(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110012296 B
(45)授权公告日 2021.08.17

(21)申请号 201811389442.4
(22)申请日 2018.11.21
(65)同一申请的已公布的文献号
申请公布号 CN 110012296 A
(43)申请公布日 2019.07.12
(73)专利权人 杭州基尔区块链科技有限公司
地址 310030 浙江省杭州市西湖区三墩镇西园三路3号5幢609室
(72)发明人 陆哲明 郁发新 罗雪雪
(74)专利代理机构 杭州天昊专利代理事务所(特殊普通合伙) 33283
代理人 董世博
(51)Int.Cl.
H04N 19/467(2014.01)
H04N 21/854(2011.01)
(56)对比文件
CN 101056392 A,2007.10.17
CN 101340579 A,2009.01.07
CN 102801947 A,2012.11.28
CN 106454368 A,2017.02.22
US 2008098022 A1,2008.04.24
EP 1542227 A1,2005.06.15
赵光赫等.《H. 264 /AVC 视频水印技术及其面向HEVC 的扩展》.《小型微型计算机系统》.2018,第39卷(第4期),第748-754页.
Bin Yan.《Spectrum Shaped Dither Modulation Watermarking for Correlated Host Signal》.《IEEE International Conference on Multimedia and Expo (ICME)》.2007,第1227-1230页.
Hao Luo.《Data Hiding in Non-expansion Visual Cryptography Based on Edge》.《The Fourth International Conference on Information Assurance and Security》.2008,第79-82页.
审查员 徐庆

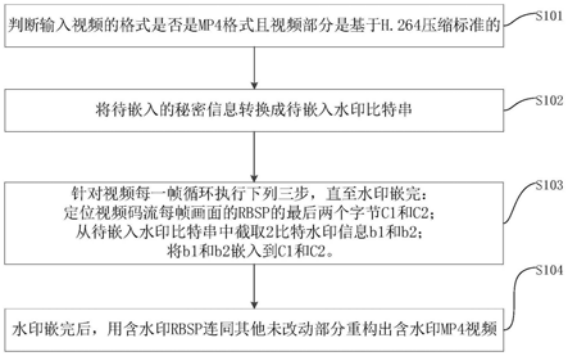
权利要求书3页 说明书10页 附图3页

(54)发明名称

一种针对MP4视频码流的快速信息嵌入方法

(57)摘要

本发明公开了一种针对MP4视频码流的快速信息嵌入方法,作为当前流行的视频格式MP4,其内部的视频编码标准是H.264;充分考察了H.264码流数据的格式,提供一种简单快速有效的码流信息隐藏方法、装置、电子设备及存储设备。



CN 110012296 B

1.一种针对MP4视频码流的快速信息嵌入方法,其特征在于,包括秘密信息嵌入方法和提取秘密信息的方法,提取秘密信息的方法具体如下步骤:

101)判断原始视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的;若是,则继续;否则,给予不能嵌入秘密信息的提示;

102)将待嵌入秘密信息转换成待嵌入水印比特串,其将针对视频的每一帧循环执行下列步骤,直到所有水印比特已嵌完或者所有帧已嵌完:

首先定位当前帧画面的RBSP的最后两个字节C1和C2;从待嵌入水印比特串中截取2比特水印信息b1和b2;最后按照一定规则将b1和b2嵌入到C1和C2;

103)水印嵌完后,基于所有含水印RBSP和其他未改动部分重构出含水印MP4视频。

2. 根据权利要求 1 所述的一种针对MP4视频码流的快速信息嵌入方法,其特征在于:所述步骤102)中按照一定规则将b1和b2嵌入到C1和C2,具体包括如下:判断最后一个字节C2是否等于0;若C2不等于0,则直接把两比特水印位b1和b2连起来并在其前后各加1比特标志位“1”一起替换C2的低4位,结束;若C2等于0,则判断倒数第二个字节C1是否等于0;若C1等于0,则原始的视频码流有误,给出错误提示,整个算法退出;若C1不等于0,则直接把两比特水印位b1和b2连起来并在其前后各加1比特标志位“1”一起替换C1的低4位,结束。

3. 根据权利要求 1所述的一种针对MP4视频码流的快速信息嵌入方法,其特征在于:所述待嵌入秘密信息转换成待嵌入水印比特串,具体包括如下:

将所述待嵌入秘密信息转换成原始比特串;

对所述原始比特串进行置乱处理,得到待嵌入水印比特串。

4. 根据权利要求 1 所述的一种针对MP4视频码流的快速信息嵌入方法,其特征在于:所述原始比特串进行置乱处理,得到待嵌入水印比特串,包括:选定置乱密钥;基于所设定密钥生成一个混沌序列;基于生成的混沌序列对所述原始比特串进行置乱处理,得到待嵌入水印比特串;还包括嵌完后,将所述置乱密钥和嵌入的水印比特串长度作为密钥提供给水印信息提取端。

5.根据权利要求1所述的一种针对MP4视频码流的快速信息嵌入方法,其特征在于,秘密信息提取方法具体包括如下步骤:

201)判断可疑视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的;若是,则继续;否则,给予不能提取秘密信息的提示;

202)针对可疑视频的每一帧循环执行下列判断,直到所有帧已提取完:

首先定位当前帧画面的RBSP的最后两个字节C1和C2;再从C1和C2中提取2比特水印信息b1和b2;然后水印提取完后,将各帧的2比特水印串成提取的水印比特串,将提取的水印比特串转换为提取的秘密信息。

6.根据权利要求5所述的一种针对MP4视频码流的快速信息嵌入方法,其特征在于,所述从C1和C2中提取2比特水印信息b1和b2,具体包括如下:

判断最后一个字节C2是否等于0;

若C2不等于0,则直接取出C2的低4位中的中间两位作为b1和b2,结束;

若C2等于0,则判断倒数第二个字节C1是否等于0;

若C1等于0,则可疑视频码流有误,给出错误提示,整个算法退出;

若C1不等于0,则直接取出C1的低4位中的中间两位作为b1和b2,结束。

7.根据权利要求5所述的一种针对MP4视频码流的快速信息嵌入方法，其特征在于，所述将提取的水印比特串转换为提取的秘密信息，包括：根据获知的水印比特串长度从所述提取的水印比特串中截取对应长度的比特串，得到截取的水印比特串；对所述截取的水印比特串进行反置乱；基于反置乱后的比特串，恢复出提取的秘密信息；

所述对所述截取的水印比特串进行反置乱，包括：

使用获知的置乱密钥产生混沌序列；基于生成的混沌序列，对所述截取的水印比特串进行反置乱处理。

8.根据权利要求5所述的一种针对MP4视频码流的快速信息嵌入方法，其特征在于，还包括：从秘密信息嵌入端提供的包含置乱密钥和水印比特串长度的密钥中获得所述置乱密钥和水印比特串长度；或者，从预先约定的包含置乱密钥和水印比特串入长度的密钥中获得所述置乱密钥和水印比特串长度。

9.根据权利要求5所述的一种针对MP4视频码流的快速信息嵌入方法，其特征在于，还包括秘密信息嵌入装置、电子设备；

秘密信息嵌入装置将原始MP4视频格式解析和判断单元，用于判断输入视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的；由秘密信息生成水印单元，用于将所述秘密信息经置乱转换成待嵌入水印比特串；水印信息嵌入单元，用于遍历视频所有帧，定位每一帧画面的RBSP的最后两个字节并在里面嵌入2比特水印信息；含水印MP4视频重构单元，用于基于所有含水印RBSP和其他未改动部分重构出含水印MP4视频；

电子设备，包括：算法处理器，以及嵌入算法存储器，用于存储秘密信息嵌入方法的程序，该设备通电并通过所述处理器运行该秘密信息嵌入方法的程序后，执行下述步骤：

判断原始视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的；若是，则继续；否则，给予不能嵌入秘密信息的提示；将待嵌入秘密信息转换成待嵌入水印比特串；针对视频的每一帧循环执行下列三步，直到所有水印比特已嵌完或者所有帧已嵌完：

首先定位当前帧画面的RBSP的最后两个字节C1和C2；再从待嵌入水印比特串中截取2比特水印信息b1和b2；最后按照一定规则将b1和b2嵌入到C1和C2；

水印嵌完后，基于所有含水印RBSP和其他未改动部分重构出含水印MP4视频；

嵌入算法存储设备，用于存储有秘密信息嵌入方法的程序，该程序被处理器运行，执行下述步骤：

判断原始视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的；若是，则继续；否则，给予不能嵌入秘密信息的提示；将待嵌入秘密信息转换成待嵌入水印比特串；针对视频的每一帧循环执行下列三步，直到所有水印比特已嵌完或者所有帧已嵌完：

定位当前帧画面的RBSP的最后两个字节C1和C2；

从待嵌入水印比特串中截取2比特水印信息b1和b2；

按照一定规则将b1和b2嵌入到C1和C2；

水印嵌完后，基于所有含水印RBSP和其他未改动部分重构出含水印MP4视频。

10.根据权利要求5所述的一种针对MP4视频码流的快速信息嵌入方法，其特征在于，还包括秘密信息提取装置，包括：

可疑MP4视频格式判断单元，用于判断可疑视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的；

水印信息提取单元，用于遍历视频所有帧，定位每一帧画面的RBSP的最后两个字节并从中提取2比特水印信息；

水印比特串反置乱单元，根据水印比特串长度从提取的水印比特串中截取指定长度的比特串，利用混沌密钥生成混沌序列，基于混沌序列对截取后的比特串进行反置乱处理；

秘密信息重构单元，由反置乱后的比特串恢复出提取的秘密信息。

一种针对MP4视频码流的快速信息嵌入方法

技术领域

[0001] 本发明涉及信息隐藏技术领域，更具体的说，它涉及一种针对MP4视频码流的快速信息嵌入方法。

背景技术

[0002] 随着网络多媒体技术和视频压缩编码技术的迅速发展，人们通过视频可以很方便地获取各种信息。网络带宽日益增加以及数字视频流媒体技术日益成熟，使得数字视频的传输和应用越来越广泛，如手机客户端、数字电视、网络视频、监控视频等，也使得网络视频用户规模保持持续增长。然而，数字视频作为数字信息的一种，具有信息量丰富、社会价值和商业价值高、易于被复制、易于被篡改的特性。随着视频的持续火热，问题也是不断涌现，例如盗版光盘，隐私视频外泄，篡改视频内容等。这就使得视频相关的利益受到损害，相关的隐私受到侵犯。目前主流的视频压缩标准H.264/AVC具有低码率、应用目标宽、容错能力强、高效的网络传输(拥有网络适应层)和极佳的图像传输质量(1Mbps码率下就可以达到DVD画质)等优点，被广泛应用于低码率的无线应用、网络流媒体、网络课程、视频会议等许许多多多媒体应用领域，从而使得基于视频产品的版权保护的问题日益严重。因此，如何保护数字视频的版权以及如何鉴别数字视频的真实性和完整性成为亟待解决的问题。

[0003] 在数字时代，信息隐藏是一种将秘密信息不可感知地嵌入到文本、音频、图像和视频等数字媒体中的技术。当用户在知晓嵌入算法和嵌入密钥的情况下，可以从承载数据的数字媒体中提取出嵌入的数据。作为一种应用型技术，信息隐藏在维护数字媒体内容安全中发挥了显著的作用。视频已成为当前网络中最流行的媒体之一，是内容丰满易于传播和使用的信息载体。为了保护视频拥有者的合法权益，可在视频中隐藏版权及其他信息来防止侵权行为的发生，目前这种技术已经受到了广泛的关注。视频编码除了考虑到帧内压缩编码，还要考虑帧间压缩编码。帧内压缩编码可以参考图像压缩标准比较简单，但是帧间压缩编码才是重点和难点，帧间压缩标准并没有成熟的模型可以参考，过程比较复杂。与此同时还需要考虑到信息隐藏方案的性能(主要包括鲁棒性和不可见性)，这也提高了视频信息隐藏设计的难度。秘密信息通常用一定的算法生成待嵌入的水印。嵌入水印之后的视频可能会受到一定的干扰，水印必须具备一定的鲁棒性来抵抗可能遇到的干扰，水印嵌入之后视频和原始视频的差异必须小到不会引起人眼的注意才行，否则水印就无法发挥其原本的作用。因此，相比于图像信息隐藏，视频信息隐藏挑战性大、技术难度高、面临的攻击方式多而复杂、需要解决实时性问题，一种性能较好的视频信息隐藏算法的提出是有一定难度的。

[0004] 根据信息的嵌入位置，视频信息隐藏算法大致可将分为三类。第一类是基于原始视频序列的信息隐藏算法。例如，利用扩频通信的思想将调制后的水印信息与原始视频数据进行叠加。第二类是与编码过程相结合的视频信息隐藏算法。该类算法的主要思路是根据水印信息修改那些视频编码过程中的可控元素，如DCT(离散余弦变换)系数、预测模式以及运动向量等。第三类是基于部分解码的视频信息隐藏算法。例如，基于水印信息对经过部分解码后I帧的DCT系数进行修改，然后再对其进行量化、熵编码等操作得到含水印视频流。

这里需要指出，帧是组成视频图像的基本单位，I帧也叫关键帧，它是帧间压缩编码里的重要帧，它是一个全帧压缩的编码帧，解码时仅用I帧的数据就可重构完整图像而不需要参考其他画面而生成。综合分析现有的三类视频信息隐藏方案可知，基于原始视频序列的信息隐藏算法将水印信息嵌入到原始视频的空域或者频域。该水印易在视频压缩、变换、量化等过程中被当成噪声去掉，鲁棒性较差。与编码过程相结合的信息隐藏算法往往需要经过解码-再编码的过程，对视频本身影响较大，且速度较慢。基于部分解码的信息隐藏算法也对视频内容有较大改变，容易造成视频体积膨胀、视频质量下降严重等问题。由此可见，现有的视频信息隐藏方法，不能很好地满足视频实时传输的需求，不能达到视频比特流变化幅度与嵌入容量的较好折中，急需一种同时满足实时性的和对比特流改变较小的信息隐藏方法。

发明内容

[0005] 本发明克服了现有技术的不足，提供一种针对MP4视频码流的快速信息嵌入方法，算法速度非常快，满足实时性；嵌入过程不改变文件大小，增强了掩蔽性。

[0006] 本发明的技术方案如下：

[0007] 一种针对MP4视频码流的快速信息嵌入方法，包括秘密信息嵌入方法和提取秘密信息的方法，提取秘密信息的方法具体如下步骤：

[0008] 101)判断原始视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的；若是，则继续；否则，给予不能嵌入秘密信息的提示；

[0009] 102)将待嵌入秘密信息转换成待嵌入水印比特串，其将针对视频的每一帧循环执行下列步骤，直到所有水印比特已嵌完或者所有帧已嵌完：

[0010] 首先定位当前帧画面的RBSP的最后两个字节C1和C2；从待嵌入水印比特串中截取2比特水印信息b1和b2；最后按照一定规则将b1和b2嵌入到C1和C2；

[0011] 103)水印嵌完后，基于所有含水印RBSP和其他未改动部分重构出含水印MP4视频。

[0012] 进一步的，所述步骤102)中按照一定规则将b1和b2嵌入到C1和C2，具体包括如下：判断最后一个字节C2是否等于0；若C2不等于0，则直接把两比特水印位b1和b2连起来并在其前后各加1比特标志位“1”一起替换C2的低4位，结束；若C2等于0，则判断倒数第二个字节C1是否等于0；若C1等于0，则原始的视频码流有误，给出错误提示，整个算法退出；若C1不等于0，则直接把两比特水印位b1和b2连起来并在其前后各加1比特标志位“1”一起替换C1的低4位，结束。

[0013] 进一步的，所述待嵌入秘密信息转换成待嵌入水印比特串，具体包括如下：将所述待嵌入秘密信息转换成原始比特串；对所述原始比特串进行置乱处理，得到待嵌入水印比特串。

[0014] 进一步的，所述原始比特串进行置乱处理，得到待嵌入水印比特串，包括：选定置乱密钥；基于所设定密钥生成一个混沌序列；基于生成的混沌序列对所述原始比特串进行置乱处理，得到待嵌入水印比特串；还包括嵌完后，将所述置乱密钥和嵌入的水印比特串长度作为密钥提供给水印信息提取端。

[0015] 进一步的，秘密信息提取方法具体包括如下步骤：

[0016] 201)判断可疑视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的；若

是,则继续;否则,给予不能提取秘密信息的提示;

[0017] 202)针对可疑视频的每一帧循环执行下列判断,直到所有帧已提取完:

[0018] 首先定位当前帧画面的RBSP的最后两个字节C1和C2;再从C1和C2中提取2比特水印信息b1和b2;然后水印提取完后,将各帧的2比特水印串成提取的水印比特串,将提取的水印比特串转换为提取的秘密信息。

[0019] 进一步的,所述从C1和C2中提取2比特水印信息b1和b2,具体包括如下:判断最后一个字节C2是否等于0;

[0020] 若C2不等于0,则直接取出C2的低4位中的中间两位作为b1和b2,结束;

[0021] 若C2等于0,则判断倒数第二个字节C1是否等于0;

[0022] 若C1等于0,则可疑视频码流有误,给出错误提示,整个算法退出;

[0023] 若C1不等于0,则直接取出C1的低4位中的中间两位作为b1和b2,结束。

[0024] 进一步的,所述将提取的水印比特串转换为提取的秘密信息,包括:根据获知的水印比特串长度从所述提取的水印比特串中截取对应长度的比特串,得到截取的水印比特串;对所述截取的水印比特串进行反置乱;基于反置乱后的比特串,恢复出提取的秘密信息;

[0025] 所述对所述截取的水印比特串进行反置乱,包括:

[0026] 使用获知的置乱密钥产生混沌序列;基于生成的混沌序列,对所述截取的水印比特串进行反置乱处理。

[0027] 进一步的,还包括:从秘密信息嵌入端提供的包含置乱密钥和水印比特串长度的密钥中获得所述置乱密钥和水印比特串长度;或者,从预先约定的包含置乱密钥和水印比特串入长度的密钥中获得所述置乱密钥和水印比特串长度。

[0028] 进一步的,还包括秘密信息嵌入装置、电子设备;

[0029] 秘密信息嵌入装置将原始MP4视频格式解析和判断单元,用于判断输入视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的;由秘密信息生成水印单元,用于将所述秘密信息经置乱转换成待嵌入水印比特串;水印信息嵌入单元,用于遍历视频所有帧,定位每一帧画面的RBSP的最后两个字节并在里面嵌入2比特水印信息;含水印MP4视频重构单元,用于基于所有含水印RBSP和其他未改动部分重构出含水印MP4视频;

[0030] 电子设备,包括:算法处理器,以及嵌入算法存储器,用于存储秘密信息嵌入方法的程序,该设备通电并通过所述处理器运行该秘密信息嵌入方法的程序后,执行下述步骤:

[0031] 判断原始视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的;若是,则继续;否则,给予不能嵌入秘密信息的提示;将待嵌入秘密信息转换成待嵌入水印比特串;针对视频的每一帧循环执行下列三步,直到所有水印比特已嵌完或者所有帧已嵌完:

[0032] 首先定位当前帧画面的RBSP的最后两个字节C1和C2;再从待嵌入水印比特串中截取2比特水印信息b1和b2;最后按照一定规则将b1和b2嵌入到C1和C2;

[0033] 水印嵌完后,基于所有含水印RBSP和其他未改动部分重构出含水印MP4视频;

[0034] 嵌入算法存储设备,用于存储有秘密信息嵌入方法的程序,该程序被处理器运行,执行下述步骤:

[0035] 判断原始视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的;若是,则继续;否则,给予不能嵌入秘密信息的提示;将待嵌入秘密信息转换成待嵌入水印比特

串;针对视频的每一帧循环执行下列三步,直到所有水印比特已嵌完或者所有帧已嵌完:

[0036] 定位当前帧画面的RBSP的最后两个字节C1和C2;

[0037] 从待嵌入水印比特串中截取2比特水印信息b1和b2;

[0038] 按照一定规则将b1和b2嵌入到C1和C2;

[0039] 水印嵌完后,基于所有含水印RBSP和其他未改动部分重构出含水印MP4视频。

[0040] 进一步的,还包括秘密信息提取装置,包括:

[0041] 可疑MP4视频格式判断单元,用于判断可疑视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的;

[0042] 水印信息提取单元,用于遍历视频所有帧,定位每一帧画面的RBSP的最后两个字节并从中提取2比特水印信息;

[0043] 水印比特串反置乱单元,根据水印比特串长度从提取的水印比特串中截取指定长度的比特串,利用混沌密钥生成混沌序列,基于混沌序列对截取后的比特串进行反置乱处理;

[0044] 秘密信息重构单元,由反置乱后的比特串恢复出提取的秘密信息。

[0045] 本发明相比现有技术优点在于:本申请通过考察MP4视频中H.264码流打包成字节的过程,提供一种快速有效的信息嵌入方法、装置、电子设备及存储设备,通过定位(可以利用FFMPEG开源程序)视频每一帧画面的RBSP的最后两个字节来嵌入水印2比特水印。经实验验证,这些改动对视频质量的影响很小,满足不可见性;嵌入信息的过程不需要解码,算法速度非常快,满足实时性;嵌入过程不改变文件大小,增强了掩蔽性。

附图说明

[0046] 图1是本申请的一种秘密信息嵌入方法的流程图;

[0047] 图2是本申请的一种秘密信息提取方法的流程图;

[0048] 图3是本申请的一种秘密信息嵌入装置的示意图;

[0049] 图4是本申请的一种嵌入电子设备的示意图;

[0050] 图5是本申请的一种秘密信息提取装置的示意图;

[0051] 图6是本申请的一种提取电子设备的示意图。

具体实施方式

[0052] 下面详细描述本发明的实施方式,其中自始至终相同或类似的标号表示相同或类似的元件或类似功能的元件。下面通过参考附图描述的实施方式是示例性的,仅用于解释本发明而不能作为对本发明的限制。

[0053] 本技术领域技术人员可以理解的是,除非另外定义,这里使用的所有术语(包括技术术语和科技术语)具有与本发明所属领域中的普通技术人员的一般理解相同的意义。还应该理解的是,诸如通用字典中定义的那些术语应该被理解为具有与现有技术的上下文中的意义一致的意义,并且除非像这里一样的定义,不会用理想化或过于正式的含义来解释。

[0054] 下面结合附图和具体实施方式对本发明进一步说明。

[0055] 实施例1:

[0056] 如图1所示,一种针对MP4视频码流的快速信息嵌入方法的秘密信息嵌入这一块。

在图中步骤S101中，判断输入视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的；若是，则继续；否则，给予不能嵌入秘密信息的提示；

[0057] 在判断时，可以用FFMPEG代码来解析MP4视频文件，并判断MP4文件里的视频部分编码是否采用H.264方式(音频部分不管)。FFMPEG是一套可以用来记录、转换数字音频、视频，并能将其转化为流的开源计算机程序。它提供了录制、转换以及流化音视频的完整解决方案。

[0058] 在步骤S102中，将待嵌入的秘密信息转换成待嵌入水印比特串。

[0059] 所述秘密信息，指待嵌入到视频中的原始版权信息、指纹信息或标注信息，如某个公司的公司名、某个员工的员工编号或其他标识信息。生成的待嵌入水印比特串可以隐藏嵌入到视频中，不会影响原视频的使用价值，也不易被探知和再次修改。但水印比特串可以被生产方识别和辨认。通过这些嵌入在视频中的水印信息，可以达到确认内容创建者、购买者、传送隐秘信息或者判断视频是否被篡改等目的。

[0060] 为了提高水印嵌入的安全性，将待嵌入秘密信息转换成待嵌入水印比特串的一种实现方式如下：先将所述待嵌入秘密信息转换成原始比特串；选定置乱密钥；基于所设定密钥利用logistics映射二值化后生成一个二值混沌序列；基于生成的混沌序列与所述原始比特串进行异或处理，就可得到待嵌入水印比特串。

[0061] 为了水印信息提取端能够获得所述置乱密钥和嵌入的水印比特串长度，可以将所述置乱密钥和待嵌入水印比特串的长度提供给水印信息提取端。将所述置乱密钥和待嵌入水印比特串的长度提供给水印信息提取端，可以采用两种方式：一种方式是：将所述置乱密钥和待嵌入水印比特串的长度以单独消息的形式发送至水印提取端；另一种方式是：以水印信息提取端和水印信息嵌入端预先约定的方式将所述置乱密钥和待嵌入水印比特串的长度提供给水印信息提取端。

[0062] 在步骤S103中，针对视频的每一帧循环执行下列三步，直到所有水印位已嵌完或者所有帧已嵌完：

[0063] 定位视频码流每帧画面的RBSP的最后两个字节C1和C2；

[0064] 从待嵌入水印比特串中截取2比特水印信息b1和b2；

[0065] 将b1和b2嵌入到C1和C2；

[0066] 这一步骤的一种具体的实现方案如下：将每帧视频码流按顺序存放在一个Packet包中，定位Packet.data的最后两个字节。举例：C1 C2:表示最后两个字节，如果最后一个字节C2为0，最后第二个字节C1不为0，那么将2比特水印b1和b2加上头尾各1比特标志位“1”，直接替换C1的最后4位；如果C2字节不为0，直接将将2比特水印b1和b2加上头尾各1比特标志位“1”替换C2的最后4位。例如：码流最后两个字节10001000|00000000，2比特水印b1和b2为11，头尾各1bit标志位信息同为1，因为码流最后的字节为0，所以将1111(头尾的1为标志位，中间两个1为水印)嵌入到10001000，嵌入后的码流变成1001111|00000000。

[0067] 在步骤S104中，水印嵌完后，用含水印RBSP连同其他未改动部分重构出含水印MP4视频。重构后的MP4视频文件的一大特点是与原始视频文件大小一模一样。

[0068] 综上实施例1首先判断原始视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的；若是，则继续；否则，给予不能嵌入秘密信息的提示；将待嵌入秘密信息转换成待嵌入水印比特串；定位每一帧画面的RBSP的最后两个字节嵌入2比特水印信息；水印嵌完

后，基于所有含水印RBSP和其他未改动部分重构出含水印MP4视频。该方法嵌入速度快，对视频质量的影响小，不改变视频文件大小。例如：对于尺寸为1920*1080的时长为87分14秒的文件大小为3.04G的MP4视频文件，嵌入秘密信息后文件大小仍为3.04G，嵌入时间为58s，与原始视频相比含水印视频质量达平均每帧峰值信噪比38dB以上。

[0069] 实施例2：

[0070] 相对实施例1，本实施例还提供了一种秘密信息嵌入装置。

[0071] 如图3所示，所述秘密信息嵌入装置包括：原始MP4视频格式解析和判断单元301，用于判断输入视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的；由秘密信息生成水印单元302，用于将所述秘密信息经置乱转换成待嵌入水印比特串；水印信息嵌入单元303，用于遍历视频所有帧，定位每一帧画面的RBSP的最后两个字节并在里面嵌入2比特水印信息；含水印MP4视频重构单元304，用于基于所有含水印RBSP和其他未改动部分重构出含水印MP4视频。

[0072] 由秘密信息生成水印单元，用于将所述秘密信息经置乱转换成待嵌入水印比特串，包括：将所述待嵌入秘密信息转换成原始比特串；对所述原始比特串进行置乱处理，得到待嵌入水印比特串；

[0073] 所述对所述原始比特串进行置乱处理，得到待嵌入水印比特串，包括：选定置乱密钥；基于所设定密钥生成一个混沌序列；基于生成的混沌序列对所述原始比特串进行置乱处理，得到待嵌入水印比特串。

[0074] 所述装置还包括：密钥提供单元，用于将所述置乱密钥和嵌入的水印比特串长度作为密钥提供给水印信息提取端。

[0075] 实施例3：

[0076] 相对实施例1，本实施例还包括了一种嵌入电子设备。

[0077] 如图4所示，嵌入电子设备包括：算法处理器401；以及嵌入算法存储器402，用于存储秘密信息嵌入方法的程序，该设备通电并通过所述处理器运行该秘密信息嵌入方法的程序后，执行下述步骤：判断原始视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的；若是，则继续；否则，给予不能嵌入秘密信息的提示；将待嵌入秘密信息转换成待嵌入水印比特串；针对视频的每一帧循环执行下列三步，直到所有水印比特已嵌完或者所有帧已嵌完：

[0078] 定位当前帧画面的RBSP的最后两个字节C1和C2；

[0079] 从待嵌入水印比特串中截取2比特水印信息b1和b2；

[0080] 按照一定规则将b1和b2嵌入到C1和C2；

[0081] 水印嵌完后，基于所有含水印RBSP和其他未改动部分重构出含水印MP4视频。

[0082] 所述按照一定规则将b1和b2嵌入到C1和C2，包括：判断最后一个字节C2是否等于0；若C2不等于0，则直接把两比特水印位b1和b2连起来并在其前后各加1比特标志位“1”一起替换C2的低4位，结束；若C2等于0，则判断倒数第二个字节C1是否等于0；若C1等于0，则原始的视频码流有误，给出错误提示，整个算法退出；若C1不等于0，则直接把两比特水印位b1和b2连起来并在其前后各加1比特标志位“1”一起替换C1的低4位，结束。

[0083] 所述将待嵌入秘密信息转换成待嵌入水印比特串，包括：将所述待嵌入秘密信息转换成原始比特串；对所述原始比特串进行置乱处理，得到待嵌入水印比特串。所述对所述

原始比特串进行置乱处理，得到待嵌入水印比特串，包括：选定置乱密钥；基于所设定密钥生成一个混沌序列；基于生成的混沌序列对所述原始比特串进行置乱处理，得到待嵌入水印比特串。

[0084] 所述嵌入电子设备还执行下述步骤：嵌完后，将所述置乱密钥和嵌入的水印比特串长度作为密钥提供给水印信息提取端。

[0085] 实施例4：

[0086] 相对实施例1，本实施例还包括了一种嵌入算法存储设备，存储有秘密信息嵌入方法的程序，该程序被处理器运行，执行下述步骤：

[0087] 判断原始视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的；若是，则继续；否则，给予不能嵌入秘密信息的提示；将待嵌入秘密信息转换成待嵌入水印比特串；针对视频的每一帧循环执行下列三步，直到所有水印比特已嵌完或者所有帧已嵌完：定位当前帧画面的RBSP的最后两个字节C1和C2；从待嵌入水印比特串中截取2比特水印信息b1和b2；按照一定规则将b1和b2嵌入到C1和C2；水印嵌完后，基于所有含水印RBSP和其他未改动部分重构出含水印MP4视频。

[0088] 实施例5：

[0089] 如图2所示，一种针对MP4视频码流的快速信息嵌入方法提供一种秘密信息提取方法。

[0090] 在步骤S201中，判断可疑视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的。若是，则继续；否则，给予不能提取秘密信息的提示。

[0091] 在判断时，可以用FFMPEG代码来解析MP4视频文件，并判断MP4文件里的视频部分编码是否采用H.264方式(音频部分不管)。FFMPEG是一套可以用来记录、转换数字音频、视频，并能将其转化为流的开源计算机程序。它提供了录制、转换以及流化音视频的完整解决方案。

[0092] 在步骤S202中，针对可疑视频的每一帧循环执行下列两步，直到所有帧已提取完：定位当前帧画面的RBSP的最后两个字节C1和C2；从C1和C2中提取2比特水印信息b1和b2。

[0093] 这一步骤的一种具体实施方式如下：判断最后一个字节C2是否等于0；若C2不等于0，则直接取出C2的低4位中的中间两位作为b1和b2，结束；若C2等于0，则判断倒数第二个字节C1是否等于0；若C1等于0，则可疑视频码流有误，给出错误提示，整个算法退出；若C1不等于0，则直接取出C1的低4位中的中间两位作为b1和b2，结束。

[0094] 在这里解释一下为什么实施例1在嵌入水印时要加标志位，也是本算法的特色之处。原因是这与水印盲提取有关，因为水印提取时原始视频文件通常已经不在手边。具体地讲，嵌入水印信息前加入标志位1的目的在于防止水印信息为00，然后嵌入最后一个字节，将最后一个字节变成00000000，从而导致检测的时候定位在了倒数第二个字节上发生错误。例如最后两个字节为11001100|00000010，因为最后一个字节00000010不为0，从而将水印信息00嵌入到最后一个字节中的最后两位，变成00000000。在检测的时候因为最后一个字节变为了0，从而算法定位倒数第二个字节的最后两位为水印信息，从而发生错误。在水印信息00前加上标志位1可以很有效的防止这样的事情发生。下面解释在水印信息后加入标志位1的原因：视频码流如果最后一个字节的最后一位为0，那么他会在其后面加入一个0字节，所以为了防止这样子的事情发生，将嵌入水印的字节最后一位强制赋值为1，这样子

就可以不改变嵌入水印的视频码流的大小。

[0095] 在步骤S203中，水印提取完后，将各帧的2比特水印串成提取的水印比特串。

[0096] 在步骤S204中，将提取的水印比特串转换为提取的秘密信息。这一步包括：根据获知的水印比特串长度从所述提取的水印比特串中截取对应长度的比特串，得到截取的水印比特串；对所述截取的水印比特串进行反置乱；基于反置乱后的比特串，恢复出提取的秘密信息。

[0097] 所述对所述截取的水印比特串进行反置乱，包括：

[0098] 使用获知的置乱密钥产生混沌序列；基于生成的混沌序列，对所述截取的水印比特串进行反置乱处理。

[0099] 作为优选，从秘密信息嵌入端提供的包含置乱密钥和水印比特串长度的密钥中获得所述置乱密钥和水印比特串长度；或者，从预先约定的包含置乱密钥和水印比特串入长度的密钥中获得所述置乱密钥和水印比特串长度。

[0100] 实施例2提供的秘密信息提取方法的实施方式进行了详细说明。本申请第二实施例提供的秘密信息提取方法，算法速度很快，满足快速检测水印的需要。例如：对于尺寸为1920*1080的时长为87分14秒的文件大小为3.04G的MP4视频文件，提取秘密信息时间为1s之内。

[0101] 实施例6：

[0102] 相对于实施例5，本实施例还提供了一种秘密信息提取装置。

[0103] 如图5所示，所述秘密信息提取装置包括：可疑MP4视频格式判断单元501，用于判断可疑视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的；水印信息提取单元502，用于遍历视频所有帧，定位每一帧画面的RBSP的最后两个字节并从中提取2比特水印信息；水印比特串反置乱单元503，根据水印比特串长度从提取的水印比特串中截取指定长度的比特串，利用混沌密钥生成混沌序列，基于混沌序列对截取后的比特串进行反置乱处理；秘密信息重构单元504，由反置乱后的比特串恢复出提取的秘密信息。

[0104] 所述水印信息提取单元，具体用于针对可疑视频的每一帧循环执行下列两步，直到所有帧已提取完：定位当前帧画面的RBSP的最后两个字节C1和C2；从C1和C2中提取2比特水印信息b1和b2。

[0105] 所述水印比特串反置乱单元，包括：根据获知的水印比特串长度从所述提取的水印比特串中截取对应长度的比特串，得到截取的水印比特串；对所述截取的水印比特串进行反置乱。所述对所述截取的水印比特串进行反置乱，包括：使用获知的置乱密钥产生混沌序列；基于生成的混沌序列，对所述截取的水印比特串进行反置乱处理。

[0106] 所述装置还包括：字节定位子单元，用于定位当前帧画面的RBSP的最后两个字节C1和C2；二比特水印提取子单元，用于从C1和C2中提取2比特水印信息b1和b2。密钥获得单元，用于从秘密信息嵌入端提供的包含置乱密钥和水印比特串长度的密钥中获得所述置乱密钥和水印比特串长度；或者，从预先约定的包含置乱密钥和水印比特串入长度的密钥中获得所述置乱密钥和水印比特串长度。

[0107] 实施例7：

[0108] 相对于实施例5，本实施例还提供了一种提取电子设备。

[0109] 如图6所示，所述提取电子设备包括：算法处理器601；以及提取算法存储器602，用

于存储秘密信息提取方法的程序，该设备通电并通过所述处理器运行该秘密信息提取方法的程序后，执行下述步骤：判断可疑视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的；若是，则继续；否则，给予不能提取秘密信息的提示；针对可疑视频的每一帧循环执行下列两步，直到所有帧已提取完：定位当前帧画面的RBSP的最后两个字节C1和C2；从C1和C2中提取2比特水印信息b1和b2；水印提取完后，将各帧的2比特水印串成提取的水印比特串；将提取的水印比特串转换为提取的秘密信息。

[0110] 所述将提取的水印比特串转换为提取的秘密信息，包括：根据获知的水印比特串长度从所述提取的水印比特串中截取对应长度的比特串，得到截取的水印比特串；对所述截取的水印比特串进行反置乱；基于反置乱后的比特串，恢复出提取的秘密信息。

[0111] 所述对所述截取的水印比特串进行反置乱，包括：使用获知的置乱密钥产生混沌序列；基于生成的混沌序列，对所述截取的水印比特串进行反置乱处理。

[0112] 所述提取电子设备还执行下述步骤：从秘密信息嵌入端提供的包含置乱密钥和水印比特串长度的密钥中获得所述置乱密钥和水印比特串长度；或者，从预先约定的包含置乱密钥和水印比特串入长度的密钥中获得所述置乱密钥和水印比特串长度。

[0113] 实施例8：

[0114] 相对于实施例5，本实施例还提供了一种提取算法存储设备，存储有秘密信息提取方法的程序，该程序被处理器运行，执行下述步骤：判断可疑视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的；若是，则继续；否则，给予不能提取秘密信息的提示；针对可疑视频的每一帧循环执行下列两步，直到所有帧已提取完：定位当前帧画面的RBSP的最后两个字节C1和C2；从C1和C2中提取2比特水印信息b1和b2；水印提取完后，将各帧的2比特水印串成提取的水印比特串；将提取的水印比特串转换为提取的秘密信息。

[0115] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员，在不脱离本发明构思的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明保护范围内。

[0116] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0117] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0118] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括非暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0119] 本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的

形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

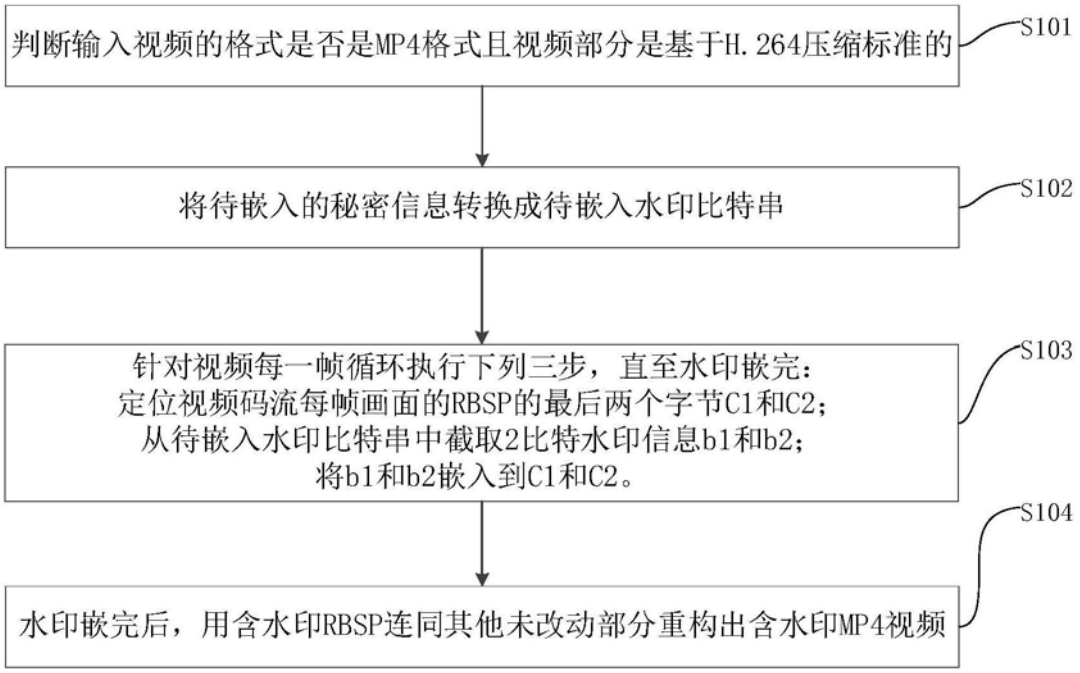

判断输入视频的格式是否是MP4格式且视频部分是基于H.264压缩标准的
S101
将待嵌入的秘密信息转换成待嵌入水印比特串
S102
针对视频每一帧循环执行下列三步，直至水印嵌完：
定位视频码流每帧画面的RBSP的最后两个字节C1和C2；
从待嵌入水印比特串中截取2比特水印信息b1和b2；
将b1和b2嵌入到C1和C2。
S103
水印嵌完后，用含水印RBSP连同其他未改动部分重构出含水印MP4视频
S104

图1

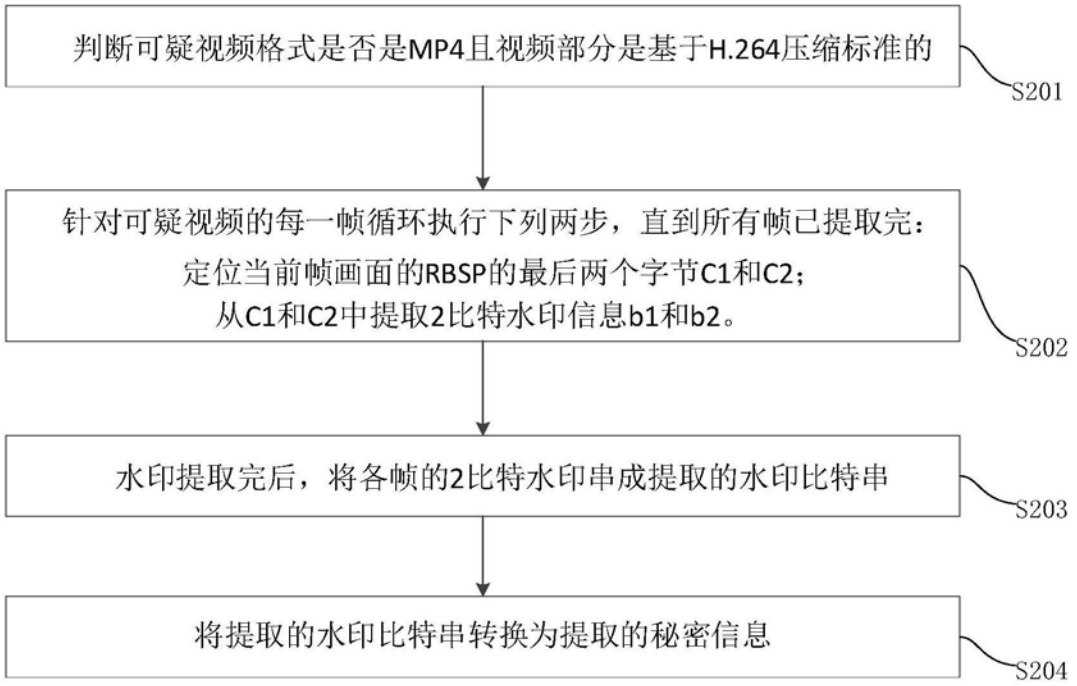

判断可疑视频格式是否是MP4且视频部分是基于H.264压缩标准的
S201
针对可疑视频的每一帧循环执行下列两步，直到所有帧已提取完：
定位当前帧画面的RBSP的最后两个字节C1和C2；
从C1和C2中提取2比特水印信息b1和b2。
S202
水印提取完后，将各帧的2比特水印串成提取的水印比特串
S203
将提取的水印比特串转换为提取的秘密信息
S204

图2

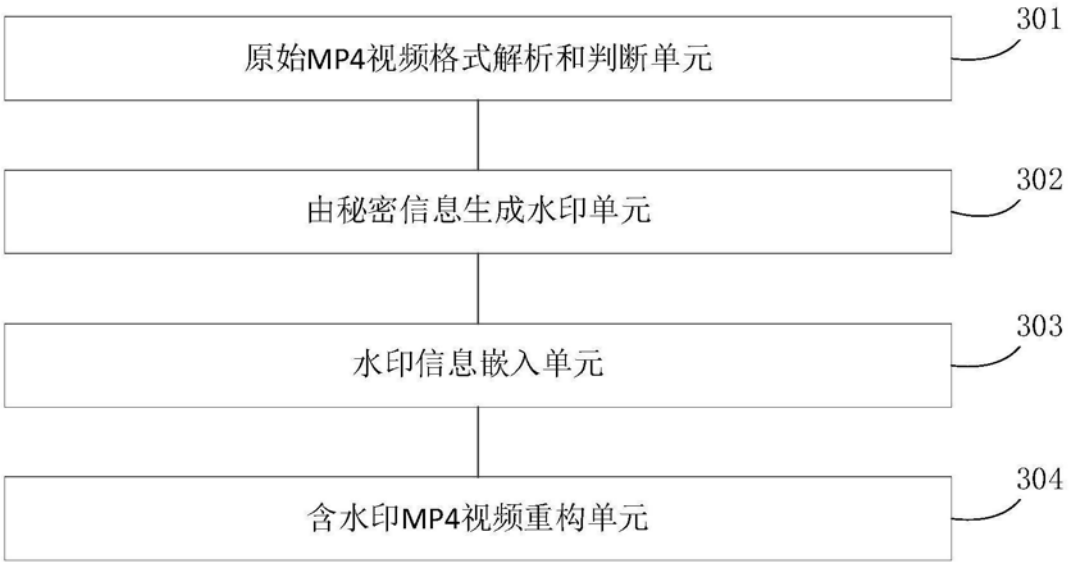

原始MP4视频格式解析和判断单元
301
由秘密信息生成水印单元
302
水印信息嵌入单元
303
含水印MP4视频重构单元
304

图3


算法处理器
401
嵌入算法存储器
402

图4

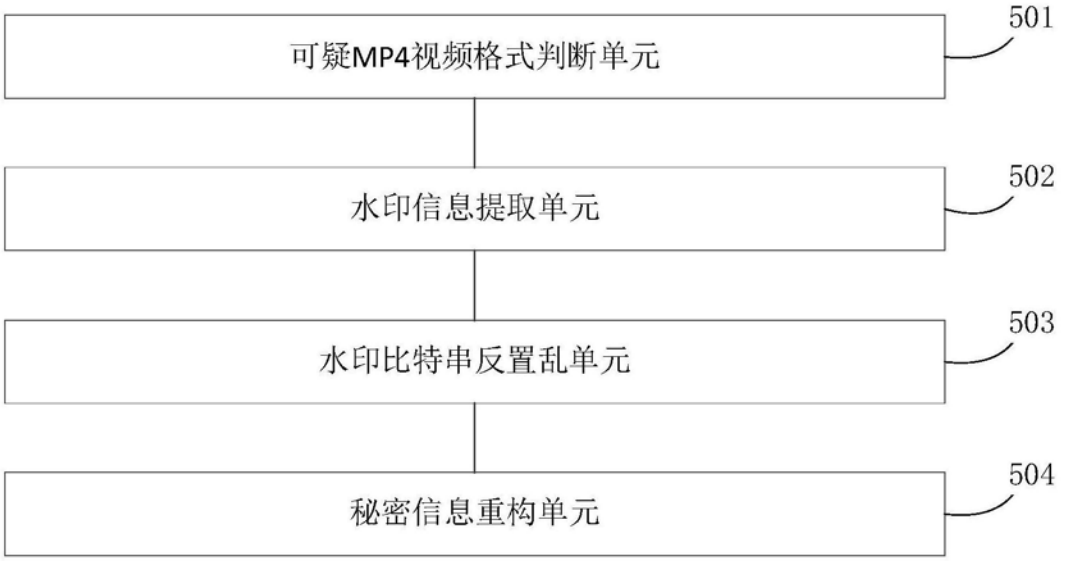

可疑MP4视频格式判断单元
501
水印信息提取单元
502
水印比特串反置乱单元
503
秘密信息重构单元
504

图5

图6