43] 公开日 2008年5月7日

[11] 公开号 CN 101174946A

[22] 申请日 2007.10.30

[21] 申请号 200710184948.7

[30] 优先权

[32] 2006.10.30 [33] JP [31] 2006-294339

[71] 申请人 株式会社日立制作所

地址 日本东京

[72] 发明人 幸松孝宪 冈本宏夫

[74] 专利代理机构 北京纪凯知识产权代理有限公司  
代理人 龙 淳

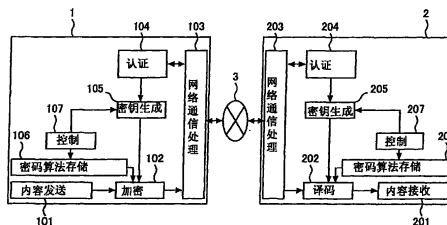
权利要求书 2 页 说明书 12 页 附图 7 页

## [54] 发明名称

内容发送装置、内容接收装置和内容加密方法

## [57] 摘要

本发明提供一种内容发送/接收装置和内容加密方法。发送装置(1)的密码算法存储部(106)存储多个密码算法。密钥生成部(105)根据接收装置(2)的认证结果生成密钥信息。控制部(107)从密码算法存储部选择一个密码算法,从密钥信息中取得密钥,提供给加密部。加密部(102)利用提供的密码算法和密钥,将内容加密。如果生成的密钥信息为有效的期间,则每当发送的内容切换时,从密码算法存储部选择不同的密码算法,从密钥信息中取得不同的密钥并将其加密。



1. 一种内容发送装置，通过网络向其它接收装置发送内容，其特征在于，具有：

向所述接收装置发送内容的内容发送部；

利用被提供的密码算法和密钥，将发送的内容加密的加密部；

存储在加密中使用的多个密码算法的密码算法存储部；

根据所述接收装置的认证结果，生成在加密中使用的密钥信息的密钥生成部；和

从所述密码算法存储部选择一个密码算法，从所述密钥信息中取得在该密码算法中使用的密钥，提供给所述加密部的控制部。

2. 如权利要求1所述的内容发送装置，其特征在于，如果所述密钥生成部生成的密钥信息为有效期间，则所述控制部每当向所述接收装置发送的内容切换时或者每当发送规定时间或规定大小的内容时，从所述的密码算法存储部选择不同的密码算法，从所述密钥信息中取得在该密码算法中使用的密钥，提供给所述加密部。

3. 如权利要求1所述的内容发送装置，其特征在于，当存在多台所述接收装置，在向第一接收装置发送内容的过程中，从第二接收装置接收到发送内容的请求时，如果所述密钥生成部生成的密钥信息为有效期间，则所述控制部为了对向所述第二接收装置发送的内容进行加密，从所述的密码算法存储部选择不同的密码算法，从所述密钥信息中取得在该密码算法中使用的密钥，提供给所述加密部。

4. 如权利要求1所述的内容发送装置，其特征在于，当从所述密码算法存储部选择不同的密码算法时，所述控制部从所述密钥信息中取得不同的密钥作为在该密码算法中使用的密钥，提供给所述加密部。

5. 如权利要求 1 所述的内容发送装置，其特征在于，当向所述接收装置发送已加密的内容时，在该内容中附加在加密中使用的密码算法的种类和有关从所述密钥信息中取得密钥时的取得位置的加密信息并进行发送。

6. 一种内容接收装置，通过网络从其它发送装置接收内容，其特征在于，具有：

从所述发送装置接收内容的内容接收部；

利用被提供的密码算法和密钥，对已接收的内容进行译码的译码部；

存储在译码中使用的多个密码算法的密码算法存储部；

根据所述发送装置的认证结果，生成在译码中使用的密钥信息的密钥生成部；和

根据附加在所述已接收内容中的加密信息，从所述密码算法存储部选择规定的密码算法，从所述密钥信息中取得规定的密钥，提供给所述译码部的控制部。

7. 一种内容加密方法，其为从发送装置向接收装置将内容加密并进行发送时的内容加密方法，其特征在于，

根据所述发送装置和所述接收装置的认证结果，生成在加密中使用的密钥信息；

从多个密码算法中选择一个密码算法；

从所述密钥信息中取得在该被选择的密码算法中使用的密钥；

并且

使用所述选择的密码算法和所述取得的密钥，将发送的内容加密。

## 内容发送装置、内容接收装置和内容加密方法

### 技术领域

本发明涉及在通过网络发送和接收图像声音等内容时，适宜于对内容的著作权进行保护的内容发送装置、接收装置和加密方法。

### 背景技术

近年来，随着数字 AV 机器的普及，提出了对从数字播放等接收的数字图像声音信息（以下简称为“内容”）进行录像，通过家庭用 LAN（局域网）将内容发送至其它 AV 机器，可以在住宅内的其它机器上视听该内容的系统。在这种情况下，发送和接收的数字内容多为著作权保护的對象，因此需要一种防止在传送中被第三者不正当盗听的技术。例如，当在数字 AV 机器之间发送内容时，通过在发送装置上进行加密并在与接收装置之间共有译码用的信息，利用作为发送目的地的内容接收装置以外的机器无法不正当地读出内容的方式，实施有防止违法复制的复制保护。

关于这时的加密处理，在特开 2000-287192 号公报中公开了为了不但在 IEEE1394 上，而且在因特网等网络上的数字内容流通中扩张复制保护技术，作成包含加密的属性信息的密码扩张头（header），与内容一起送出的技术。

另外，在日本特开 2001-358706 号公报中，公开了为了可靠地进行再现次数等的解读限制信息的更新，防止数字内容的不正当解读，用时变密钥使解读限制信息加密，在机密保护的狀態下，与发送接收机器共有的技术。

在上述现有的技术中，当利用网络传递内容时，内容的加密使用相同的密码方式进行。即：每当在发送和接收开始时，在发送和接收机之间对互相的机器进行认证，在这些机器连接的期间内使用相同的密码方式（密码密钥）。在这种情况下，在传送中一旦被第三者解读密码密钥，其后传送的内容就会被完全读取，危害扩大。另外，在将相

同内容发送至多台接收机器的情况下，如果对各个接收机器的内容的密码密钥共同的话，同样危险。为了防止这种危险，在内容传送中将密码密钥变更一点即可，但当每次进行机器认证时，必需作成新的密钥，由于传送中断，所以不实用。另外，每当对相同内容的发送目的地的接收机器进行密码密钥变更时，希望可以高效率地实行。

### 发明内容

本发明的目的在于提供一种当将内容加密传送时，将由不正当盗听而引起的危害限制到最小，同时可迅速而简单地进行密码方式的处理的技术。

本发明的内容发送装置，通过网络向其它接收装置发送内容，其特征在于，包括：

向接收装置发送内容的内容发送部；

利用被提供的密码算法和密钥，将发送的内容加密的加密部；

存储在加密中使用的多个密码算法的密码算法存储部；

根据接收装置的认证结果，生成在加密中使用的密钥信息的密钥生成部；和

从密码算法存储部选择一个密码算法，从密钥信息取得在选择的密码算法中使用的密钥，提供给加密部的控制部。

另外，如果密钥生成部生成的密钥信息为有效期间，则控制部每当向接收装置发送的内容切换时或者每当发送规定时间或规定大小的内容时，从密码算法存储部选择不同的密码算法，从密钥信息取得在选择的密码算法中使用的密钥，提供给加密部。

另外，当存在多台接收装置，在向第一接收装置发送内容的过程中，从第二接收装置接收到发送内容的请求时，如果密钥生成部生成的密钥信息为有效期间，则控制部为了对向第二接收装置发送的内容加密，从密码算法存储部选择不同的密码算法，从密钥信息取得在选择的密码算法中使用的密钥，提供给加密部。

本发明的内容接收装置，通过网络从其它发送装置接收内容，其特征在于，包括：

从发送装置接收内容的内容接收部；

利用被提供的密码算法和密钥，对已接收的内容进行译码的译码部；

存储在译码中使用的多个密码算法的密码算法存储部；

根据发送装置的认证结果，生成在译码中使用的密钥信息的密钥生成部；和

根据附加在已接收内容中的加密信息，从密码算法存储部选择规定的密码算法，从密钥信息取得规定的密钥，提供给译码部的控制部。

本发明的内容加密方法，其为从发送装置向接收装置将内容加密并进行发送时的内容加密方法，其特征在于，

根据发送装置和接收装置的认证结果，生成在加密中使用的密钥信息；

从多个密码算法中选择一个密码算法；

从密钥信息取得在被选择的密码算法中使用的密钥；并且使用选择的密码算法和取得的密钥，将发送的内容加密。

根据本发明，可以迅速而简单地实行密码方式的变更处理，并可将由传送内容的不正当盗听而造成的危害限制到最小。

## 附图说明

本发明的这些以及其它的特点、目的和优点从以下结合附图进行的说明中将会更清楚。其中：

图 1 为表示内容发送接收系统的一个实施例的构成图；

图 2 为表示进行内容传送的住宅内 LAN3 的构成例子的图；

图 3 为表示实施例 1 的内容发送接收的顺序流程的一个示例的图；

图 4 为表示发送多个内容时的加密和译码化的处理的流程图；

图 5 为表示容纳多个密码算法的一个示例的图；

图 6 为表示密钥生成部生成的密钥信息的一个示例的图；

图 7 为表示被加密的内容的格式的一个示例的图；

图 8 为表示实施例 2 的内容发送接收的顺序流程的一个示例的图；

图 9 为表示实施例 3 的内容发送接收系统的构成的图；

## 具体实施方式

以下，利用附图，详细说明本发明的实施方式。

### (实施例 1)

图 1 为表示内容发送接收系统的一个实施例的构成图。在本系统中，内容发送装置 1 和内容接收装置 2 通过 LAN3 互相连接。这个系统，例如相当于从作为内容发送装置 1 的发送接收机将图像声音内容发送至作为内容接收装置 2 的监视器装置的情况。

在内容发送装置 1 中，内容发送部 101 将内容送出至内容接收装置 2。加密部 102 将从内容发送部 101 输出的内容加密。网络通信处理部 103 通过 LAN3 将加密部 102 的输出和认证部 104 的输入输出与其它装置（这里为内容接收装置 2）进行交换。认证部 104 与其它装置之间交换信息，进行装置间的互相认证。密钥生成部 105 根据认证部 104 输出的信息，生成为了在加密部 102 将内容加密所必要的密钥信息。密码算法存储部 106 保存加密用的多个密码算法。控制部 107 从密码算法存储部 106 选择一个密码算法，提供给加密部 102。另外，控制部 107 从密钥生成部 105 生成的密钥信息中取得在上述选择的密码算法中使用的密钥，提供给加密部 102。加密部 102 利用上述提供的密码算法和密钥，将内容加密。

另一方面，在内容接收装置 2 中，网络通信处理部分 203 与其它装置（这里为内容发送装置 1）之间，通过 LAN3 交换对译码部 202 的输入和认证部 204 的输入输出。译码部 202 对从发送装置 1 送出的加密内容进行译码，输出至内容接收部 201。认证部 204 与其它装置之间交换信息，进行装置间的相互认证。密钥生成部 205 根据认证部 204 输出的信息，生成为了在译码部 202 中对内容进行译码所必要的密钥信息。该密钥信息与发送装置 1 的密钥生成部 105 生成的密钥信息相同。密码算法存储部 206 保存用于译码的多个密码算法。该密码算法与发送装置 1 的密码算法存储部 106 保存的密码算法相同。控制部 207 从密码算法存储部 206 选择一个密码算法，提供给译码部 202。另外，控制部 207 从由密钥生成部 205 生成的密钥信息中取得在上述选择的密码算法中使用的密钥，提供给译码部 202。这时，根据附加在内容中的加密信息，提供与在发送装置 1 中选择的密码算法和使用的密钥相

同的信息。译码部 202 使用上述提供的密码算法和密钥，对内容进行译码。

在本实施例中，其特征在于：内容发送装置 1 的密码算法存储部 106 保存多个密码算法，对于每个发送的内容变更选择密码算法，并从密钥信息中取得加密所用的密钥。另外，在内容接收装置 2 中，其特征在于：密码算法存储部 206 保存与发送侧同样的多个密码算法，以与被发送的内容一致的方式选择密码算法，并从与发送侧同样的密钥信息中取得译码所用的密钥。结果，假设即使发送中的一个内容被第三者盗听，因为下一个内容变更加密条件，难以译解，所以能够将危害控制在最小范围内。

图 2 为表示在装置间进行内容传送用的住宅内 LAN3 的构成例子的图。一台内容发送装置 1 和 2 台内容接收装置 2a、2b 分别通过有线 LAN3 的电缆与网络集线器装置 31 连接。网络集线器装置 31 与路由器 32 连接，再通过调制解调器或光电变换器等与因特网连接。内容发送装置 1，内容接收装置 2a、2b 和路由器 32 分别具有在 LAN 上识别自身的 IP 地址。另外，在制造时，预先将 48 位 MAC（媒体访问控制：Media Access Control）地址分配给各装置的网络通信处理部的接口部。在各装置的 IP 地址的设定中使用在网络地址的自动设定中广泛采用的 DHCP（动态主机配置协议：Dynamic Host Configuration Protocol）。例如，使路由器 32 作为 DHCP 服务器动作，从这里分配各装置的 IP 地址即可。还有，当使用 IPV6（因特网协议版本 6）时，根据被称为无状态自动设定的方法，各装置也可从路由器 32 的 IP 地址的上位 64 位和 MAC 地址决定自身的 IP 地址。采用这种网络结构，各装置能够互相认证对方装置，传送内容。另外，在这个例子中虽然表示了各装置与住宅内 LAN 连接的情况，但并不限于此，还能够扩展为通过因特网与住宅外装置之间进行信息的传送。

图 3 为表示本实施例的内容的发送和接收的顺序（sequence）流程的一个示例的图。

首先，从内容接收装置 2 制作认证请求。将由特定的认证机关生成的接收装置 2 的装置固有的公开密钥和该公开密钥的证书附加到认证请求中，送至内容发送装置 1（S301）。当发送装置 1 收到认证请求



时,将接收确认返回给接收装置 2。接着,从发送装置 1 制作认证请求,与接收装置 2 的情况同样,附加发送装置 1 的固有的公开密钥及其证书,送至接收装置 2 (S302)。接收装置 2 一旦收到认证请求,就将接收确认返回给发送装置 1。

当发送装置 1 从接收装置 2 取得认证请求时,根据规定的公开密钥署名算法,进行接收装置 2 的认证。在认证成功的情况下,发行认证响应,发送至接收装置 2 (S303)。同样,一旦接收装置 2 收到从发送装置 1 发出的认证请求就进行认证,在成功的情况下发行认证响应,并发送至发送装置 1 (S304)。当如上述这样相互认证成功时,各装置互相生成并共有共同的认证密钥。在认证密钥的生成中,能够利用 Diffie-Hellman 等众所周知的密钥交换算法。

当认证密钥的共有结束时,发送装置 1 生成交换密钥和随机数,利用认证密钥分别将交换密钥和随机数加密,发送至接收装置 2 (S305,S306)。这时,也可将交换密钥和随机数集中发送。接收装置 2 利用认证密钥对从发送装置 1 送来的交换密钥和随机数进行译码,保存被译码过的交换密钥和随机数。接着,发送装置 1 和接收装置 2 分别利用交换密钥和随机数,根据预先决定的计算算法生成共同密钥。

当从接收装置 2 向发送装置 1 进行内容的发送请求时 (S307),发送装置 1 选择保存的密码算法,利用上述共同密钥对内容进行加密,发送至接收装置 2 (S308)。在接收装置 2 中,利用上述密码算法和上述共同密钥,对接收的加密内容进行译码。

这里所述的共同密钥为前述的“密钥信息”,因为只是认证完的发送装置 1 和接收装置 2 共有的信息,所以隐秘性高。另外,通过选择密码算法,减轻内容被盗听的担心。下面,就此进行详细说明。

图 4 是表示在图 3 中发送多个内容时的加密、译码的处理流程的图。首先,发送装置 1 和接收装置 2 共有认证处理的结果,和内容的加密与译码中所使用的共同密钥(密钥信息) KK (S400)。共同密钥 KK 具有能够使用的有效期间。并且,在能够有效使用该共同密钥 KK 的期间中,设想依次发送广播节目等多个内容(#1,#2)的情况。

发送装置 1 从接收装置 2 一旦接收到内容(#1)的发送请求(S401),就返回接收响应 (S402)。然后,发送装置 1 从保存在密码算法存储部

106 的多个密码算法中选择一个（例如算法 A），对在密钥生成部 105 生成的共同密钥 KK 的有效范围进行设定。所谓有效范围表示用于从共同密钥 KK 中取得在实际的加密中使用的密钥（K1）的取得位置。接着，加密部 102 利用选择的密码算法和设定的共同密钥的有效范围（密钥 K1），将内容（#1）加密。加密的内容（#1）被依次从网络通信处理部 103 发送（S403）。

当接收装置 2 接收到加密的内容（#1）时，就在译码部 202 中进行译码。为了译码，从密码算法存储部 206 保存的多个密码算法中选择一个（算法 A），对在密钥生成部 205 生成的共同密钥 KK 的有效范围（密钥 K1）进行设定。这时，因为应当选择的密码算法和应当设定的共同密钥的有效范围作为加密信息被附加在接收的内容（#1）中，所以根据它进行选择。

在内容（#1）的发送结束，共同密钥 KK 能够有效使用期间，接着，发送装置 1 从接收装置 2 接收下一个内容（#2）的发送请求（S404），返回接收响应（S405）。然后，发送装置 1 切换到保存在密码算法存储部 106 中的其它密码算法（例如算法 B）并进行选择。并且，对在密钥生成部 105 中生成的共同密钥 KK 的有效范围（密钥 K2）在此进行设定。在这种情况下，密钥 K2 虽然不是必需与以前的密钥 K1 不同，但通过变更安全性会更高。接着，加密部 102 利用变更过的密码算法（算法 B）和共同密钥的有效范围（密钥 K2），对内容（#2）进行加密。加密的内容（#2）被依次从网络通信处理部 103 发送（S406）。

当接收装置 2 接收到被加密过的内容（#2）时，就在译码部 202 进行译码。在这种情况下，因为应当选择的密码算法（算法 B）和应当设定的共同密钥的有效范围（密钥 K2）作为加密信息附加在接收的内容（#2）中，所以根据它进行切换。

接着，就从密码算法存储部 106，206 取得密码算法的方法和从在密钥生成部 105，205 生成的共同密钥（密钥信息）中取得密钥的方法详细地加以说明。

图 5 是表示存储在密码算法存储部 106，206 中的多个密码算法的一个示例的图。项目 501 是密码算法的种类，在此存放有 4 种密码算法（算法 A，B，C，D）。项目 502 是使用各密码算法时必需的密钥的

密钥长度（位数），表示分别使用不同密钥长度（128，128，61，192 位）的密钥。

即，在为了对内容进行加密和译码，从密码算法存储部 106，206 选择算法 A 的情况下，控制部 107，207 必需从在密钥生成部 105，205 生成的密钥信息中取得密钥长度为 128 位的密钥。

图 6 为表示密钥生成部 105,205 生成的密钥信息的一个示例的图。在这个例子中，密钥信息 600 的位长取为 256 位，下面是取得密钥长度为 128 位的密钥的情况。(a) 表示将密钥信息 600 的上位 128 位作为密钥 601 进行分配而取得的情况，(b) 表示将密钥信息 600 的下位 128 位作为密钥 602 进行分配的情况，(c) 表示将密钥信息 600 的任意位置的 128 位作为密钥 603 进行分配的情况。这样，参照相同的密钥信息 600，通过改变其取得位置，就能够简单地生成完全新的密钥。

当从密码算法存储部 106 选择例如图 5 的算法 A 时，内容发送装置 1 的控制部 107 从在密钥生成部 105 生成的密钥信息 600 中取得例如图 6 (a) 的上位 128 位的密钥 601。然后，将取得的密码算法 A 和密钥 601 提供给加密部 102。加密部 102 利用算法 A 和密钥 601 将从内容发送部 101 输出的内容加密。在内容接收装置 2 中，按同样的顺序使用算法 A 和密钥 601 进行译码。

图 7 是表示从内容发送装置 1 发送向内容接收装置 2 的被加密过的内容的格式的一个示例的图。在发送内容中附加有将加密信息记述在加密内容 700 中的密码头 (header) 710。在密码头 710 中包含密码算法的种类 711，和表示用于取得密钥的取得位置的开始位 712 和结束位 713 的信息。密码算法的种类 711 识别存放在密码算法存储部 106，206 中的密码算法。例如，可以将“0x01”定义为算法 A，将“0x02”等定义为算法 B。开始位 712 和结束位 713 表示在图 6 的密钥信息 600 中分配哪个范围作为密钥。如果是图 6 (a) 的情况，因为使用密钥信息 600 的上位 128 位，所以将开始位 712 记述为“0”，结束位 713 记述为“127”。在密码头 710 中作为其它的密码信息，也可以包含例如“Copy Never”“Copy once”这样的复制限制信息或密码头 710 被有效使用的加密内容长度等。

当内容接收装置 2 接收到内容时，就对上述密码头 710 的加密信

息进行分析, 根据该信息对加密内容进行译码。控制部 207 根据密码算法种类 711 的信息, 从密码算法存储部 206 取得规定的密码算法。另外, 根据开始位 712 和结束位 713 的取得位置的信息, 从密钥生成部 205 所生成的密钥信息中取得规定密钥, 提供给译码部 202。译码部 202 使用上述密码算法和上述密钥, 对在网络通信处理 203 中接收的被加密过的内容进行译码, 输向内容接收部 201。

这样, 在本实施例中, 在每次切换发送的内容时, 变更密码算法。并且, 通过变更共同密钥(密钥信息)的有效范围(取得位置), 加密中使用的密钥在实效上与使用完全新的密钥的情况有同样的效果。在现有的方法中, 每当请求发送内容时, 必须在装置间进行认证处理, 生成新的共同密钥。因此, 有时因内容的发送开始延迟而不得不中断。与此相对, 在本实施例中, 对于密码算法和密钥的变更, 不进行装置间的新的认证处理就能够迅速而简单地进行。另外, 通过在每个内容中变更加密方式, 能够更安全地发送内容。

在本实施例中, 虽然将变更密码算法的时机设定在切换发送的内容(节目)的时刻, 但不限于此, 也可以设定为将内容的形式例如从 MPEG 文件等图像文件切换为 JPEG 等图像文件的时刻。另外, 也可以在发送完规定时间的内容的时刻或发送完规定大小的内容的时刻进行密码算法的变更。

#### (实施例 2)

本实施例为在图 2 的传送系统中, 将内容从内容发送装置 1 发送至多个内容接收装置 2a、2b 的情况。

图 8 为表示本实施的内容发送接收的顺序流程的一个示例的图。在此, 设想在从发送装置 1 向接收装置 2a 进行加密内容发送时, 存在从其它的接收装置 2b 向发送装置 1 的内容发送要求的情况。即: 在发送装置 1 和接收装置 2a 之间的共同密钥在有效期内, 而且向接收装置 2b 发送的情况。

首先, 发送装置 1 从接收装置 2a 接收内容的发送要求 (S801)。在发送装置 1 和接收装置 2a 之间进行认证处理, 如果认证成功, 互相生成共同密钥(密钥信息) KK (S802)。发送装置 1 选择算法 A, 使用从共同密钥 KK 取得的密钥 ka, 对内容进行加密, 发送至接收装置

2a (S803)。接收装置 2a 接收该加密内容, 利用算法 A 和从共同密钥 KK 取得的密钥 ka 对内容进行译码。在此, 发送装置 1 和接收装置 2a 的密码算法的选择和密钥的取得以及加密信息的传递与实施例 1 的情况相同地进行。

其次, 在向接收装置 2a 发送的过程中, 发送装置 1 从其它的接收装置 2b 接收到内容的发送要求 (S804)。在发送装置 1 和接收装置 2b 之间进行认证处理, 如果认证成功, 生成与在上述接收装置 2a 之间共有的共同密钥相同的共同密钥 (密钥信息) KK (S805)。这可将生成相同的共同密钥 KK 的信息从发送装置 1 发送至接收装置 2b。另外, 发送装置 1 选择不同的算法 B, 利用从共同密钥 KK 取得的不同的密钥 Kb, 对内容进行加密, 发送至接收装置 2b (S806)。接收装置 2b 接收该加密内容, 利用算法 B 和从共同密钥 KK 取得的密钥 Kb 对内容进行译码。在这种情况下, 密钥 Kb 没必要一定与以前的密钥 Ka 不同, 但通过变更, 安全性更高。

在本实施例中, 在共同密钥有效的期间内, 变更密码算法和密钥, 对内容进行加密, 并传送至作为发送目的地的接收装置 2a 和接收装置 2b。这时, 由认证处理得到的共同密钥 (密钥信息) 具有与发送装置 1, 接收装置 2a 和接收装置 2b 三者都相同的共同密钥。通过使用相同的共同密钥, 和变更从它取得的有效范围 (开始位和结束位), 可以简单地变更密钥。附带说一下, 在现有的发送方法中, 由于使用相同的密码算法和相同的密钥, 对内容进行加密并传送至多个接收装置, 因此与此相比, 在本实施例中, 发送装置可以更安全地传送内容。

### (实施例 3)

图 9 作为上述实施例 1, 实施例 2 的适用例子, 表示从广播接收机将图像声音数据发送至记录器和监视器的内容发送接收系统的结构的图。在该系统中具有作为发送装置的数字广播接收机 10, 作为接收装置 2a 的记录器 20a 和监视器 20b。这些装置通过集线器 31, 利用 IP 网络连接。

数字广播接收机 10 除了图 1 所示的密码处理功能外, 还包括数字发送接收天线 108, 调谐器 109, 译码器 110。在此, 内容发送系统有二个系统。首先, 在进行从数字广播接收机 10 向记录器 20a 发送内容

(图像声音数据)的情况下,利用调谐器 109 选择由天线 108 接收的 MPEG-TS 内容,由加密部 102 进行加密,从网络通信处理部 103 向记录器 20a 发送。另外,在进行从数字广播接收机 10 向监视器 20b 发送内容的情况下,在利用译码器 110 对接收的 MPEG-TS 内容进行译码后,由加密部 102 进行加密,从网络通信处理部 103 向监视器 20b 发送。这时,加密部 102 对二种内容进行加密处理。发送至记录器 20a 的内容为 MPEG 数据,发送至监视器 20b 的内容为基带的数据。两者发送的数据量(带宽)大不相同。

在本实施例中,与上述实施例 2 同样,加密部 102 使发送至记录器 20a 的内容的密码算法和发送至监视器 20b 的内容的密码算法不同,对其进行加密。这时,由于发送至记录器 20a 的内容为数据量少的 MPEG 数据,所以可使用作为复杂的密码算法(重的处理)的例如称为 AES 或 DES 的分组密码。另外,由于发送至监视器 20b 的内容为数据量多的基带的数据,所以使用作为简单的密码算法(轻的处理)的例如流(stream)密码。结果两者的发送的加密后的内容的数据量(带宽)的差缩小,利用共同的接口能够高效率地进行双方的内容的发送。

在现有方式中,对多个发送系统使用相同的密码算法。由此,例如在向记录器 20a 发送加密内容时为正常地发送,但一旦向监视器 20b 发送,处理变重,产生图像不能正常地显示的事态。作为其对策,必需增设分别与记录器 20a 用和监视器 20b 用的数据量相应的二个系统的接口。在本实施例中,通过适当地切换密码算法,对内容进行加密,可以减少接口个数,具有可以高效率地使用效果。

如上所述,根据各实施例,在通过网络的内容传送中,通过当变更传送的内容时或接在内容传送过程中,从其它的装置接收到内容发送要求时,切换选择密码算法,变更从在认证时生成的密钥信息取得的密钥,进行加密,可以更安全地传送加密的内容。变更密码方式的契机不限于此,传送一定时间的内容时或传送一定大小的内容时也可以。这样可将由不正当盗听而造成的危害限制到最小。因为密码方式的变更可从多个密码算法切换和由密钥信息的有效范围设定得到,因此可迅速而简单地实行变更处理。

虽然,已说明了根据本发明的几个实施例,但应理解,在不偏离

---

本发明的范围的条件下，容易变更和修正上述的实施例。因此，本发明不受所示和所描述的细节的限制，而是包括在权利要求书范围内的所有的这种变更和修正。

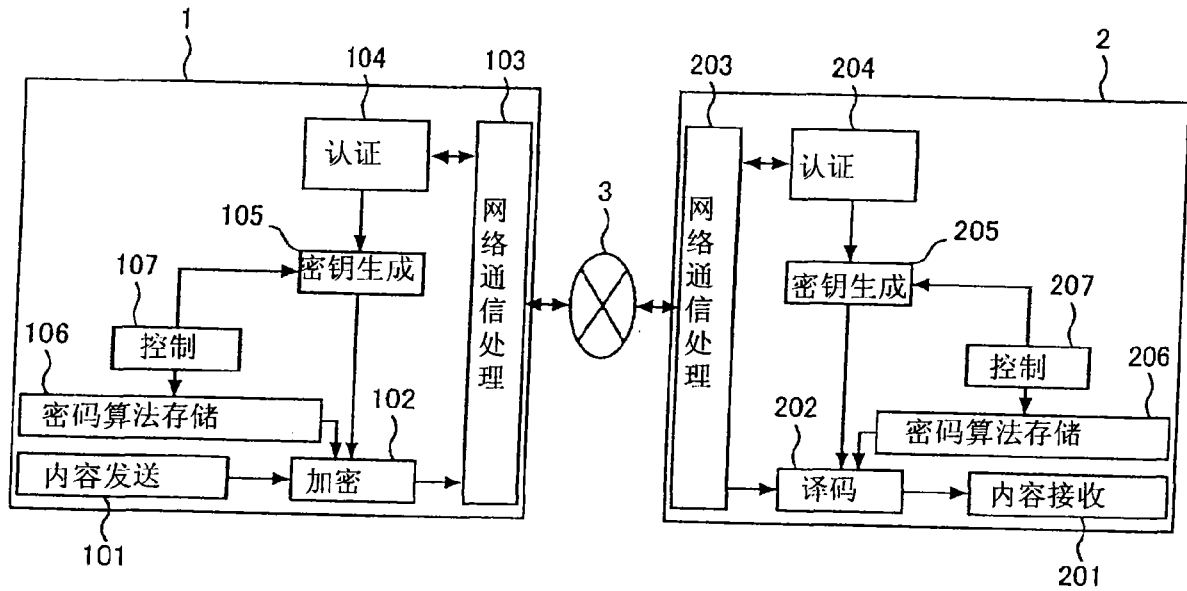


图1

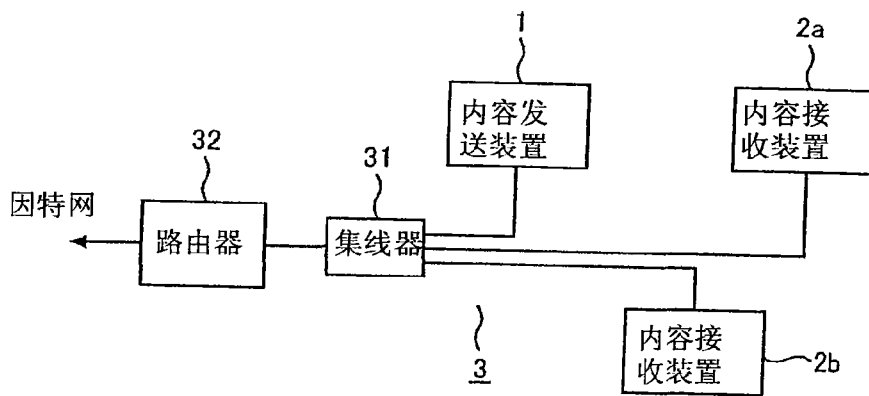


图2





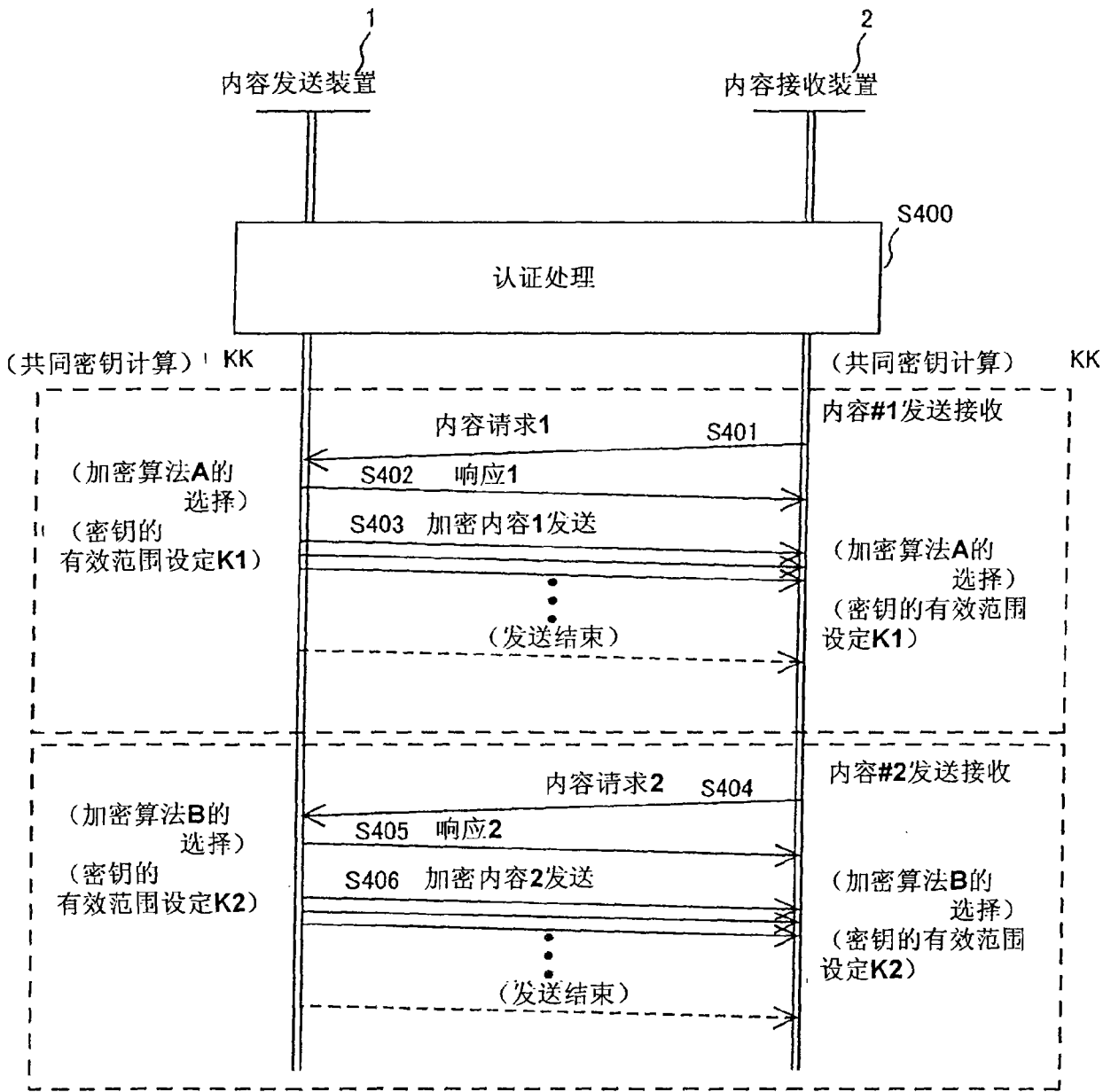
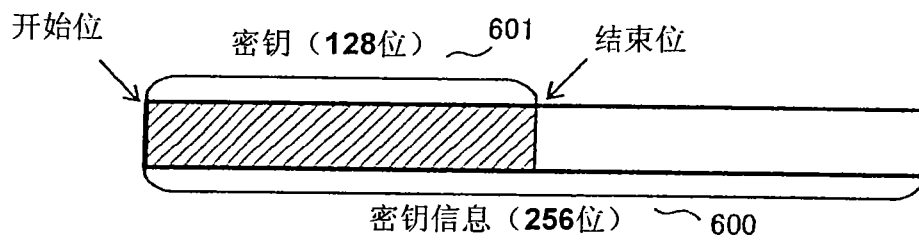


图4

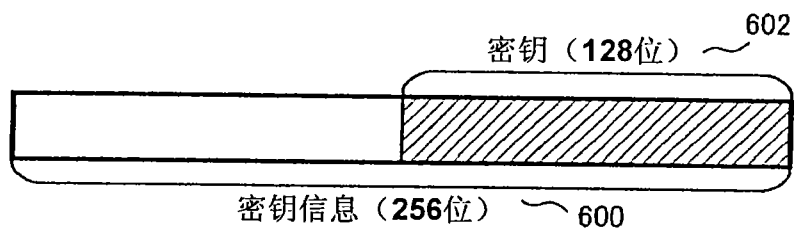
501 密码算法	502 密钥长度
算法A	128位
算法B	128位
算法C	64位
算法D	192位

图5

(a) 当以上位128位为密钥时



(b) 当以下位128位为密钥时



(c) 当以任意128位为密钥时

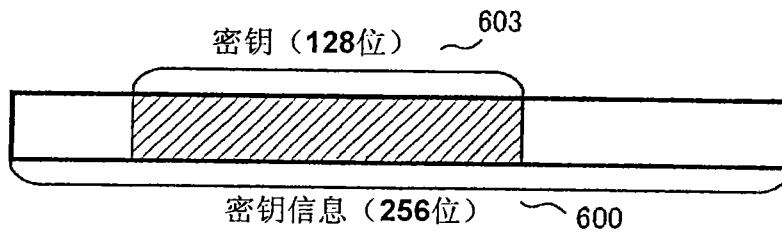


图6

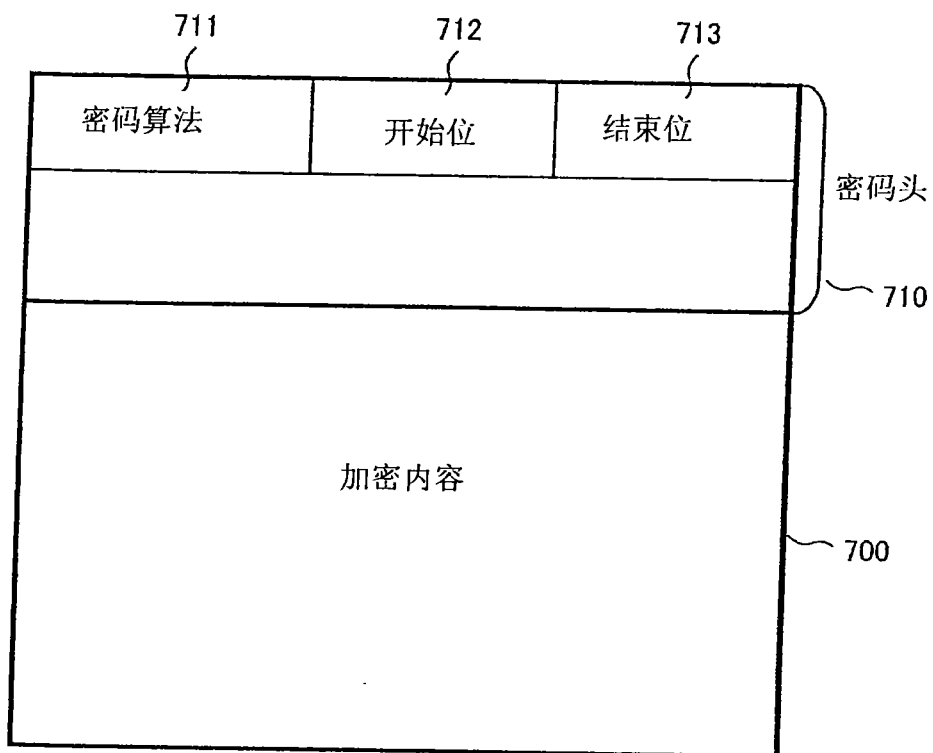


图7

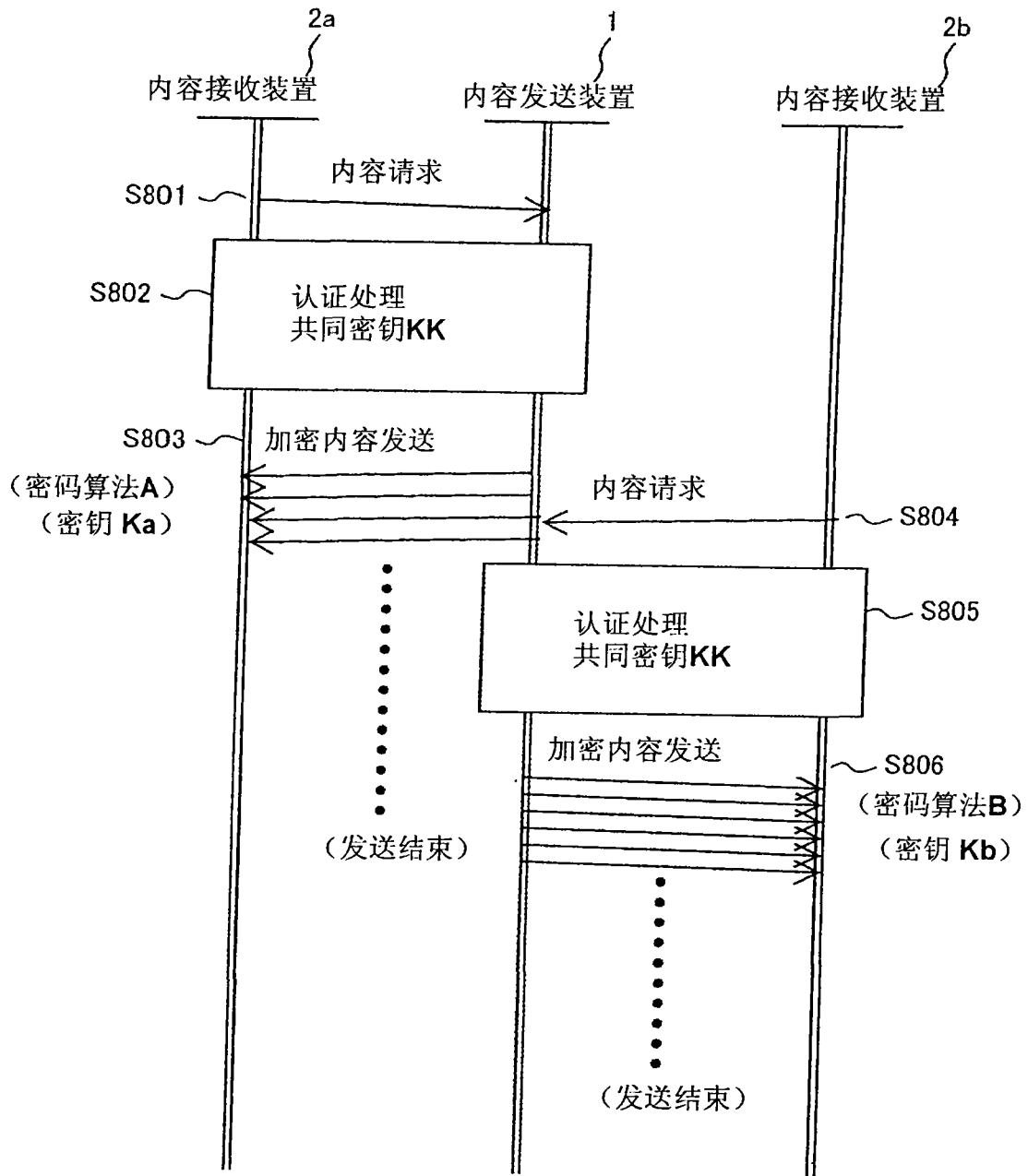


图8

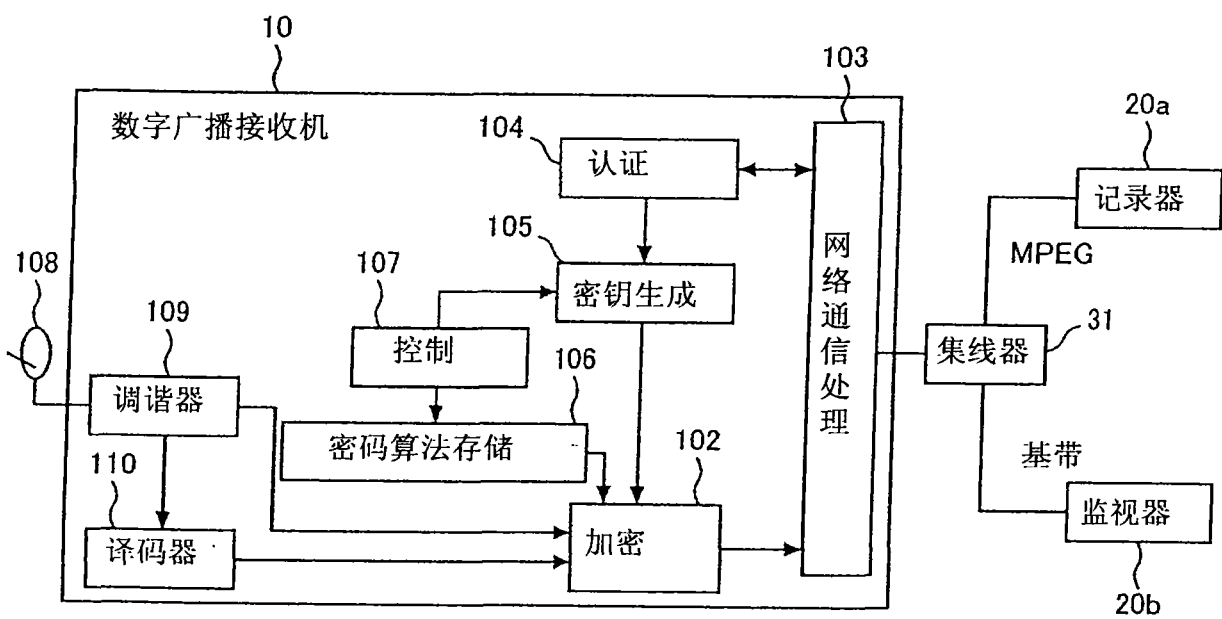


图9