一种基于秘密共享与运动矢量的视频水印算法

徐甲甲[1],张卫明[1],俞能海[1],郭宝安[2],钱杨春[1]
(1.中国科学技术大学信息科学技术学院,安徽合肥 230027; 2. 航天信息股份有限公司,北京 100195)

摘 要: 本文在"压缩嵌入联合编码"框架下,提出一种基于秘密共享和信息分级保护的水印生成算法.与用算术编码压缩水印相比,本文的秘密共享方案在保证水印可认证性的前提下大幅度减少了信息嵌入量,同时对嵌入的信息依其重要程度进行分级保护,有效地增强了水印的鲁棒性.在此基础上,利用当前宏块与其周围宏块的运动矢量的相关性,提出一种基于运动矢量的自适应视频水印算法,可有效控制运动矢量的修改幅度,保证视频质量.实验表明该方案能保持很小的峰值信噪比损失和较好的视觉效果,且对于删帧攻击具有较强的鲁棒性.

关键词: 视频水印; 秘密共享; 运动矢量
中图分类号: TP391.41 **文献标识码:** A **文章编号:** 0372-2112 (2012) 01-0008-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.01.002

A Video Watermarking Algorithm Based on Secret Sharing and Motion Vectors

XU Jia-jia[1], ZHANG Wei-ming[1], YU Neng-hai[1], GUO Bao-an[2], QIAN Yang-chun[1]
(1. *MOE-Microsoft Key Laboratory of Multimedia Computing and Communication, University of Science and Technology of China, Hefei, Anhui* 230027, *China*; 2. *Aisino Corporation, Beijing* 100195, *China*)

Abstract: Under the framework of joint information embedding and lossy compression, an algorithm based on secret sharing and unequal protection is proposed. Comparing with arithmetic coding which compressed watermark length, our algorithm can dramatically reduce the amount of information bits embedded into video cover while guaranteeing watermarking authentication. Our algorithm not only improves compression efficiency but also adopts unequal protection strategy, thus improving watermark's robustness considerably. Furthermore, by making full use of dependency among neighbouring macroblocks, an adaptive watermarking algorithm based on motion vectors is proposed to effectively control motion vector's modification and guarantee video quality after watermarking. Experiments demonstrate that this algorithm not only keeps a small PSNR loss and satisfactory visual quality, but also shows resistance against frame-deletion attack.

Key words: video watermarking; secret sharing; motion vectors

1 引言

近几年随着 YouTube 等视频网站和网络电视的快速兴起,视频版权纠纷问题也日益严重.因而,作为视频版权保护的主要技术—视频水印受到越来越多的重视.针对视频水印的嵌入方法已有多种,其中常用方式是将水印嵌入视频的 DCT 系数中[1~3].将水印嵌在 DCT 系数上存在的问题是:P、B 帧均采用帧间预测编码,经过量化后大部分 DCT 系数为零,可利用的 DCT 系数有限;I 帧是视频的关键,对其修改容易引起误差累积从而对视频质量造成较大的影响.在 H.264 编码标准中,P、B 帧均是以 I 帧为参考帧通过预测编码得到的,运动矢量很丰富且与宏块具体内容无关,所以较之 DCT 系数而言在运动矢量中能嵌入更多信息,因此将水印嵌入运动矢量是研究热点之一[4~7].但是将水印嵌入运动矢量中也存在一定的局限性,即对运动矢量的大幅度修改会影响视频的视觉质量,甚至会影响能否正常解码,因此将水印嵌入运动矢量时,要保证修改幅度尽可能小,信息嵌入量不能过大.然而为了增强视频水印抗攻击性,常需要增加冗余信息,但冗余信息的引入又增加了要嵌入视频的信息量.为了在视频质量、水印抗攻击性取得一个折中,就需要寻找一种方式,在保证水印验证效果的前提下降低水印的嵌入量,因此"先压缩再嵌入"成为数字水印和其他信息隐藏技术中常用的手法.

"压缩嵌入联合编码"[8,9]作为近几年一种新兴的水印嵌入方式,其优良的性能框架受到学术界和工业界

收稿日期:2011-01-10;修回日期:2011-07-24
基金项目:国家科技重大专项子项目"新型移动多媒体音视频编解码关键技术研发"(No.2010ZX03004-003);国家自然科学基金(No.60933013,No.60803155);中央高校基本科研业务费专项资金(No.WK2100230002);国家科技支撑计划(No.2008BAH22B07)

的广泛关注. Maor 和 Wu 等人[8,9]在中对“压缩嵌入联合编码”做了理论分析,证明将信息先压缩再嵌入可在信息的嵌入量、失真和稳健性等性能指标之间达到最佳折中.本文在此框架下,通过采用(n,n)门限秘密共享体制[10~12]将原始水印分解为 n 份影子,任选一份影子作为待嵌入水印,其余 $n-1$ 份影子保存为验证密钥,从而使嵌入信息压缩为原始水印的 $1/n$,并且不影响水印的可验证性.但压缩率提高的同时意味着鲁棒性降低,为此我们考虑对嵌入的信息进行分级保护,根据信息的重要程度选用不同的保护策略[14],以达到压缩性能和鲁棒性的最佳折中.本文以嵌入一幅256级灰度水印图像为例,每个像素用8比特表示,但这8比特对该像素值的影响是不同的,最高位对像素值影响最大,依此为据我们用较多的冗余来保护较高位的数据.

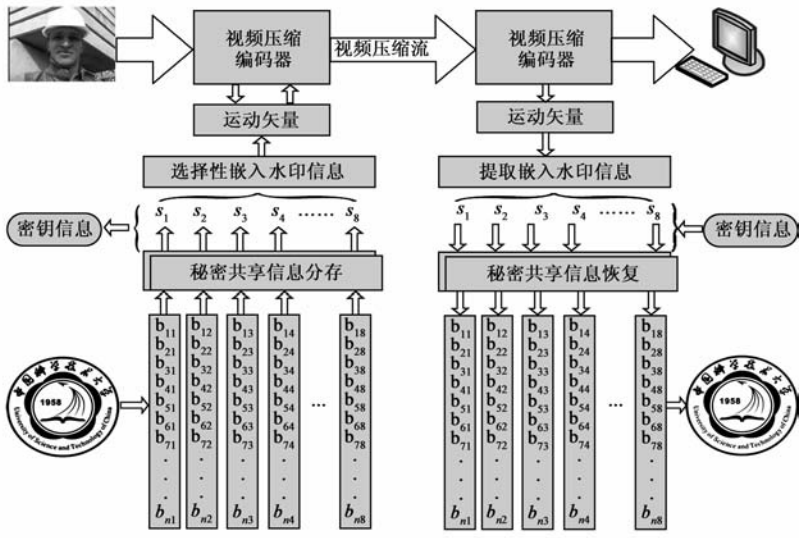

图1　视频水印嵌入的整体框架

由于当前宏块与周围宏块的运动矢量具有相关性,可利用这种相关性来控制当前宏块的修改幅度,基于上述思考我们提出一种自适应的基于运动矢量的视频水印嵌入算法.本文提出视频水印方案框架如图1.

2　基于秘密共享和信息分级保护的水印生成策略

2.1　影子水印生成算法

Shamir[10]提出的基于多项式插值的(n,n)门限秘密共享算法,具有三个特征:(1)将秘密信息分拆为 n 份影子;(2)当影子份数不少于 k 份时,可以恢复秘密信息,其中 $k\leqslant n$;(3)任何少于 k 份的影子都无法恢复秘密信息.

对于秘密信息 D,通过式(1)将其分成 n 份影子

$$q(x)=a_0+a_1x+a_2x^2+\cdots+a_{k-1}x^{k-1} \bmod 2^m \quad (1)$$

其中:$q(x)$是定义在有限域 $GF(2^m)$上的多项式,$a_1,\cdots,a_{k-1}\in GF(2^m)$是随机选取的数;$a_0$ 等于要分解的秘密信息 D,然后选择 $GF(2^m)$中 n 个不同的数 $x_1,x_2,\cdots,x_n$,代入式(1)计算 n 份影子:

$$s_i=q(x_i)\ ,\ 1\leqslant i\leqslant n \quad (2)$$

由拉格朗日插值法知,利用$(x_i,s_i),1\leqslant i\leqslant n$,中的任意 k 对数就可以恢复出多项式(1)的 k 个系数,进而可以恢复秘密消息 a_0.

本文的目的是利用秘密共享对水印进行压缩,所以我们采用(n,n)门限体制,即令多项式(1)中的 $k=n$,并且使用多项式的所有系数表示秘密消息,这样可以使一份影子的大小仅为原始秘密信息的 $1/n$.通常,秘密消息为二进制序列,通过填充消息可以使消息长度为 $m*n$ 的整数倍.然后我们将消息序列分成不相交的分组,每组包含 $m*n$ 比特,对每一组分别进行秘密共享.以第一组为例,设第一组消息为 $b_1,b_2,\cdots,b_{m\times n}$,每 m 比特消息可以映射成 $GF(2^m)$中的一个数,所以一组消息可以用 $GF(2^m)$中的 n 个数表示,记作 $a_1,\cdots,a_{n-1}$,用这 n 个数构造 $GF(2^m)$上的多项式:

$$q(x)=a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1} \bmod 2^m \quad (3)$$

然后在 $GF(2^m)$中选择 n 个不同的数 $x_1,x_2,\cdots,x_n$,代入式(3)计算 n 份影子:

$$s_i=q(x_i)\ ,\ 1\leqslant i\leqslant n \quad (4)$$

因为每个 s_i 需要用 m 比特表示,所以每份影子的大小是原消息分组的 $1/n$.若消息序列由 U 个 $m*n$ 长分组构成,则对每个分组重复上述过程,最后合并得到 n 份影子,每份影子由 U 个 $GF(2^m)$中的数组成,其大小为整个序列的 $1/n$.

假设原始水印为一幅256级灰度图像,尺寸为 $M\times N$.通过 Arnold 变化将图像置乱*,并将置乱后的图像表示成矢量,记作 $\boldsymbol{I}=[p_i],1\leqslant i\leqslant M\times N$.每个像素的灰度值是0~255之间的整数,可以用8位比特表示,记作 $p_i=[b_{i,1},b_{i,2},\cdots,b_{i,8}]$本文以左侧表示高位.这样,图像 $\boldsymbol{I}$ 可以分解成8个位平面,从高到底分别为 $\boldsymbol{I}_1,\boldsymbol{I}_2,\cdots,\boldsymbol{I}_8$,其中 $\boldsymbol{I}_j=[b_{1,j},b_{2,j},\cdots,b_{M\times N,j}],1\leqslant j\leqslant 8$;对各个位平面用上述的$(n,n)$秘密共享算法进行分解,则每个位平面被分解成 n 份影子,第 j 个位平面的 n 份影子记作 $\boldsymbol{S}_j=[s_{j,1},s_{j,2},\cdots,s_{j,n}],1\leqslant j\leqslant 8$;在每个位平面的 n 份影子中取一份,构成影子水印.不失一般性,对每个

* 置乱可以将提取过程中的失真均匀扩散到整幅图像,从而提高所提水印的视觉质量.

位平面都取第 i 份影子,则影子水印 $\boldsymbol{I}_s$ 为 $\boldsymbol{I}_s=[s_{1,i},s_{2,i},\cdots,s_{8,i}]$,其余 $n-1$ 份影子,由版权拥有者保存为认证密钥.

2.2 影子水印的分级保护

注意影子水印 $\boldsymbol{I}_s$ 已压缩为原始水印 $\boldsymbol{I}$ 的 $1/n$,显然嵌入 $\boldsymbol{I}_s$ 比直接嵌入 $\boldsymbol{I}$ 引起的失真要小,但是稳健性也降低了.另一方面,由于 $\boldsymbol{I}_s$ 很小,使我们有更多的嵌入冗余进行纠错保护来提高稳健性.注意到影子水印的 8 个分量重要性不同,高位平面对应的影子更为重要.我们可以采取分级保护策略,对重要信息予以重点保护.考虑到实际应用中视频水印系统对实时性的要求,嵌入算法的计算复杂度要尽量低,所以本文选择简单的重复编码进行纠错,即将每个比特重复扩展多次,解码时采用择多校验即可.对于影子水印的 8 个分量我们可采取多个级别的保护.为了实现简单,本文采用两个保护级别.设置阈值为 T,对 $\boldsymbol{I}_s$ 的前 T 个分量,使用 L 次扩展,对后 $8-T$ 的分量使用 R 次扩展,其中 $L>R$.用 S^r 表示对信号 S 的 r 次扩展,则扩展后的影子水印为

$$\boldsymbol{W}=[s_{1,1}^{L},\cdots,s_{T,1}^{L},s_{T+1,1}^{R},\cdots,s_{8,1}^{R}] \tag{5}$$

则待嵌入水印 $\boldsymbol{W}$ 与原始水印 $\boldsymbol{I}$ 的长度比为 $[TL+(8-T)R]/8n$.

使用者可以根据不同需求选择参数 n,T,L,R,在载体失真和水印稳健性之间进行折中.n 越大嵌入的信息量越小,因而载体失真越小,但水印稳健性越弱;T,L 或 R 越大,嵌入的信息量越大,载体失真也越大,但水印稳健性越强.

2.3 水印生成算法及可认证性

通过以上对秘密共享和分级保护策略的论述,水印算法的具体流程如下:

(1)预处理:将尺寸大小为 $M\times N$ 水印灰度图像置乱,置乱后的图像表示成矢量,记作 $\boldsymbol{I}=[p_i]$,$1\leqslant i\leqslant M\times N$,将每点像素值表示成 8 位比特,则有 $p_i[b_{i,1},b_{i,2},\cdots,b_{i,8}]$.将所有像素点按比特位从高到低分解成 8 个位平面,记为 $\boldsymbol{I}_1,\boldsymbol{I}_2,\cdots,\boldsymbol{I}_8$ 其中,$\boldsymbol{I}_j=[b_{1,j},b_{2,j},\cdots,b_{M\times N,j}]$,$1\leqslant j\leqslant 8$.

(2)信息秘密共享:通过式(3)对 $\boldsymbol{I}_j(1\leqslant j\leqslant 8)$,进行秘密共享,即可得到共享后的信息矩阵 $\boldsymbol{S}=\{\boldsymbol{S}_1\cdots\boldsymbol{S}_j\cdots\boldsymbol{S}_8\}$,其中 $\boldsymbol{S}_j=[s_{j,1},s_{j,2},\cdots,s_{j,n}]$,$1\leqslant j\leqslant 8$.从中选取 1 份对每个位平面都取第 i 份影子,构成影子水印 $\boldsymbol{I}_s=[s_{1,i},s_{2,i},\cdots,s_{8,i}]$;

(3)信息的分级保护:通过式(5)对 $\boldsymbol{I}_s$ 进行分级保护,得到扩展的影子水印 $\boldsymbol{W}$,作为待嵌入的水印信息,其余影子留作验证密钥;

(4)水印 $\boldsymbol{W}$ 的嵌入与提取:在第三节中详细描述;

(5)信息恢复:提出水印后,通过纠错解码,得到影子水印 $\boldsymbol{I}_s$ 的估计值,与作为密钥的 $n-1$ 份影子结合,通过拉格朗日插值算法恢复秘密信息 $\boldsymbol{I}$,将 $\boldsymbol{I}$ 反置乱就得到水印图像.

将秘密共享引入版权保护领域,取代传统的压缩技术,可以以更大的压缩率实现对水印的压缩,但是并不影响水印的可认证性.水印的可认证性,包括以下两方面:

(ⅰ)无密匙的非法用户不能认证:(n,n)门限秘密共享的安全性保证了验证者必须提供作为密钥的 $n-1$ 份影子,才能重构水印图像,完成认证.

(ⅱ)有密钥者不能对无水印信息的作品声称拥有版权.表面看起来,持有密钥的人拥有原始水印图像的绝大部分信息($n-1$ 份影子,信息占用率达到 $(n-1)/n$),即使从不含水印的载体中提取一份随机影子 $\boldsymbol{W}'$,也可能以很好的视觉质量重构原始水印图像.但事实上,秘密共享算法的安全性保证了在可行的计算能力下,由 $n-1$ 份影子得不到原始水印图像的任何有效信息.若作品中没有嵌入水印,则提取出信息可以认为是与水印图像无关的一条伪随机序列.实验结果如图 2 所示:(a)表示原始水印图像 $\boldsymbol{I}$;(b)由 $\boldsymbol{I}$ 的 $n-1$ 份影子和随机生成的一份伪影子(伪随机序列)合并所恢复的水印信息.

(a) 原始图像 (b) 恢复图像

图2 由伪影子恢复的水印图像

3 基于运动矢量的视频水印嵌入与提取算法

运动矢量信息是视频最重要信息之一,运动矢量的较大幅度改变会影响视频的视觉质量,甚至会影响能否正常解码,因此我们将水印嵌入运动矢量中要保证尽可能少的嵌入量及尽可能小的修改幅度.本文采用(n,n)门限秘密共享使得水印的嵌入量降为原来的 $1/n$,如何尽量小幅度地修改运动矢量成为关键问题.

3.1 视频水印嵌入

从 H.264 标准上看,当前宏块运动矢量的预测与其左、上及右上的三个相应的块相关性大;从视频内容上看,当前宏块与周围的宏块很大概率上是同时属于视频里的运动物体或背景.基于上述两点我们提出一种嵌入模板如图 3 所示:该模板由四个宏块组成,通过上面的分析,可以看出当前宏块运动矢量与其周围宏块的运动矢量在很大概率上是相关的,并且运动矢量的幅度相差不大,因此我们可以充分利用这种相关性来控制当前宏块的修改幅度.嵌入的思想:找出其周围宏块运动矢量幅度的最大值和最小值,结合当前宏块运动矢量值构造一个控制函数,满足条件则嵌入水印,不满足则跳到下一组模板.

嵌入的位置如图 4 所示,三组模板的示意图说明了水印的嵌入过程,可以看出每组模板中待嵌入水印位置即 $mv[i][j]$ 没有重复交叉的情况,这可以保证水印能够准确的提取;周围宏块可被多次使用,最大程度地利用了周围宏块,按照此思路水印可能的嵌入位置如图 4 所示,需要说明的是在本文中要求当前块与邻近块的尺寸相同.令

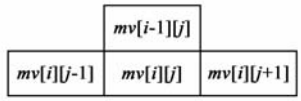

图3　嵌入水印方案示意图

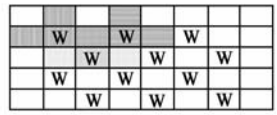

图4　水印的可能嵌入位置示意图

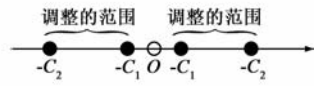

图5　运动矢量调整范围

$$A_{\max}=\max\{mv[i-1][j],mv[i][j-1],mv[i][j+1]\} \tag{6}$$

$$A_{\min}=\min\{mv[i-1][j],mv[i][j-1],mv[i][j+1]\} \tag{7}$$

我们有　$\Delta=\left|\sqrt{|A_{\max}\times A_{\min}|}-|mv[i][j]|\right|$　(8)

设置阈值 C_2,当 $\Delta<C_2$,当前分组嵌入 1 比特信息,否则跳到下一分组.通过调整 C_2 的大小可以控制对运动矢量的修改幅度.其步骤简述如下:

(1)首先确定模板的位置,获取每组模板内的宏块运动矢量,以计算 $A_{\max}$,$A_{\min}$和 Δ;

(2)通过判断 $\Delta<C_2$,确定该组模板是否嵌入水印,若满足条件则执行(3),否则跳到下一组判断;

(3)在条件(2)下,待嵌入的水印序列为 b_{ij},则有

(*a*)当 $b_{ij}=1$ 时,则要求该组模板 $\sqrt{|A_{\max}\times A_{\min}|}>|mv[i][j]|+C_1$,若不满足此条件,则调整 $mv[i][j]$,若 $mv[i][j]$为正则负向调整,反之则正向调整,使 $mv[i][j]$减小直到满足模板的要求;

(*b*)当 $b_{ij}=0$ 时,则要求该组模板 $\sqrt{|A_{\max}\times A_{\min}|}\leqslant|mv[i][j]|-C_1$,若不满足此条件,则调整 $mv[i][j]$,若 $mv[i][j]$为正则正向调整,反之则负向调整,使 $mv[i][j]$增大直到满足模板的要求;

(4)判断水印是否嵌入完毕.由式(8)及 $\Delta<C_2$ 可推知,嵌入水印调整当前宏块的 $mv[i][j]$时,调整的最大幅度为 C_2-C_1 如图 5 所示,即嵌入水印调整后的当前块运动矢量值为:

$$mv[i][j]\in\{mv[i][j],\ mv[i][j]\pm1,\cdots,mv[i][j]\pm(C_2-C_1)\} \tag{9}$$

通过 C_1,C_2 即可有效地控制嵌入水印时对宏块运动矢量的调整幅度,保证嵌入水印后的视频质量.

3.2　水印提取流程

由嵌入规则可知,将水印嵌入在当前宏块的运动矢量中,并没有修改其周围的运动矢量,因此按照嵌入时规则定义和计算 $A_{\max}$,$A_{\min}$和 Δ,提取的步骤如下:

(1)判断 $\Delta<C_2$ 是否成立,若成立则执行(2);否则跳到下一个可能嵌入的位置重新计算 $A_{\max}$,$A_{\min}$和 Δ;

(2)依据下面的公式提取水印:

$$b_{ij}=\begin{cases}1, & \sqrt{|A_{\max}\times A_{\min}|}>|mv[i][j]|+C_1\\ 0, & \sqrt{|A_{\max}\times A_{\min}|}<|mv[i][j]|-C_1\end{cases} \tag{10}$$

通过上述两步骤即可提取水印.

4　实验与分析

为了验证本文所提出的算法性能,在 Windows XP 平台上进行实验,H.264/AVC 参考软件 T264;水印图像尺寸为 80×80;在实验中有限域 $GF(2^m)$中取 $m=8$;通过秘密共享将水印分成 $n=200$ 份影子;考虑到实际应用视频水印系统对实时性的要求,嵌入的复杂度尽量低,本文在分级保护策略中选取 $T=2$,$L=2$,$R=1$;嵌入流程中控制参数 $C_1=1$,$C_2=3$;本文选取不同格式、不同尺寸及不同帧数的测试数据,包括 foreman,stefan,silent,coastguard,mobile,news.它们具有不同的运动复杂度和纹理复杂度,因而在相同的控制条件下每个视频序列有不同的嵌入容量,我们将一套水印均匀地嵌入到标准测试视频中.

4.1　主观评价

对水印的评价首先是视觉上的影响,不可见性是

(*a*1) 原始视频　(*b*1) 嵌入水印后　(*a*2) 原始视频　(*b*2) 嵌入水印后　(*a*3) 原始视频　(*b*3) 嵌入水印后

(*a*4) 原始视频　(*b*4) 嵌入水印后　(*a*5) 原始视频　(*b*5) 嵌入水印后　(*a*6) 原始视频　(*b*6) 嵌入水印后

图6　嵌入水印前后视频的视觉效果图

水印的基本要求,不可见性指的是嵌入水印后视频质量不能明显降低,至少人眼觉察不到.对标准视频的测试结果如图6所示,可以看出水印嵌入前后无明显视觉差异.

4.2 客观评价

峰值信噪比(PSNR)值是衡量视频质量的客观标准,可以在一定程度上反映视频的质量.实验中对表1所列的视频作了测试,结果如图7所示,可以看出嵌入水印对视频峰值信噪比造成的损失很小,从而保证了视频的质量.

4.3 攻击实验

这里通过一组视频序列验证算法的有效性.需要指出的是嵌入水印时我们采取的是循环嵌入策略,一段长视频可以循环多次嵌入水印,所以一般而言,视频序列越长水印信息提取的准确性越高.但在本实验中,我们采取在一定帧数内嵌入一套完整的水印,从中随机删去2帧,删帧后得到的实验结果如表1示.

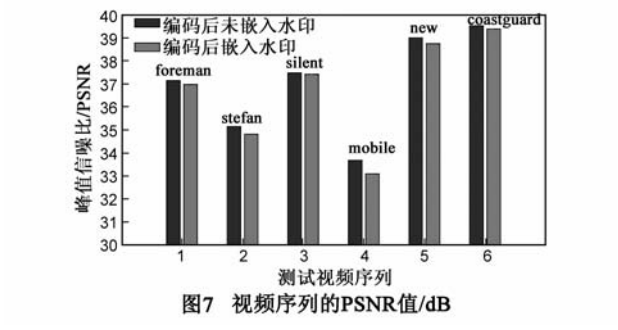

图7 视频序列的PSNR值/dB

表1 随机删一帧后检测出的效果

视频 删/帧数	Foreman 2/400	Molile 2/170	Stefan 2/170	Silent 2/260	New 2/300	Coastguard 2/170
检测效果 (随机删2帧)						

4.4 对比实验

在"压缩嵌入联合编码"框架下,我们做了对比实验,在对比实验中采用算术编码对水印进行压缩,将压缩后的水印嵌入视频序列中.原始水印大小为 $I=51.2$KB,则本文方法需要嵌入的信息量为:

$$\begin{aligned}&[TL+(8-T)R]\times I/8n\\&=[2\times 2+(8-2)\times 1]\times 51.2/8\times 200\\&=0.32\text{KB}\end{aligned}\tag{11}$$

(1)在嵌入相同水印信息的情况下,本文算法能够保证持有密钥者不能对无水印信息的作品声称拥有版权.如图8(b)所示,当密钥者持有 $n-1$ 份影子,信息占用率达到 $(n-1)/n$ 时是无法恢复水印图像的,因而保证了可认证性.但采用算术编码则无法保证,首先将水印图像分成 $n=200$ 份,然后分别对其进行算术编码,从压缩后的 n 份信息中选取一份作为水印,这时嵌入量即是原图像的 $1/n$,其余 $n-1$ 份作为密钥,实验表明,在此情况下密钥持有者用 $n-1$ 份信息恢复的水印如图8(c),可以看出采用算术编码无法保证可认证性.

(2)在保证持有密钥者不能对无水印信息的作品声称拥有版权的前提下,本文的算法嵌入量为0.32KB.


(a) 原始水印图 (b) 秘密共享n-1份恢复 (c) 算术编码n-1份恢复

图8 由n-1份信息恢复的水印图像

但当使用算术编码时,如图8(c)所示密钥信息为 $n-1$ 份是不能保证可认证性的,因此我们需要进一步减少密钥信息的份额,增加水印的嵌入量,通过实验我们发现当嵌入信息占压缩水印的3/4时(密钥信息为1/4),可保证水印的可认证性(如图9所示).本文中,算术编码的压缩效率 $\beta=87.3\%$,所以需要嵌入的信息量为:

$$3I\beta/4=3\times 51.2\times 0.873/4=33.52\text{KB}$$

由上可以看出在保证水印可验证的前提下,采用一般的压缩算法需要嵌入的信息量远大于本文提出的方法,因而嵌入过程会对载体引入更大的失真或者需要更多的帧才能嵌入一套水印.而需要更多帧嵌一套水印,则必然导致抗删帧攻击的能力下降,因而本文提出方案更具有实用性.

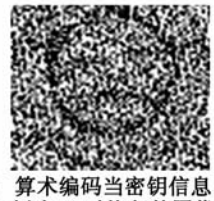
图9 算术编码当密钥信息比例为1/4时恢复的图像

5 结语

本文在"压缩嵌入联合编码"框架下,提出一种新的水印生成方法,通过秘密共享机制使得水印的嵌入量降为原水印的 $1/n$,而且对嵌入的信息进行分级保护,根据信息的重要程度选用不同的保护策略.另外,本文提出一种自适应的基于运动矢量的视频水印嵌入方案,利用当前宏块与其周围宏块的运动矢量间的相关性来控制当前宏块的修改幅度.本文的视频水印方案实现简单快速,具有失真小和抗删帧的特性.本文的水印生成算法具有一般性,也可用于其他的水印方案.

参考文献

[1] HY Huang, CH Yang, WH Hsu. A video watermarking technique based on Pseudo-3-D DCT and quantization index modulation[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(4): 625 – 637.

[2] 王国栋,刘粉林,刘媛,姚刚.一种能区分水印或内容篡改的脆弱水印算法[J].电子学报,2008,36(7):1349 – 1354.
Wang Guo-dong, Liu Fen-lin, Liu Yuan, Yao Gang. An image authentication scheme with discrimination of tampers on watermark or image[J]. Acta Electronica Sinica, 2008, 36(7): 1349 – 1354. (in Chinese)

[3] J Zhang, ATS Ho, G Qiu, P Marziliano. Robust video watermarking of H.264/AVC[J]. IEEE Trans on Circuits and Systems-II: Express briefs, 2007, 54(2): 205 – 209.

[4] M Kutter, F Jordan, T Ebrahimi. Proposal of A Watermarking Technique for Hiding/Retrieving Data in Cmpressed and Dcompressed Video[R]. Technical Report M2281, lSO/IEC document, JTCI/SC29/WGll, 1997.

[5] KA Saadi, A Bouridane, A Gessoum. H.264/AVC video authentication based video content[A]. I/V Communications and Mobile Network[C]. 2010 5th International Symposium on, 2010. 1 – 4.

[6] 张立和.隐藏信息检测与新型数字水印算法[D].北京:北京邮电大学博士学位论文,2004.5.
Zhang Li-he. Hiding Information Detection and Novel Digital Watermarking Algorithm[D]. Beijing: Beijing University of Posts and Telecommunications, 2004.5.

[7] 钱杨春.基于 AVS 标准的 IPTV 关键技术研究[D].合肥:中国科学技术大学硕士论文,2010.6.
Qian Yang-chun. Research on AVS-Based IPTV Key Techniques[D]. Hefei: University of Science and Technology of China, 2010.6. (in Chinese)

[8] A Maor, N Merhav. On joint information embedding and lossy compression[J]. IEEE Transactions on Information Theory, 2005, 51(8): 2998 – 3008.

[9] G Wu, EH Yang. Joint watermarking and compression using scalar quantization for maixmizing robustness in the presence of additive Gaussianattacks[J]. IEEE Trans Signal Process, 2005. 53(2): 834 – 844.

[10] A Shamir. How to share a secret[J]. Communication of the ACM, 1979, 22(11): 612 – 613.

[11] 温晓军,田原,牛夏牧.一种基于秘密共享的量子强盲签名协议[J].电子学报,2010,38(3):720 – 724.
Wen Xiao-jun, Tian Yuan, Niu Xia-mu. A strong blind quantum signature protocol based on secret sharing[J]. Acta Electronica Sinica, 2010, 38(3): 720 – 724. (in Chinese)

[12] GR Blakley. Safeguarding cryptographic keys[A]. Proc AFIPs I979 National Computer Conference[C]. New York, 1979. 313 – 317.

[13] A Mansouri, AM Aznaveh, F Torkamani-Azar, F Kurugollu. A low complexity video watermarking in H.264 compressed somain[J]. IEEE Transactions on Information Forensics and Security, Dec. 2010, 5(4): 649 – 657.

[14] 付正欣,郁滨,房礼国.一种新的多秘密分享视觉密码[J].电子学报,2011,39(3):714 – 718.
Fu Zheng-xin, Yu Bin, Fang Li-guo. A new multi-secret sharing visual cryptography[J]. Acta Electronica Sinica, 2011, 39(3): 714 – 718. (in Chinese)

[15] 金喜子,姜文哲.块级篡改定位的 JPEG 图像脆弱水印[J].电子学报,2010,38(7):1585 – 1589.
Jin Xi-zi, Jiang Wen-zhe. Fragile watermarking capable of locating tampered blocks in JPEG images[J]. Acta Electronica Sinica, 2010, 38(7): 1585 – 1589. (in Chinese)

[16] CC Chang, CC Lin, CH Lin, YH Chen. A novel secret image sharing scheme in color images using small shadow images[J]. Information Sciences . 2008. 178(11): 2433 – 2447.

[17] 秦拯,易叶青,林亚平.基于 JADE 算法的鲁棒性数字水印[J].电子学报,2008,36(6):1149 – 1153.
Qin Zheng, Yi Ye-qing, Lin Ya-ping. Robust watermark based on JADE algorithm[J]. Acta Electronica Sinica, 2008, 36(6): 1149 – 1153. (in Chinese)

作者简介

徐甲甲　男,1987 年生于安徽亳州.中国科学技术大学电子工程与信息科学系硕士研究生.研究方向为信息隐藏、视频编码与视频分析.
E-mail: xujiajia@mail.ustc.edu.cn

张卫明　男,1976 年生于河北定州.中国科学技术大学信息科学技术学院副教授,研究方向为信息隐藏、密码学和媒体内容安全.
E-mail: zwmshu@gmail.com

俞能海　男,1964 年生于安徽无为.中国科学技术大学信息科学技术学院教授,博士生导师.研究方向为图像处理与媒体内容安全、互联网信息检索与数据挖掘.
E-mail: ynh@ustc.edu.cn