(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 102843588 A
(43)申请公布日 2012.12.26

(21)申请号 201210376604.7

(22)申请日 2012.09.29

(71)申请人 金纯
地址 401100 重庆市沙坪坝区政法一村 14 号 5-2

(72)发明人 金纯

(51)Int.Cl.
H04N 21/266(2011.01)
H04N 21/8358(2011.01)
H04N 21/434(2011.01)

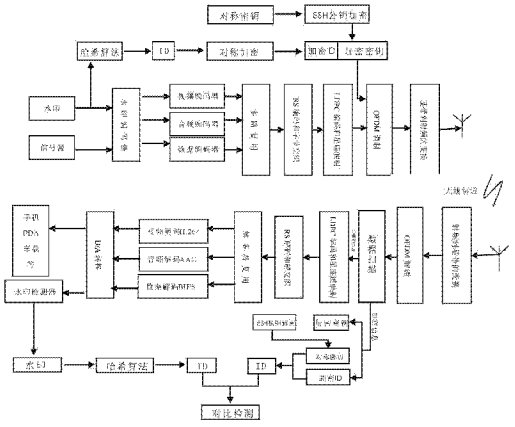
权利要求书 1 页 说明书 6 页 附图 2 页

(54)发明名称

一种基于水印技术 CMMB 播放系统入侵检测系统及方法

(57)摘要

本发明涉及 CMMB 视频广播信息的检测应用领域，尤其涉及基于水印技术的 CMMB 广播检测系统级方法。步骤如下：步骤 1、嵌入水印：CMMB 广播信息数据变换到变换域，将水印嵌入 CMMB 广播信息中；步骤 2、发送信息：将嵌入水印的 CMMB 广播信息通过 CMMB 发射系统处理后发送；步骤 3、信息接收：CMMB 接收端接收到发射端的广播信息，处理后提取 CMMB 广播信息和水印信息；步骤 4、水印检测：将步骤 3 提取的水印信息与约定的水印进行对比监测，如果没有监测到水印或监测到的水印有误，触发报警。采用水印信息对 CMMB 信息进行加密，具有隐蔽性、鲁棒性和密匙的唯一性特点，能有效的保证入侵检测的可靠性，能够实现对 CMMB 广播内容实行跟踪认证。



CN 102843588 A

1. 一种基于水印技术 CMMB 播放系统入侵检测方法，其特征在于所述方法步骤如下：

步骤 1、嵌入水印：CMMB 广播信息数据变换到变换域，将水印嵌入 CMMB 广播信息中；

步骤 2、发送信息：将嵌入水印的 CMMB 广播信息通过 CMMB 发射系统处理后发送；

步骤 3、信息接收：CMMB 接收端接收到发射端的广播信息，处理后提取 CMMB 广播信息和水印信息；

步骤 4、水印检测：将步骤 3 提取的水印信息与约定的水印进行对比监测，如果没有监测到水印或监测到的水印有误，触发报警。

2. 一种基于水印技术 CMMB 播放系统入侵检测方法，其特征在于所述方法步骤如下：

步骤 1、嵌入水印：CMMB 广播信息数据变换到变换域，将水印嵌入 CMMB 广播信息中；

步骤 2、水印 ID 加密：将步骤 1 中的水印通过哈希函数运算，生成 ID，采用对称加密算法对 ID 进行加密，生成加密 ID；

步骤 3、密钥加密：将步骤 2 中对称加密的对称密钥采用椭圆算法进行加密，即对应每个 CMMB 接收端设置有一个私钥，采用与各个接收端的私钥相对应的公钥把对称密钥进行加密，每个接收端对应有一个加密对称密钥，多个组成加密对称密钥组，然后将生成的加密对称密钥组和步骤 2 中的加密 ID 打包成一组数据，称作水印密钥包；

步骤 4、发送信息：将嵌入水印的 CMMB 广播信息通过 CMMB 发射系统处理后发送，同时将水印密钥包也向外发送；

步骤 5、信息接收：CMMB 接收端接收到发射端的信息，扫描后将分流出带水印的 CMMB 广播信息和水印密钥包，将水印从 CMMB 信息中提取出来；

步骤 6、水印检测：将步骤 5 中的接收到的水印密钥包，提取出加密 ID 和加密对称密钥组，用接收端唯一的私钥对加密对称密钥组进行解密，解密出该接收端唯一对应能解开的加密对称密钥，获得对称密钥；用对称密匙对加密 ID 进行解密，获得原 ID；将步骤 5 中提取的水印用哈希函数运算生成对比 ID，将解密获得的 ID 和对比 ID 进行比对，检测是否一致，如果检测到有误，或没有检测到 ID，触发报警。

3. 根据权利要求 2 所述的方法，其特征在于对于每个 CMMB 接收端，配有唯一私钥，解密出其对应的公钥的加密信息。

4. 根据权利要求 2 所述的方法，其特征在于所述的哈希函数是密钥池中的选取的同一哈希函数，或者是密钥池中随机选取的哈希函数。

5. 根据权利要求 2 所述的方法，其特征在于所述的水印可以是同一水印，或者采用实时变化的水印。

6. 一种基于水印技术 CMMB 播放系统入侵检测系统，其特征在于包括：

水印嵌入模块，用于将水印嵌入到原始的 CBBM 广播信息中；

水印加密嵌模块，用于对水印进行哈希函数运算，进行对称加密和 SSH 加密；

水印信息解密模块，用于提取接收的加密信息的 ID，并与接收到的水印信息运算后生成的对比 ID 进行比对，检测信息；

报警模块，用于没有监测到水印或监测到的水印有误触发的报警；

视频质量监测装置，用于随时监测水印嵌入 CMMB 信息对视频质量的影响。

一种基于水印技术 CMMB 播放系统入侵检测系统及方法

技术领域

[0001] 本发明涉及 CMMB 视频广播信息的检测应用领域，尤其涉及基于水印技术的 CMMB 广播检测系统及方法。

背景技术

[0002] 数字水印技术其实是一种信息隐藏技术，它的基本思想源于古代的密写术。视频水印是指将与多媒体内容相关或不相关的一些标志信息直接嵌入多媒体内容当中，但不影响原内容的使用价值，并不容易被人的视觉系统察觉或注意到，只有通过专用的水印检测器才可以监测出隐藏的数字水印信息。其具有鲁棒性、安全性、透明性等特征。根据视频水印技术的不同研究领域和不同应用环境，可以有多种不同的分类方法。例如按照水印在不同变换域的研究，可以分为时域水印和频域水印等。而根据视频数据是否被压缩处理，可以分为压缩域与非压缩域的视频水印。

[0003] 水印信息由原始水印图像变换后形成，经过水印编码器将水印信号嵌入到视频数据流当中，在嵌入水印之前，可以先对水印信息进行扰乱、加密处理，以便每次加入的水印信息都不尽相同；在传输过程中，嵌入水印的视频数据流可能会遭受到各种针对视频内容的攻击，同时由于无线传输的特点，会发生衰落、多径干扰、多普勒频移等影响接受信号质量的状况；在接收端，水印解码器先通过相应的水印提取算法将水印提取出来，然后根据密钥对提取到得水印信息进行解密等相应处理，并使用归一化相关系数的数学模型来判定提取出的视频水印与原始嵌入水印的相关性。

[0004] CMMB 是我国推出的无线视频广播技术，在我国的发展已经初具规模。由于无线传播的特点，在传播过程中不仅容易受到各种干扰，而且更容易受到各种攻击。据报道，我国的鑫诺卫星曾多次受到法轮功等敌对势力的攻击，利用我国卫星进行反动宣传，对我国的卫星信息传输、远程教育、电视广播等造成严重影响，影响国家、社会的安定，在国际上损害中国的形象，也影响人民的正常生活。因此，必须采取必要的技术措施，遏制攻击行为。此外，若使用无线传输方式，则可以随时随地的通过无线发射器发射信息，屏蔽真正从基站发来的视频信息，一旦被不法分子破解信息，或是抢占基站等设施，则会严重影响正常信息的通讯，这为一些不法分子从事违法活动创造了契机。

[0005] 然而国内目前制定的关于 CMMB 的标准中，没有包含基于水印技术的 CMMB 安全方面的内容，及其安全机制来实现安全监测。因此. 发展对数字电视播出质量、传输质量和播出内容进行准确、快速的自动监测技术成为广播电视监测业务的当务之急。

[0006] 实现对数字广播视频技术安全监测的同时，应尽可能不影响视频图像的质量或将这种影响降低到最小。同时要考虑到监测系统应简单易行，而且成本要小，因为以后可能将在全国范围内进行大量的部署，成本过高将抑制其发展。监测系统还应有实时性，即随时都可以用来监测所发送的内容是否合法。

[0007] 广播电视监测工作在保障安全播出、加强政府管理、促进事业产业发展中发挥越来越重要的作用。因此建立一套基于水印技术的 CMMB 安全监测系统平台，实现对 CMMB 视

频内容的安全监测是十分必要的。

发明内容

[0008] 本发明针对上述问题，为解决 CMMB 信息安全有效的传输，设计了一种基于水印技术 CMMB 播放系统入侵检测方法和系统。

[0009] 首先在 CMMB 发射模块方面，要实现水印嵌入技术的实现。水印的嵌入技术要求做到嵌入算法简单、复杂度低，同时水印的嵌入不应该对视频质量产生明显的影响。在水印嵌入之前，对水印进行一些简单的处理，如对水印信息进行加密等，可以使水印信息在安全方面更加可靠，而且在传输过程中对于各种有意或无意的攻击有更强的适应能力。

[0010] 在接收测所作的工作与发射模块所作的工作正好相反，要进行水印的提取工作，对提出的水印信息解密并与原水印信息进行比对分析。如果没有监测到水印信息，则 LED 等亮起同时发出报警声音；若监测到水印信息，则对水印信息的完整新及可恢复性等进行分析，如果水印受到连续的严重攻击，发出报警信号。此外还要选择合适的评估规则，对水印的性能的好坏进行评估，对水印的评估监测一般包括两个方面的内容，对叠加水印后的视觉质量优劣进行评测，以及对水印鲁棒性的评测。

[0011] 根据上述要求，一种基于水印技术 CMMB 播放系统入侵检测方法，步骤如下：

步骤 1、嵌入水印：CMMB 广播信息数据变换到变换域，将水印嵌入 CMMB 广播信息中；

步骤 2、发送信息：将嵌入水印的 CMMB 广播信息通过 CMMB 发射系统处理后发送；

步骤 3、信息接收：CMMB 接收端接收到发射端的广播信息，处理后提取 CMMB 广播信息和水印信息；

步骤 4、水印检测：将步骤 3 提取的水印信息与约定的水印进行对比监测，如果没有监测到水印或监测到的水印有误，触发报警。

[0012] 上述方法，只是简单的实现了水印检测技术，但从安全性来说，由于无线信息传输的开放性，很容易被截获并破解。因此需要使用更加安全的加密技术，对信息进一步加密。由此设计了具有加密技术的一种基于水印技术 CMMB 播放系统入侵检测方法，步骤如下：

步骤 1、嵌入水印：CMMB 广播信息数据变换到变换域，将水印嵌入 CMMB 广播信息中；

步骤 2、水印 ID 加密：将步骤 1 中的水印通过哈希函数运算，生成 ID，采用对称加密算法对 ID 进行加密，生成加密 ID；

步骤 3、密钥加密：将步骤 2 中对称加密的对称密钥采用椭圆算法进行加密，即对应每个 CMMB 接收端设置有一个私钥，采用与各个接收端的私钥相对应的公钥把对称密钥进行加密，每个接收端对应有一个加密对称密钥，多个组成加密对称密钥组，然后将生成的加密对称密钥组和步骤 2 中的加密 ID 打包成一组数据，称作水印密钥包；

步骤 4、发送信息：将嵌入水印的 CMMB 广播信息通过 CMMB 发射系统处理后发送，同时将水印密钥包也向外发送；

步骤 5、信息接收：CMMB 接收端接收到发射端的信息，扫描后将分流出带水印的 CMMB 广播信息和水印密钥包，将水印从 CMMB 信息中提取出来；

步骤 6、水印检测：将步骤 5 中的接收到的水印密钥包，提取出加密 ID 和加密对称密钥组，用接收端唯一的私钥对加密对称密钥组进行解密，解密出该接收端唯一对应能解开的加密对称密钥，获得对称密钥；用对称密匙对加密 ID 进行解密，获得原 ID；将步骤 5 中提取

的水印用哈希函数运算生成对比 ID，将解密获得的 ID 和对比 ID 进行比对，检测是否一致，如果检测到有误，或没有检测到 ID，触发报警。

[0013] 对于每个 CMMB 接收端，配有唯一私钥，解密出其对应的公钥的加密信息。对水印进行运算的哈希函数，可以是密钥池中的选取的同一哈希函数，或者是密钥池中随机选取的哈希函数。而采用的水印也可以是同一水印，或者采用实时变化的水印，不断进行更换。

[0014] 一种基于水印技术 CMMB 播放系统入侵检测系统，包含有现有 CMMB 广播系统的发射端和接受端，另外还包括以下模块：

水印嵌入模块，用于将水印嵌入到原始的 CBBM 广播信息中；

水印加密嵌模块，用于对水印进行哈希函数运算，进行对称加密和 SSH 加密；

水印信息解密模块，用于提取接收的加密信息的 ID，并与接收到的水印信息运算后生成的对比 ID 进行比对，检测信息；

报警模块，用于没有监测到水印或监测到的水印有误触发的报警；

视频质量监测装置，用于随时监测水印嵌入 CMMB 信息对视频质量的影响。

[0015] 本发明设计了一种有效的 CMMB 信息入侵检测方法和系统，采用水印信息对 CMMB 信息进行加密，具有隐蔽性、鲁棒性和密匙的唯一性特点，能有效的保证入侵检测的可靠性，能够实现对 CMMB 广播内容实行跟踪认证，及时发现违法插播、乱播现象，并发出报警。系统简单易行，价格低廉，便于推广。同时采用双频道发射数据，进行快速检测，保证数据的实时性，不影响视频图像质量，具有实用性。实现对 CMMB 的安全监测，监测广播频段内是否有非法电台以及是否有不法分子伪造视频信息或者修改原视频信息，同时对监测到得信息及时进行反馈。确保 CMMB 广播视频有一个安全、健康、稳定的播出平台，为广大人民群众提供优质的视频信息，促进社会文化发展、繁荣。

[0016]

附图说明

[0017] 图 1 为 CMMB 安全监测系统结构图；

图 2 为 CMMB 安全监测流程图；

图 3 为发射端原理图；

图 4 为接收端原理图。

具体实施方式

[0018] 下面结合具体实施例和说明书附图对本发明作进一步说明。此处所描述的具体实施例仅用以解释本发明，并不用于限定本发明。

[0019] 实施例：一种基于水印技术 CMMB 播放系统入侵检测方法，步骤如下：

步骤 1、嵌入水印：CMMB 广播信息数据变换到变换域，将水印嵌入 CMMB 广播信息中；

步骤 2、发送信息：将嵌入水印的 CMMB 广播信息通过 CMMB 发射系统处理后发送；

步骤 3、信息接收：CMMB 接收端接收到发射端的广播信息，处理后提取 CMMB 广播信息和水印信息；

步骤 4、水印检测：将步骤 3 提取的水印信息与约定的水印进行对比监测，如果没有监测到水印或监测到的水印有误，触发报警。

[0020] 上述方法，只是简单的实现了水印检测技术，但从安全性来说，由于无线信息传输的开放性，很容易被截获并破解。因此需要使用更加安全的加密技术，对信息进一步加密。由此设计了具有加密技术的一种基于水印技术 CMMB 播放系统入侵检测方法，步骤如下：

步骤 1、嵌入水印：CMMB 广播信息数据变换到变换域，将水印嵌入 CMMB 广播信息中；

步骤 2、水印 ID 加密：将步骤 1 中的水印通过哈希函数运算，生成 ID，采用对称加密算法对 ID 进行加密，生成加密 ID；

步骤 3、密钥加密：将步骤 2 中对称加密的对称密钥采用椭圆算法进行加密，即对应每个 CMMB 接收端设置有一个私钥，采用与各个接收端的私钥相对应的公钥把对称密钥进行加密，每个接收端对应有一个加密对称密钥，多个组成加密对称密钥组，然后将生成的加密对称密钥组和步骤 2 中的加密 ID 打包成一组数据，称作水印密钥包；步骤 4、发送信息：将嵌入水印的 CMMB 广播信息通过 CMMB 发射系统处理后发送，同时将水印密钥包也向外发送；

步骤 5、信息接收：CMMB 接收端接收到发射端的信息，扫描后将分流出带水印的 CMMB 广播信息和水印密钥包，将水印从 CMMB 信息中提取出来；

步骤 6、水印检测：将步骤 5 中的接收到的水印密钥包，提取出加密 ID 和加密对称密钥组，用接收端唯一的私钥对加密对称密钥组进行解密，解密出该接收端唯一对应能解开的加密对称密钥，获得对称密钥；用对称密匙对加密 ID 进行解密，获得原 ID；将步骤 5 中提取的水印用哈希函数运算生成对比 ID，将解密获得的 ID 和对比 ID 进行比对，检测是否一致，如果检测到有误，或没有检测到 ID，触发报警。

[0021] 对于每个 CMMB 接收端，配有唯一私钥，解密出其对应的公钥的加密信息。对水印进行运算的哈希函数，可以是密钥池中的选取的同一哈希函数，或者是密钥池中随机选取的哈希函数。而采用的水印也可以是同一水印，或者采用实时变化的水印，不断进行更换。

[0022] 一种基于水印技术 CMMB 播放系统入侵检测系统，包含有现有 CMMB 广播系统的发射端和接受端，另外还包括以下模块：

水印嵌入模块，用于将水印嵌入到原始的 CBBM 广播信息中；

水印加密嵌模块，用于对水印进行哈希函数运算，进行对称加密和 SSH 加密；

水印信息解密模块，用于提取接收的加密信息的 ID，并与接收到的水印信息运算后生成的对比 ID 进行比对，检测信息；

报警模块，用于没有监测到水印或监测到的水印有误触发的报警；

视频质量监测装置，用于随时监测水印嵌入 CMMB 信息对视频质量的影响。

[0023] 从图 1 和图 2 可知该系统首先将原始 CMMB 视频与经过预处理的水印信息输入到水印编码器进行水印嵌入处理，然后进行基带的 RS 编码和 OFDM 调制处理，将经过基带处理的信号映射为射频信号，通过上行广播信道和上行分发信道发往 CMMB 同步卫星。在接收端将经过地面增补转发网接受到得信号先进行射频到基带的转换，然后进行基带处理，RS 解码 /OFDM 解调等，最后将得到的信息进行小波变换，监测是否含有水印及所含水印与原始水印的相关性，若没有检测到水印或所监测水印与原始水印的相关性低于阀值，则发出报警，并通过网络告知工作人员。该系统是基于视频数字水印技术提出的。

[0024] 水印嵌入：先将水印图像作时域上的变换，目的是对水印信息进行乱序，达到加密的效果。采用基于 Arnold 变换的图像置乱技术：

$$A_N(K):\begin{bmatrix}x'\\y'\end{bmatrix}=\begin{bmatrix}1 & 1\\ 2 & 2+1\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}\bmod N$$

N 表示矩阵的大小，mod 为模运算。数字图像可以看为一个二维矩，经过变换之后图像的像素位置会重新排列，这样图像会显得杂乱无章，从而实现了对图像的置乱加密效果。由于 Arnold 变换具有周期性，如果重复的进行 Arnold 变换，经过一定的次数之后必然会还原出原始图像。比如本文中使用的水印图像大小为 64×64，周期为 48。

[0025] 然后采用 Daubechies 小波变换对原始要嵌入水印的帧图像 X 进行三级小波分解，得到低频分量小波系数 x(LL_3 ,i,j)、水平分量小波系数 x(LH_n,i,j) 、垂直分量小波系数 x(HL_n,i,j) 和对角分量小波系数 x(HH_n,i,j) ， n =1,2,3 ； 参照对嵌入位置的分析，根据水印二值图像在每个采样点的值按下式修改原始视频帧图像底层的垂直分量小波系数 x(HL_3,i,j) 和水平分量小波系数 x(LH_3,i,j) ：

1) 当水印图像采样点(i，j)的值为 0 时：

$$x'(HL_3,i,j)=(x(HL_3,i,j)+x(LH_3,i,j))/2$$

$$x'(LH_3,i,j)=(x(HL_3,i,j)+x(LH_3,i,j))/2+\Delta$$

2) 当水印图像采样点(i，j)的值为 1 时：

$$x'(HL_3,i,j)=(x(HL_3,i,j)+x(LH_3,i,j))/2$$

$$x'(LH_3,i,j)=(x(HL_3,i,j)+x(LH_3,i,j))/2-\Delta$$

其中 X'(i,j) 是嵌入水印图像的小波系数，X(i,j) 是原始视频帧图像的小波系数。此算法根据水印图像采样点的值，修改原始视频帧图像三级小波变换后水平分量小波系数 x(LH_3,i,j) 和垂直分量小波系数 x(HL_3,i,j) ，由于经过小波变换后，帧图像的能量主要集中在低频 LL 子带，高频子带主要是垂直、水平及对角线的边缘信息，含有的能量较少。一般地，人眼的视觉对图像平滑部分细节和细微变化敏感，而对图像边缘或纹理部分的微小变化不太敏感。因此对其修改并不会对原始图像的重构造成大的影响，并且通过对小波系数的修改，使得加水印图像具有很好的健壮性。式中 Δ 是水印嵌入强度，其取值应权衡不可见性和鲁棒性要求， Δ 越大，水印虽越强壮，但是嵌入水印的图像质量就会降低。反之，取值小，图像质量虽提高了，但同时会削弱水印的鲁棒性。在本实验中 Δ 的最佳取值区间为(3.5 ～ 12)。最后，使用修改过之后的水平分量小波系数和垂直分量小波系数进行三级小波重构得到最终的嵌入水印图像。

[0026] 水印的提取过程：提取水印时，也需要对原始视频水印进行分段，在每段视频中先选取特定的嵌入水印的视频帧，对原始已嵌入水印的帧图像进行三级小波分解，得到得到低频分量小波系数 x(LL_3 ,i,j)、水平分量小波系数 x(LH_n,i,j) 、垂直分量小波系数 x(HL_n,i,j) 和对角分量小波系数 x(HH_n,i,j) ， n =1,2,3 ；比较其对应的水平分量小波系数与垂直分量小波系数 x(LH_3,i,j) 和 x(HL_3,i,j) 的差值 Δ，如果 Δ >0，则表示水印图像在该采样点的值为 0，反之，若 Δ <0，表示为 1。根据得到水印信息在各个采样点的值进行组合重构得到嵌入的水印信息，然后将得到的水印信息进行 T-k 次置乱(T 为水印图像的

Arnold 置乱周期，k 为嵌入时水印图像的置乱次数）即得到最终的水印信息。

[0027] 图 3 发射机工作原理：发射机要在实现 CMMB 发射功能：采样、载频、编码、交织等的基础之上，要能够实现在采集到的信息码流之中嵌入水印信息，同时不影响视频质量。

[0028] 图 4 接收机工作原理：接收机的工作方式与发射机正好相反，需要实现解交织、解码等功能，同时能够从接收到的信号中监测到是否含有水印信息。

[0029] 对接收机的监测结果和水印添加效果进行分析。如果监测到水印，则对监测到的水印信息的完整性等进行分析，如果水印不完整或与原水印信息不相符，则发出报警，告知监测人员。

[0030] CMMB 安全监测系统的目的是为了保证其安全播出，及时发现信号中断、非法插播等问题，核实播出效果，确保节目内容安全。

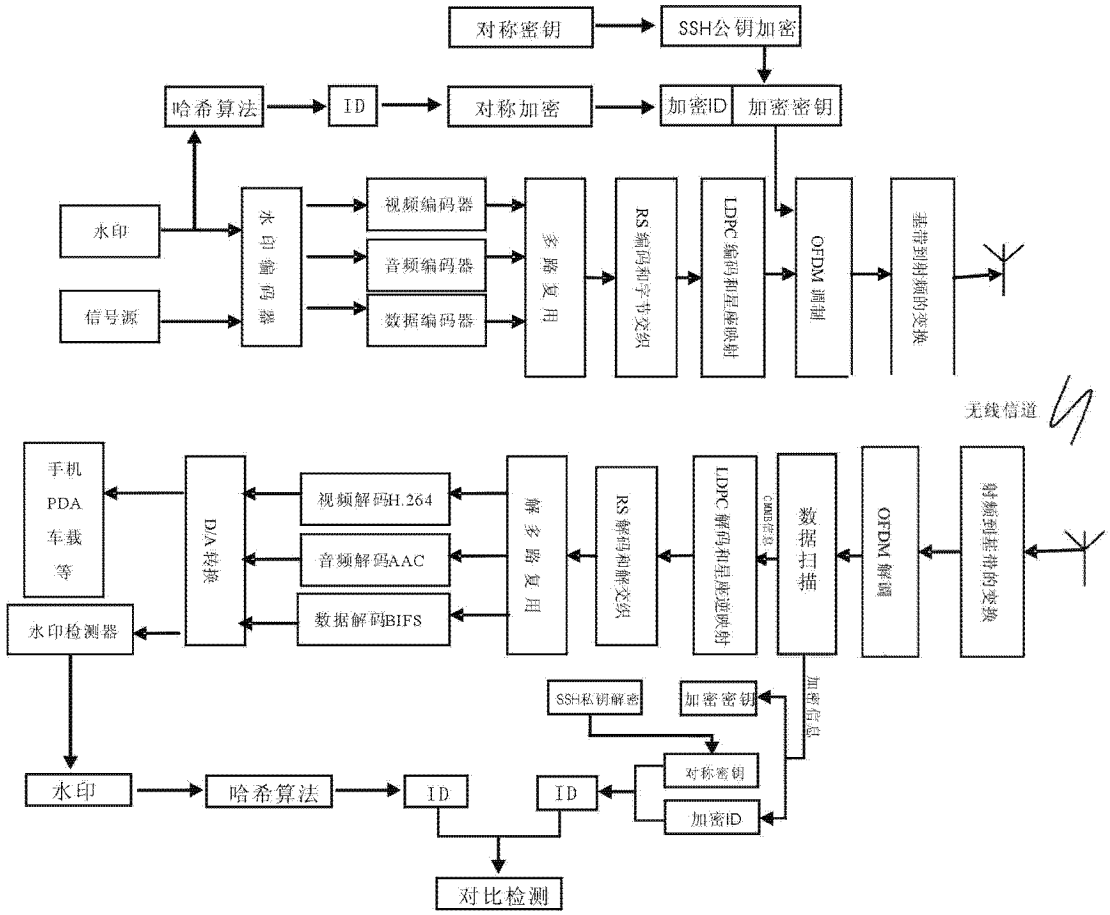

对称密钥
SSH公钥加密
哈希算法
ID
对称加密
加密ID
加密密钥
水印
信号源
水印编码器
视频编码器
音频编码器
数据编码器
多路复用
RS编码和字节交织
LDPC编码和星座映射
OFDM调制
基带到射频的变换
无线信道
手机
PDA
车载
等
D/A转换
水印检测器
视频解码H.264
音频解码AAC
数据解码BIFS
解多路复用
RS解码和解交织
LDPC解码和星座逆映射
数据扫描
OFDM解调
射频到基带的变换
SSH私钥解密
加密密钥
对称密钥
加密ID
加密信息
水印
哈希算法
ID
ID
对比检测

图 1

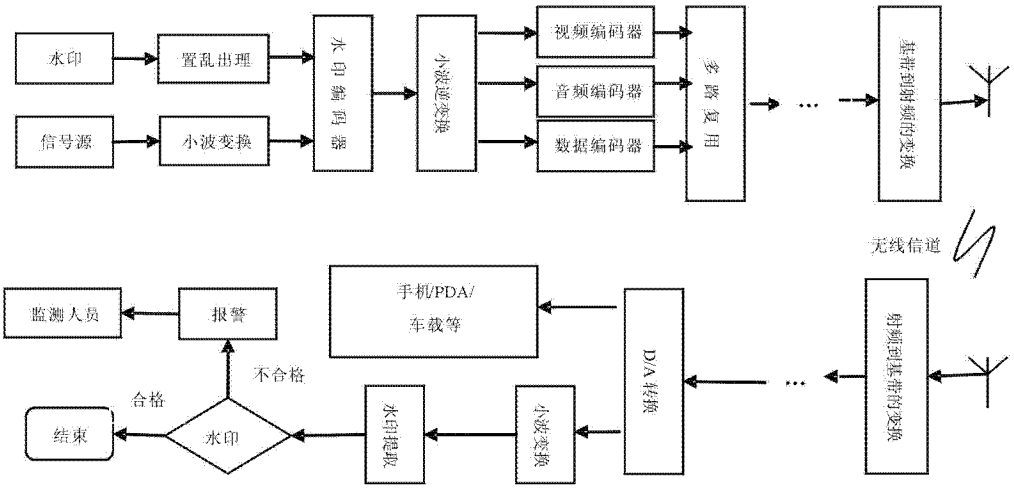

水印
置乱出理
信号源
小波变换
水印编码器
小波逆变换
视频编码器
音频编码器
数据编码器
多路复用
基带到射频的变换
无线信道
监测人员
报警
手机/PDA/
车载等
D/A转换
射频到基带的变换
不合格
合格
结束
水印
水印提取
小波变换

图 2

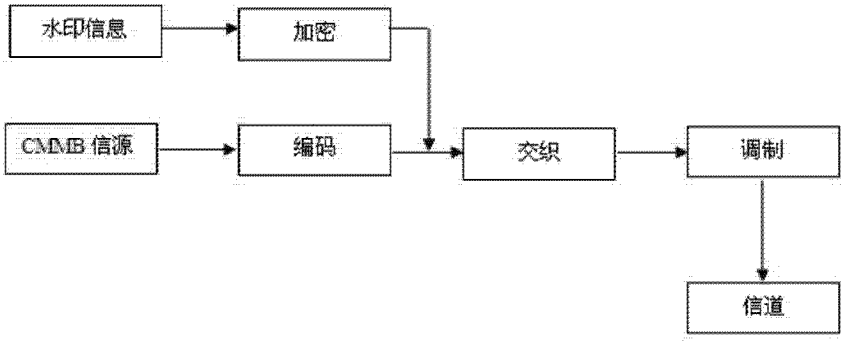

水印信息
加密
CMMB 信源
编码
交织
调制
信道

图 3

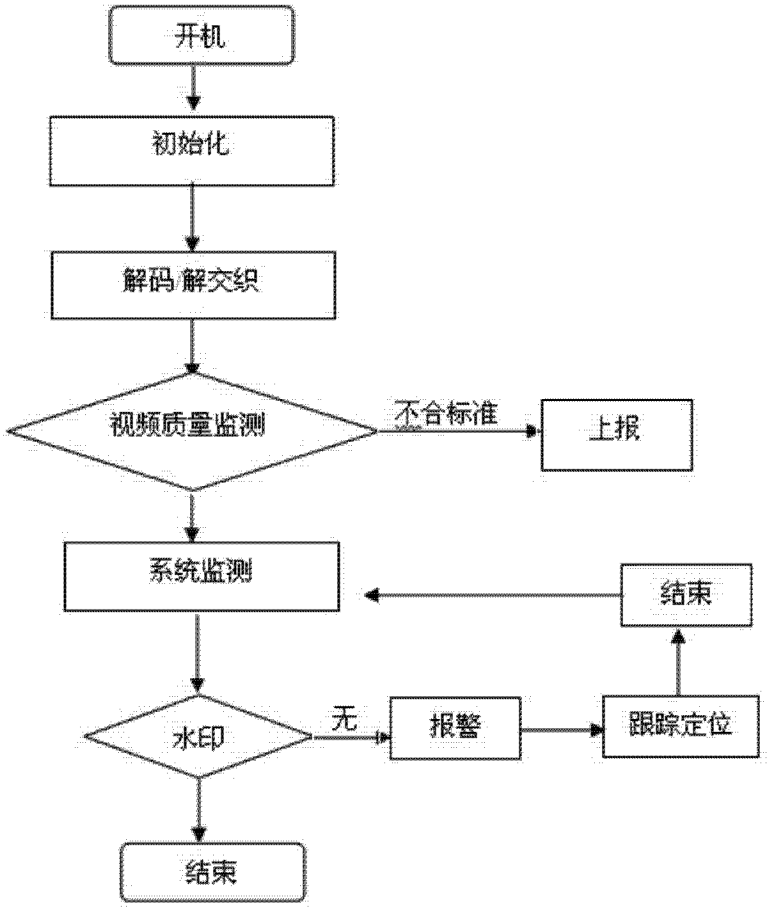

开机
初始化
解码/解交织
视频质量监测
不合标准
上报
系统监测
结束
水印
无
报警
跟踪定位
结束

图 4