基于小波变换的抵抗几何攻击的鲁棒视频水印*

赵 耀

(北京交通大学信息科学研究所, 北京 100044)

摘要 如何有效抵抗几何形变的攻击是当今数字水印研究的热点和难点之一. 提出一种能够有效抵抗几何攻击的鲁棒视频水印方案, 在其嵌入方案中, 提出了一种针对几何形变的不变量——平均交流能量(average AC energy, AAE). 利用该不变量, 并使用小波变换的空-频特性和人眼视觉特性嵌入有意义水印; 在水印提取方案中, 提出了最佳白化滤波器, 能够根据视频的统计特性设计白化滤波器的参数, 有效提高检测性能. 实验结果表明, 该水印方案有效提高了视频的视觉质量, 同时具有很强的抵抗几何形变攻击的能力, 对于其他攻击, 如时间维上的低通滤波、去帧等攻击也具有很强的鲁棒性.

关键词 数字水印 几何形变攻击 白化滤波器 小波变换

与相应的模拟数据相比, 数字媒体(数字音频、图像、数字视频)具有几个显著的优点: 质量高、编辑加工容易、拷贝不失真、传输容易等. 由于这些特点, 最近几年, 数字媒体技术的开发和应用有了爆炸性的发展. 然而, 数字媒体的无限次完美复制和通过网络的迅速传播给媒体原始拥有者的权益造成了潜在的威胁: 其艰苦劳动的成果有可能在一夜间被无偿地复制并传播到世界的每一个角落. 这种威胁将极大地打击数字媒体创作者的积极性. 因而数字媒体的版权保护成为一个迫切需要解决的问题.

数字水印是解决数字版权保护问题的有效办法. 它通过在原始数据中嵌入秘密信息——水印, 来证实该数据的所有权归属[1]. 水印可以是代表所有权的文字、所有人ID、二维图像、印章、随机序列等.

收稿日期: 2005-01-31; 接受日期: 2005-10-26

* 教育部博士点基金、国家自然科学基金(批准号: 60373028)及教育部新世纪优秀人才支持计划资助项目

数字水印应该具有隐蔽性、鲁棒性、抗攻击性、安全性等特性，而鲁棒性和抗攻击性是一个数字水印方案能够保护版权的最基本条件.

自 1994 年Schyndel等人发表了第一篇有关数字水印的文章[2]，数字水印的研究已引起了研究者的广泛关注. 目前大部分的数字水印方案能够抵抗常见的信号处理，如滤波、增强、数据压缩等攻击，但最近的研究表明，哪怕十分微弱的几何变换也能摧毁大多数的水印方案，特别是在盲水印系统中[3]. 因此，如何有效抵抗几何形变的攻击已成为数字水印的研究热点之一.

几何形变的攻击是恶意攻击者利用图像处理手段对加过水印的图像或视频进行几何形状的修改，如对图像进行旋转、平移、伸缩等仿射变换或随机几何变换. 这样攻击后，当发生版权纠纷需要提取水印时，攻击后的图像与水印信号之间失去了同步关系，使得二者的相关值很低，从而导致检测失败.

研究者已经提出了许多抵抗几何形变攻击的水印方案，主要可以分为三类: 一类方案是穷尽搜索法，即检测器将所有可能的几何形变都尝试一遍，以求最大相关值. 这种方法显然十分耗时，并且容易产生误报等问题[4].

另一类称之为几何反变换法. 我们知道，经过几何形变后，水印信号依然存在于图像之中，只不过水印信号与原图像之间的同步发生了变化，致使检测失败. 由此不难想像，如果我们能够知道攻击者所进行的几何变换，那么在水印检测时就能将攻击后的图像反变换回来，从而提取出水印. 这类算法按照是否需要原始图像，分为半盲相关法和盲相关法. 半盲检测算法在检测水印时借助原始图像，根据原始图像和攻击后的图像的特征点之间的对应关系来判断所经历的几何变换[4]或者用原始图像弥补几何变换(剪切、缩放等)引起的失真[5,6]. 实际上，借助原始图像也未必能解决水印同步问题，特别是当图像同时旋转和缩放或者经历打印、扫描过程时[7,8]，再者，检测的时候如果需要原始图像，这无疑会增加存储成本；盲相关法是抗几何攻击的水印算法的主流，在抵抗几何攻击检测水印时，不需要原始图像. 有些研究者提出一种基于模板的同步技术，针对仿射变换，通过在嵌入水印的过程中嵌入的特定的模板，在检测过程中利用此模板预测遭受的仿射变换[9]. 这些模板通常由频率峰值组成，频率峰值的位置组成特殊的形状，如圆形、方形等，检测过程中利用模板峰值位置的改变预测仿射变换. 这种方法的缺点是模板很容易被滤除[10]；Kutter提出了一种自参考方法(self-reference)[11]，将同一个水印在图像 4 个不同的位置分别嵌入，在检测过程中首先计算预测水印的自相关函数，由于水印的 4 次嵌入会使结果出现 9 个峰值，利用峰值位置改变可以预测仿射变换. 这种水印算法可以较好地抵抗旋转、伸缩、平移和改变长宽比等全局几何攻击以及打印扫描攻击，但是不能很好地抵抗滤波和镜像等攻击.

第三类方法称为几何不变量法. 即挖掘原始媒体中不随几何形变的特征或矩，并将水印信号调制在这些不变量中. 文献[12]采用Fourier-Mellin变换将图像

转换到RST(旋转、尺度和平移)不变域，然后在RST不变域嵌入水印．这种方法通过改变RST不变域的某些值，从而将水印嵌入RST不变域．同样，水印提取时将水印图像进行Fourier-Mellin变换，将图像转化到RST不变域，根据确定的水印嵌入方法提取水印．该方法由于要对图像先后进行Fourier变换和Mellin变换，同时由于受log-polar映射的分辨率的影响，对图像的恢复将造成很大的失真．Haitsma等人利用视频的平均亮度具有不随几何变换而改变的这一特性，将数字水印信号加入平均亮度中，取得了较为满意的几何鲁棒性[13]．本文作者在其基础上进一步针对时间维上的可能攻击进行了改进．而大量的实验结果表明，这种改变直流分量的方案虽然具有极高的鲁棒性，但在水印强度较高时，由于水印信号改变了每帧的平均亮度，故容易产生帧间闪烁现象，致使视频的视觉质量下　　降[14].

针对这一问题，我们提出了一种新的几何形变不变量——平均交流能量，并将水印信号嵌入其中，有效避免了帧间闪烁现象．同时利用小波变换和人眼视觉的掩蔽特性进一步提高图像质量；在水印提取时，利用白化噪声滤波器并推导其最佳参数，有效提高了水印的检测性能.

1　平均交流能量(AAE)

显然，如果我们能够将水印信号加入视频的几何不变量中，则该水印系统能够有效抵抗几何形变的攻击．下面我们将导出一种几何不变量.

对于视频序列的第t帧的像素点$f_t(x, y)$，经过某种几何变换，比如旋转和平移后，其位置坐标(x, y)改变为(x', y')，但其图像灰度值并不改变[1)]，即

$$f_t(x,y)=f_t(x',y'),\tag{1}$$

则

$$\sum_{x,y} f_t(x,y)=\sum_{x',y'} f_t(x',y'),\tag{2}$$

$$\sum_{x,y} f_t^2(x,y)=\sum_{x',y'} f_t^2(x',y').\tag{3}$$

定义 **1**　由于$\sum_{x,y} f_t^2(x,y)$是整幅图像的总能量，$\sum_{x,y}\left(\frac{1}{KL}\sum_{x,y} f_t(x,y)\right)^2=\frac{1}{KL}\left(\sum_{x,y} f_t(x,y)\right)^2$为图像的直流分量的能量，其中$K$, L为图像的长和宽．则我们称下式为图像$f_t(x, y)$的平均交流能量，用$v(t)$表示:

1) 对于连续图像来说，旋转或平移后，图像灰度值不改变；对于实际的数字图像，由于坐标点的离散化，灰度值会有少许变化，但本文使用的基本上是图像灰度的一些统计值，从统计意义上，尽管单个灰度值发生少许变化，但某些统计值基本保持不变

$$v(t)=\frac{1}{KL}\left(\sum_{x,y}f_t^2(x,y)-\frac{1}{KL}\left(\sum_{x,y}f_t(x,y)\right)^2\right). \tag{4}$$

AAE 具有以下特点:

1) 经几何形变后, 如果图像的长宽不变, 则 $v(t)$保持不变. 根据(2)和(3)式, 可证.

$$\begin{aligned}v'(t)&=\frac{1}{K'L'}\left(\sum_{x',y'}f_t^2(x',y')-\frac{1}{K'L'}\left(\sum_{x',y'}f_t(x',y')\right)^2\right)\\&=\frac{1}{KL}\left(\sum_{x,y}f_t^2(x,y)-\frac{1}{KL}\left(\sum_{x,y}f_t(x,y)\right)^2\right)=v(t).\end{aligned} \tag{5}$$

2) 如果图像大小以尺度因子 s 进行了伸缩, 则 $v(t)$仍保持不变.

$$\begin{aligned}v'(t)&=\frac{1}{s^2KL}\left(s^2\sum_{x,y}f_t^2(x,y)-\frac{1}{s^2KL}\left(s^2\sum_{x,y}f_t(x,y)\right)\right)^2\\&=\frac{1}{KL}\left(\sum_{x,y}f_t^2(x,y)-\frac{1}{KL}\left(\sum_{x,y}f_t(x,y)\right)^2\right)=v(t).\end{aligned} \tag{6}$$

3) 如果图像经历了几何变换, 而变换后新图像的某些周边部分用新值填充, 一般说来, 填充值为 0, $v(t)$发生改变.

$$v'(t)=\frac{1}{K'L'}\left(\sum_{x',y'}f_t^2(x',y')-\frac{1}{K'L'}\left(\sum_{x',y'}f_t^2(x',y')\right)^2\right)$$

$$=\frac{1}{K'L'}\left(\sum_{\text{图像部分}}f_t^2(x',y')+\sum_{\text{周边填充部分}}f_t^2(x',y')\right.$$

$$\left.-\frac{1}{K'L'}\left(\sum_{\text{图像部分}}f_t^2(x',y')+\sum_{\text{周边填充部分}}f_t^2(x',y')\right)^2\right)$$

$$=\frac{1}{K'L'}\left(\sum_{x,y}f_t^2(x,y)+\sum_{\text{周边填充部分}}f_t^2(x',y')\right.$$

$$\left.-\frac{1}{K'L'}\left(\sum_{x,y}f_t^2(x,y)+\sum_{\text{周边填充部分}}f_t^2(x',y')\right)^2\right)$$

$$= \frac{1}{K'L'}\left(\sum_{x,y} f_t^2(x,y) - \frac{1}{K'L'}\left(\sum_{x,y} f_t^2(x,y)\right)^2\right) \approx \frac{KL}{K'L'} v(t). \tag{7}$$

由此可见，虽然 $v(t)$发生了改变，但 $v(t)$和 $v'(t)$保持一种近似的线性关系.

综上，图像的 AAE 在大多数几何形变的攻击下保持不变，即使在有些情形下(即新图像的有些部分被填充，这种情况在实际中并不多见，因为这种情况容易暴露被攻击的迹象)发生了改变，也保持一种近似的线性关系，这对于相关检测来说影响不大. 因此可以预见，如果将水印信号嵌入 $v(t)$中必能有效抵抗几何形变的攻击.

2　水印嵌入方案

根据前面的分析，将水印信号嵌入 $v(t)$中能够有效抵抗几何形变的攻击. 现在的问题是: 如何将水印信号调制到平均交流能量上? 根据著名的 Parseval 定理，图像的能量在正交变换前后保持不变，而且经过正交变换后容易区分图像的直流能量和交流能量. 因此本文通过正交变换完成水印的嵌入. 水印嵌入流程如图 1 所示.

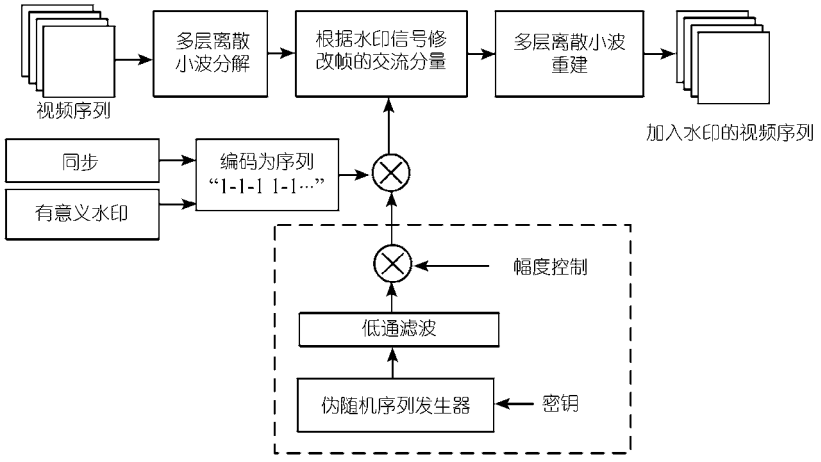

图 1　水印嵌入流程图

为了能够从任一帧开始获取水印信息同时抵抗去帧等恶意攻击，我们在视频序列中嵌入有意义水印的同时嵌入同步，并将同步和有意义水印交叠嵌入，如图 2 所示. 在实际方案中，同步信号是一个预先设定的比特串.

任何的水印和同步都可看成 1 和 0 组成的比特串，也就可看成 1 和–1 组成的比特序列，用$b_1b_2\cdots b_i\cdots$来表示. 我们使用扩频方式来隐藏这些信息串[1].

图 1 中的伪随机序列生成器用来产生两个伪随机序列，一个用于表示水印的信息比特，一个用于表示同步比特，两个伪随机序列的生成密钥和生成长度可以

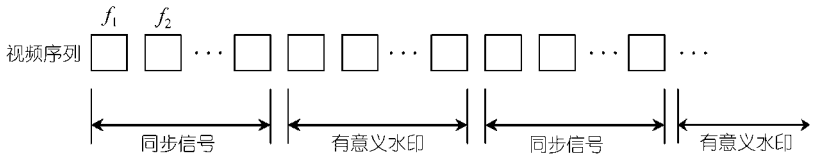

图 2 同步和有意义水印交叠嵌入示意图

不同.

这两个伪随机序列在统计意义上是Gauss白噪声，考虑到恶意攻击者可以在对视频信号影响不大的情况下利用时间轴方向的低通滤波等处理去除水印信号，本方案不直接采用白噪声，而是先对白噪声进行低通滤波. 考虑到时间维人眼视觉系统在低于 1Hz时敏感性下降这一特性[15]，我们所设计的低通滤波器的截止频率大约在 1Hz左右，其传递函数如下式:

$$H(Z)=\frac{1}{1-0.4505Z^{-1}-0.988Z^{-2}+0.0429Z^{-3}+0.5112Z^{-4}}. \tag{8}$$

由于同步比特的伪随机序列和水印比特的伪随机序列的构造、嵌入和提取等过程类似，故在后文中统一用 $W(t)$表示.

为简化后续的相关检测，要求在构造 $W(t)$时具有零均值，即 $EW(t)=0$，并且可以通过控制其最大幅度 Am 来控制水印的嵌入强度.

水印的嵌入过程就是将水印信号 $W(t)$嵌入视频的 AAE 序列 $v(t)$中，即通过水印信号修改每一帧的交流成分. 为此，对于 128×128 大小的图像帧，使用双正交小波进行 7 层小波分解. 所用的分解和合成滤波器的系数如表 1 所示.

表 1 本文采用的双正交 9/7 滤波器组

n	分解滤波器		重建滤波器	
	低通滤波器 $h(n)$	高通滤波器 $g(n)$	低通滤波器 $s(n)$	高通滤波器 $r(n)$
0	0.8527	0.7885	0.7885	0.8527
+1, −1	0.3774	−0.4181	0.4181	−0.3774
+2, −1	−0.1106	−0.0407	−0.0407	−0.1106
+3, −3	−0.0238	0.0645	−0.0645	0.0238
+4, −4	0.0378			0.0378

根据图 1，对于某个信息比特b_i，其嵌入水印的过程，就是将水印的伪随机序列$W(t)$调制到$v(t)$上，即

$$v_W(t)=v(t)+b_i\cdot W(t), \tag{9}$$

即要对原来的$v(t)$增加$b_i\cdot W(t)$，根据(4)式，有

$$v(t)+b_i\cdot W(t)=\frac{1}{KL}\left(\sum_{x,y}f_t^2(x,y)-\frac{1}{KL}\left(\sum_{x,y}f_t(x,y)\right)^2\right)+b_i\cdot W(t)$$

$$= \frac{1}{KL}\left(\sum_{x,y} f_t^2(x,y) - \frac{1}{KL}\left(\sum_{x,y} f_t(x,y)\right)^2 + KL \cdot b_i \cdot W(t)\right)$$

$$= \frac{1}{KL}(E_{AC}(t) + KL \cdot b_i \cdot W(t)), \tag{10}$$

其中 $E_{AC}(t) = \sum_{x,y} f_t^2(x,y) - \frac{1}{KL}\left(\sum_{x,y} f_t(x,y)\right)^2$ 为该帧的交流能量. 因此, 只要将该帧的交流能量进行修改, 且修改量为$KL \cdot b_i \cdot W(t)$, 即可完成对$v(t)$的调制.

小波变换后, 在修改交流能量时, 考虑到系统的抗攻击能力(不选包含直流能量的 LL7, 同时不选最高频系数以抵抗空间低通滤波的攻击), 仅选取第 2~7 层的 AC 系数进行修改. 修改的范围如图 3 所示. 图中阴影部分为选取的修改区域.

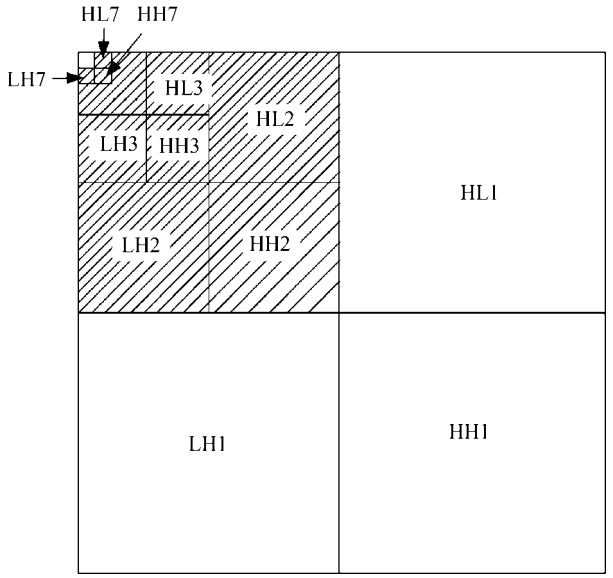

图 3　待修改的小波系数

设Ω 为所有选取的交流系数点的坐标的集合, 则选定交流系数的能量为 $\sum_{(u,v)\in\Omega} F_t^2(u,v)$. 对于选定的系数, 假设系数修改前后的关系为

$$F_{tW}(u,v) = \alpha \cdot F_t(u,v), \tag{11}$$

其中α为修改比例因子, 根据水印嵌入前后交流能量的关系有

$$\sum_{(u,v)\in\Omega} F_{tW}^2(u,v) = \alpha^2 \sum_{(u,v)\in\Omega} F_t^2(u,v) = \sum_{(u,v)\in\Omega} F_t^2(u,v) + KL \cdot b_i \cdot W(t). \tag{12}$$

由此可得

$$\alpha = \sqrt{\frac{\sum_{(u,v)\in\Omega} F_t^2(u,v) + KL \cdot b_i \cdot W(t)}{\sum_{(u,v)\in\Omega} F_t^2(u,v)}}. \tag{13}$$

本文之所以选取小波分解，是因为小波分解具有优良的空-频分解特性. 在空间域变化较大的区域，其对应的小波分解系数$F_t(u, v)$的绝对值也较大，按照(11)式，在这些点上进行的修改也较大；反之，在变化较小的区域进行较小的修改. 而对人眼视觉特性的研究发现，人眼对于图像中复杂纹理区域变化的敏感程度比简单区域的低[15]. 因此，这种修改方案与人眼的视觉特性相一致.

当修改系数结束后，通过小波重建，得到空间域的图像帧，从而完成该帧水印信号的嵌入. 视频所有帧嵌完后，也就完成对该视频的水印嵌入.

3 水印提取方案

图 4 给出了水印提取的过程. 水印的提取无须从视频的第 1 帧开始，可以从视频的任一帧开始. 检测器首先逐帧检测同步的存在，若从当前点直到结束均检测不到同步，则证明此视频中不存在水印. 若检测到同步，则计算相邻两同步之间的帧数是否正确. 若正确，则提取水印；否则，则可能遭到了去帧或增帧等攻击，这部分检测不出正确的水印，需要检查下面两同步，…，依次类推. 在同步检测和水印比特的提取中，都采取互相关的方法，将在后面统一论述.

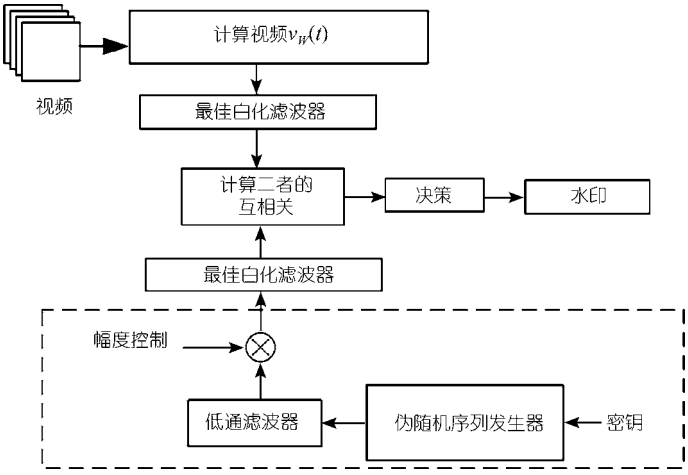

图 4 水印提取流程图

首先利用(4)式计算该视频的平均交流能量序列$v_W(t)$，同时根据版权拥有者手中的密码产生表示水印比特和同步比特的伪随机序列$W(t)$，计算$v_W(t)$与$W(t)$之间的互相关来检测水印和同步是否存在，如下式:

$$R_{v_W,W}(0)=E[v_W(t)W(t)]=E[(v(t)+b_i\cdot W(t))W(t)]$$

$$=E[v(t)W(t)]+b_iE[W(t)^2]=R_{v,W}(0)+b_iE[W(t)^2]. \tag{14}$$

$v(t)$与 $W(t)$是相互独立的, 则

$$R_{v,W}(0)=E(v(t)W(t))=E(v(t))\cdot E(W(t))=0. \tag{15}$$

因此, 若视频没有嵌入水印, 则(14)式为 0; 否则, 等于$b_iE[W(t)^2]$. 因此我们能够通过设置阈值$E[W(t)^2]/2$来判断水印或同步比特的存在, 并根据正负号判定 0 或 1.

需要说明的是, 在实际计算(14)和(15)式中, $v(t)$, $v_W(t)$, $W(t)$的序列长度都有限, (15)式(也即$v(t)$和$v_W(t)$的互相关)的估计公式实际为

$$\mathrm{Cor}(v(t),W(t))=\frac{1}{N}\sum_{t=0}^{N-1}v(t)\cdot W(t), \tag{16}$$

其中 N 为伪随机序列的长度.

(16)式的值就不一定为 0, 其方差的大小直接影响检测的性能[16].

为提高水印的检测性能, 即减少(16)式的方差, 我们采用白化滤波器提高性能. 下面我们将介绍白化滤波器, 并推导其最佳参数.

4　最佳白化滤波器的设计

首先, 对(16) 式进行定量分析, 求出其方差.

定理 **1**　(16) 式是一个零均值的变量, 其方差为

$$\mathrm{Var}\left[\mathrm{Cor}(v(t),W(t))\right]=\frac{2}{N^2}\sum_{\Delta=1}^{N-1}(N-\Delta)\cdot R_v(\Delta)R_W(\Delta)+\frac{1}{N}R_v(0)R_W(0), \tag{17}$$

其中$R_v(\Delta)$, $R_W(\Delta)$为$v(t)$和$W(t)$的自相关.

证　$\mathrm{Cor}(v(t), W(t))$的均值为

$$E\left[\mathrm{Cor}(v(t),W(t))\right]=E\left[\frac{1}{N}\sum_{t=0}^{N-1}v(t)\cdot W(t)\right]$$

$$=\frac{1}{N}\sum_{t=0}^{N-1}E\left[v(t)\cdot W(t)\right]=E\left[v(t)\right]\cdot E\left[W(t)\right]=0, \tag{18}$$

其方差为

$$\mathrm{Var}\left[\mathrm{Cor}(v(t),W(t))\right]=E\left[\mathrm{Cor}(v(t),W(t))^2\right]=E\left[\left(\frac{1}{N}\sum_{t=0}^{N-1}v(t)\cdot W(t)\right)^2\right]$$

$$=\frac{1}{N^2}E\left[\left(\sum_{m=0}^{N-1}v(m)\cdot W(m)\right)\cdot\left(\sum_{n=0}^{N-1}v(n)\cdot W(n)\right)\right]=\frac{1}{N^2}\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}E\left[v(m)W(m)v(n)W(n)\right]$$

$$= \frac{1}{N^2}\sum_{m=0}^{N-1}\sum_{n=0}^{N-1} E\left[v(m)v(n)\right]E\left[W(m)W(n)\right] = \frac{1}{N^2}\sum_{m=0}^{N-1}\sum_{n=0}^{N-1} R_v(m-n)\cdot R_W(m-n). \quad (19)$$

下面我们来简化(19)式中的两次求和. 将 $\sum_{m=0}^{N-1}\sum_{n=0}^{N-1} R_v(m-n)\cdot R_W(m-n)$ 展开为

$$\begin{array}{llll} R_v(0-0)R_W(0-0) & +R_v(0-1)R_W(0-1) & +R_v(0-2)R_W(0-2) & +\cdots \quad +R_v(0-N+1)R_W(0-N+1) \\ +R_v(1-0)R_W(1-0) & +R_v(1-1)R_W(1-1) & +R_v(1-2)R_W(1-2) & +\cdots \quad +R_v(1-N+1)R_W(1-N+1) \\ \vdots & \vdots & \vdots & \vdots \\ +R_v(N-1-0)R_W(N-1-0) & +R_v(N-1-1)R_W(N-1-1) & +R_v(N-1-2)R_W(N-1-2) & +\cdots \quad +R_v(N-1-N+1)R_W(N-1-N+1). \end{array}$$

观察上面展开式的规律, 即可得到

$$\sum_{m=0}^{N-1}\sum_{n=0}^{N-1} R_v(m-n)\cdot R_W(m-n) = \sum_{\Delta=-(N-1)}^{N-1}(N-|\Delta|)\cdot R_v(\Delta)R_W(\Delta), \quad (20)$$

考虑到 $R_v(-\Delta) = R_v(\Delta)$ 和 $R_W(-\Delta) = R_W(\Delta)$, 有

$$\sum_{m=0}^{N-1}\sum_{n=0}^{N-1} R_v(m-n)\cdot R_W(m-n) = 2\cdot\sum_{\Delta=1}^{N-1}(N-\Delta)\cdot R_v(\Delta)R_W(\Delta) + N\cdot R_v(0)R_W(0). \quad (21)$$

因此(19)式就变成

$$\mathrm{Var}\left[\mathrm{Cor}(v(t),W(t))\right] = \frac{2}{N^2}\sum_{\Delta=1}^{N-1}(N-\Delta)\cdot R_v(\Delta)R_W(\Delta) + \frac{1}{N}R_v(0)R_W(0). \quad (22)$$

由(22)式可知, 当 N 为有限长时, 两信号互相关的方差并不一定为 0, 水印检测的错误比特率(BER)往往取决于这个值, 很显然这个值越小越好.

从检测的理论, 相关检测器在线性时不变、频率不发散、加性Gauss白噪声信道是最优的[16]. 但在我们的系统中, 视频平均交流能量序列是一个高度相关的量, 且经过低通滤波处理的伪随机信号也是高度相关的. 为了达到更好的检测性能, 我们在检测之前, 首先使用白化滤波器对$v_W(t)$和水印信号$W(t)$进行白化, 所使用的白化滤波器是一阶参数化FIR滤波器, 如下式:

$$G(z) = 1 - aZ^{-1}. \quad (23)$$

那么如何选择参数 a 才能获得最佳性能呢? 也即如何尽可能减少白化后两信号的互相关的方差? 我们有如下定理.

定理 2 设 $v(t)$经白化滤波后记为 $v'(t)$, $W(t)$经白化滤波后记为 $W'(t)$, 则白化后二者互相关的方差变为

$$\begin{aligned} &\mathrm{Var}\left[\mathrm{Cor}(v'(t),W'(t))\right] \\ &= \frac{2}{N^2}\sum_{\Delta=1}^{N-1}\Big[(N-\Delta)\cdot\left((1+a^2)R_v(\Delta) - aR_v(\Delta-1) - aR_v(\Delta+1)\right) \\ &\quad\cdot\left((1+a^2)R_W(\Delta) - aR_W(\Delta-1) - aR_W(\Delta+1)\right)\Big] \end{aligned}$$

$$+\frac{1}{N}\left[\left((1+a^2)R_v(0)-2aR_v(1)\right)\cdot\left((1+a^2)R_W(0)-2aR_W(1)\right)\right]. \tag{24}$$

证　由(23)式可知, 经过白化处理后, 平均交流能量和水印信号变为

$$v'(t)=v(t)-av(t-1)\,, \tag{25}$$

$$W'(t)=W(t)-aW(t-1)\,. \tag{26}$$

由定理 1,

$$\mathrm{Var}\left[\mathrm{Cor}(v'(t),W'(t))\right]=\frac{2}{N^2}\sum_{\Delta=1}^{N-1}(N-\Delta)\cdot R_{v'}(\Delta)R_{W'}(\Delta)+\frac{1}{N}R_{v'}(0)R_{W'}(0)\,. \tag{27}$$

因为

$$\begin{aligned}R_{v'}(\Delta)&=R_{v'}(m-n)=E\left[v'(m)v'(n)\right]=E\left[(v(m)-av(m-1))\cdot(v(n)-av(n-1))\right]\\&=E\left[v(m)v(n)-av(m-1)v(n)-av(m)v(n-1)+a^2v(m-1)v(n-1)\right]\\&=(1+a^2)R_v(m-n)-aR_v(m-n-1)-aR_v(m-n+1)\\&=(1+a^2)R_v(\Delta)-aR_v(\Delta-1)-aR_v(\Delta+1).\end{aligned} \tag{28}$$

同样

$$R_{W'}(\Delta)=(1+a^2)R_W(\Delta)-aR_W(\Delta-1)-aR_W(\Delta+1)\,. \tag{29}$$

则(27)式变为

$$\begin{aligned}&\mathrm{Var}\left[\mathrm{Cor}('v(t),W(t))\right]\\&=\frac{2}{N^2}\sum_{\Delta=1}^{N-1}\left[(N-\Delta)\cdot\left((1+a^2)R_v(\Delta)-aR_v(\Delta-1)-aR_v(\Delta+1)\right)\right.\\&\quad\left.\cdot\left((1+a^2)R_W(\Delta)-aR_W(\Delta-1)-aR_W(\Delta+1)\right)\right.\\&\quad\left.+\frac{1}{N}\left[\left((1+a^2)R_v(0)-2aR_v(1)\right)\cdot\left((1+a^2)R_W(0)-2aR_W(1)\right)\right].\end{aligned}$$

显然, 利用最小二乘法, 将(24)式对参数 a 求导, 即可求出参数 a 的最佳取值. 但定理 2 给出的公式依然复杂, 我们将分情况进行简化.

情况 1: 在大多数情况下, 视频的帧间信号的自相关可建模为一个指数函数曲线[17]. 因此假设$v(t)$和$W(t)$的归一化自相关函数可用 $\rho_v(\Delta)=\alpha^{|\Delta|}$, $\rho_W(\Delta)=\beta^{|\Delta|}$ 来表示, α, β为两个与信号本身有关的常数. 则(24)式变为

$$\begin{aligned}&\mathrm{Var}\left[\mathrm{Cor}(v'(t),W'(t))\right]\\&=\frac{R_v(0)R_W(0)}{N}\left\{\frac{2}{N}\cdot\frac{(\alpha\beta)^{N-1}-N+(N-1)(\alpha\beta)^{-1}}{[1-(\alpha\beta)^{-1}]^2}\right.\\&\quad\left.\cdot\left[(1+a^2)-a\cdot\alpha^{-1}-a\cdot\alpha\right]\cdot\left[(1+a^2)-a\cdot\beta^{-1}-a\cdot\beta\right]\right.\end{aligned}$$

$$+(1+a^2-2a\alpha)(1+a^2-2a\beta)\Big\}. \tag{30}$$

利用最小二乘法，可得到最优参数a，尽管我们可以得到一个封闭的形式，但其表达式仍然复杂而失去实际意义. 为使其具备实际意义，我们在不同α和β的情况下，给出最佳参数a与α的关系曲线，如图 5 所示.

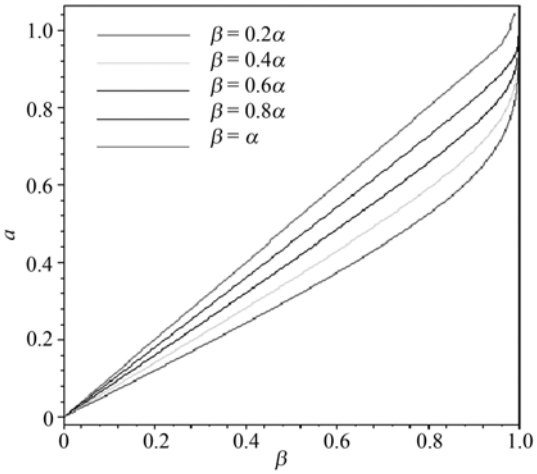

图 5 不同α和β的情况下最佳参数a与α的关系曲线

在许多情况下，信号的自相关可以用指数形式表示，这时我们可以利用图 5 选择最佳参数.

情况 2: 如果$\rho_V(\Delta)=1$，则(24)式变为

$$\begin{aligned}&\mathrm{Var}\left[\mathrm{Cor}(v'(t),W'(t))\right]\\&=\frac{1}{N}R_v(0)(1-a)^2\cdot\left[\frac{2}{N}R_v(0)\sum_{\Delta=1}^{N-1}\left[\left((1+a^2)R_W(\Delta)-aR_W(\Delta-1)-aR_W(\Delta+1)\right)\right]\right.\\&\left.+\left((1+a^2)R_W(0)-2aR_W(1)\right)\right].\end{aligned} \tag{31}$$

显然a=1 使(31)式为 0，即互相关的方差达到最小. 这说明当$\rho_v(\Delta)=1$时，不管水印信号的统计特性如何，最佳白化滤波器都是$G(Z)=1-Z^{-1}$.

5 实验结果

下列实验中使用两个视频测试序列: Philips 公司的测试序列和标准测试序列“Salesman”. Philips 测试序列是由不同的场景拼接而成，场景跳变较多，序列长为 12300 帧，是一个画面复杂的视频序列. 这两个序列都采用 YUV 格式存储，图像

大小为 128×128, 每一基色的每个像素值用 8 比特表示. “Salesman”序列长为 12572 帧, 场景变化相对较少.

所用水印信号的最大幅度为 $Am = 512$, 表示每一个信息比特的伪随机序列 PRS 的长度为 $N = 4000$. 在这种情况下, 两个序列能够成功检测到水印, 而且加入水印的视频没有视觉上的闪烁感. 对 Philips 测试序列, 嵌入水印的整个视频的平均峰峰信噪比 $PSNR$=48.6 dB, 对“Salesman”, 平均峰峰信噪比 $PSNR$=49.1 dB.

下面实验中分别对白化滤波器的性能、检测性能、抗几何攻击性能、抗空间时间低通滤波等性能进行测试.

实验 **1**　本实验测试最优白化滤波器的设计和性能. 为此我们在提取水印时分别使用不同的白化滤波器参数 a. 采用归一化互相关值的分布曲线衡量检测性能. 一般说来, 分布曲线越尖锐, 则方差越小, 性能越好. 对 Philips 测试序列, 其实验结果如图 6(a)所示. 从实验结果看, $a = 0$, 也即不使用白化滤波器时, 性能显然不及 $a = 0.8$, $a = 1$, $a = 1.2$ 等情况. 在 a 的各种取值中, $a = 1$ 获得最佳性能.

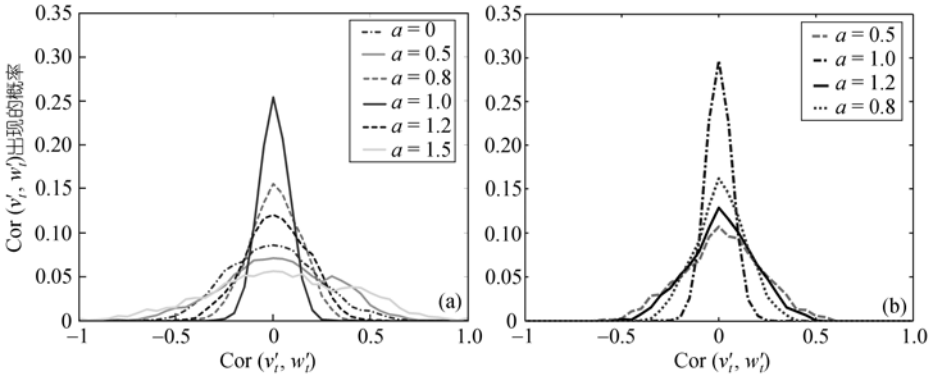

图 6　参数 a 不同取值时相关值分布曲线

(a) Philips 测试序列; (b) “Salesman” 测试序列

对Philips视频的$v(t)$序列进行统计, 其归一化自相关函数的计算结果如下: $\rho_v(0) = 1$, $\rho_v(1) = 0.9965$, $\rho_v(2) = 9919$, …, 基本符合定理 2 的第 2 种情况, 即$\rho_v(\Delta) = 1$, 所以此时的最佳白化滤波器为 $G(Z) = 1 - Z^{-1}$, 这与实验结果相符. 对“Salesman”测试序列, 也得到类似的结论, 如图 6(b)所示.

实验 **2**　该实验主要测试本水印方案的抗几何攻击能力. 对嵌入水印的视频序列分别进行如下攻击: 将每帧图像旋转 45°, 平移 20×20 像素及将其缩小为 64×64 大小. 在前两种攻击中, 我们保持原图像的大小不变, 因此原图像的某些部分被剪切, 新图像的有些部分可能填 0. 图 7 给出了两个测试序列在三种情况下的互相关. 在平移情况下, 正确位置点的相关值略有降低, 但我们仍然可以正

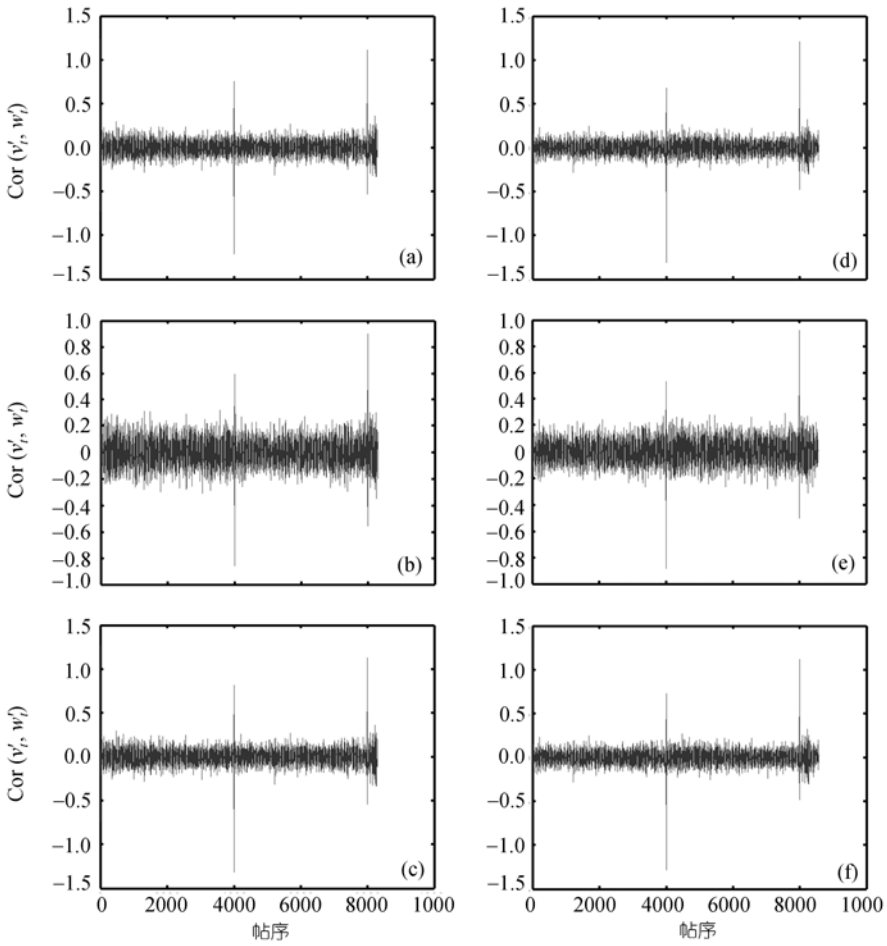

图 7 在三种攻击下的互相关

(a) Philips 序列旋转 45°; (b) Philips 序列移位 20×20 像素; (c) Philips 序列缩小为 64×64 大小; (d) “Salesman” 序列旋转 45°; (e) “Salesman”序列移位 20×20 像素; (f) “Salesman”序列缩小为 64×64 大小

确提取水印.

实验 **3** 本实验测试本方案的抗其他攻击的能力. 本文在时间维对加入水印的平均交流能量序列$v_W(t)$进行低通滤波, 所用滤波器为$H(z) = 0.5+0.5z^{-1}$. 另外, 使用低通滤波模板 $h=\frac{1}{5}\begin{bmatrix}0 & 1 & 0\\ 1 & 1 & 1\\ 0 & 1 & 0\end{bmatrix}$ 对视频的每帧进行滤波. 攻击后, 互相关如图 8 所示. 由实验结果可见, 空间域上的滤波攻击对检测影响不大, 而时间维的滤波攻击, 在正确位置点的相关值的幅度明显减少, 但仍可与非嵌入点的相关值区别开来.

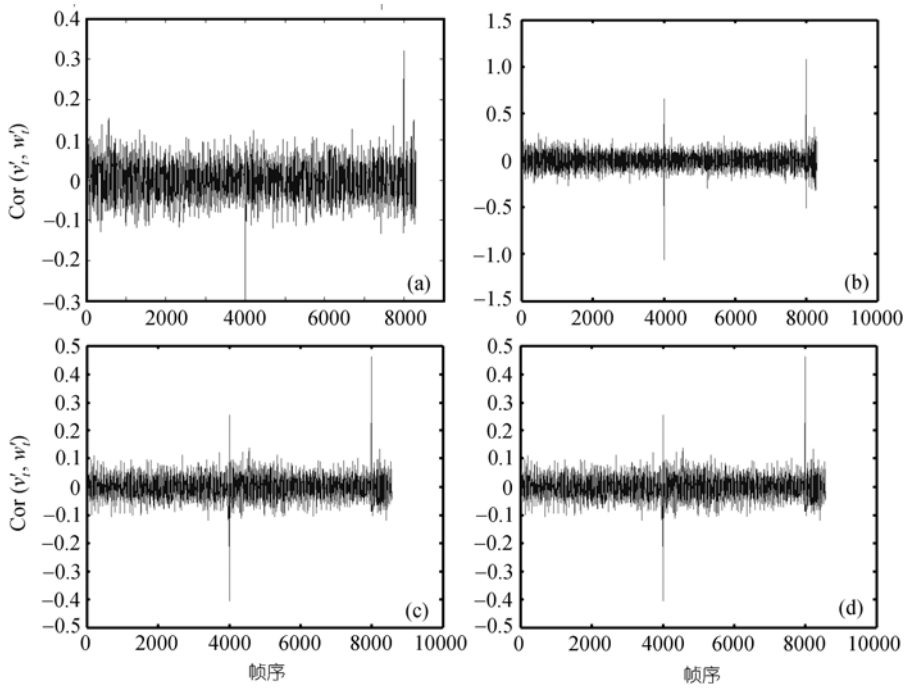

图 8　本方案对低通滤波的抵抗性能

(a) Philips 序列经时间维滤波攻击后的互相关情况; (b) Philips 序列经空间域滤波攻击后的互相关情况; (c) “Saleman”序列经时间维滤波攻击后的互相关情况; (d) “Saleman”序列经空间域滤波攻击后的互相关情况

6　结论

本文设计的视频水印方案具有以下特点:

1) 提出了一种几何不变量——平均交流能量, 并将水印信号嵌入其中, 不仅克服了文献[13, 14]中的帧闪现象, 而且具有很高的抗几何攻击的能力;

2) 利用小波分解的空-频特性, 在伪随机序列的构造、嵌入强度和嵌入点等方面, 充分考虑人眼视觉特性, 将水印信号造成的视觉失真降至最小;

3) 在水印嵌入方案中, 引入同步, 使得水印提取可以从任一帧开始, 同时可以有效抵抗丢帧、并帧、增帧等恶意攻击, 同时采用低频伪随机序列, 有效抵制时间维上的低通滤波攻击;

4) 在水印提取方案中, 采用白化滤波器提高检测性能, 并推导了最佳参数.

致谢　本文的部分成果得到了荷兰 Delft University of Technology 的 Lagendijk 教授和 Philips Research (Eindhoven)的 Ton Kalker 研究员的指导和帮助, 在此深表谢意.

参 考 文 献

1 Cox I J, Kilian J, Leighton T, et al. Secure spread spectrum watermarking for multimedia. Technical Report 95-10, NEC Research Institute, 1995

2 Schyndel R G van, Tirkel A Z, Osborne C F. A digital watermark. In: Proc IEEE Int Conf on Image Processing (ICIP'94), 1994. II: 86~90

3 Petitcolas F A P, Anderson R J, Kuhn M G. Attacks on copyright marking systems. In: Proc Workshop Information Hiding, 1998. 15~17

4 Bas P, Chassery J M, Macq B. Geometrically invariant watermarking using feature points. IEEE Trans on Image Processing, 2002, 11(9): 1014~1028[DOI]

5 Cox I J, Kilian J, Leighton T, et al. Secure spread spectrum watermarking for multimedia. IEEE Trans on Image Processing, 1997, 6(12): 1673~1687[DOI]

6 Davoine F, Bas P, Hebert P A, et al. Watermarking et résistance aux déformations géométriques. In: Coresa99, 1999

7 Lin C Y, Chang S F. Distortion modeling and invariant extraction for digital image print-and-scan process. In: Proc Int Symp on Multimedia Information Processing (ISMIP 99), 1999

8 Lefebvre F, Gueluy A, Delannay D, et al. A print and scan optimized watermarking scheme. In: Proc IEEE Fourth Workshop on Multimedia Signal Processing, 2001, 511~516

9 Pereira S, Ruanaidh J, Deguillaume F, et al. Template based recovery of fourier-based watermarks using log-polar and log-log maps. In: Proc Int Conf on Multimedia Computing and Systems, 1999

10 Voloshynovskiy S, Herrigel A, Rytsar Y B. Watermark template attack. In: Proc SPIE, 2001, 22~25

11 Kutter M. Watermarking resisting to translation, rotation and scaling. In: Proc SPIE Int Symp on Voice, Video, and Data Communication, 1998

12 Oruanaidh J, Pun T. Rotation, scale and translation invariant spread spectrum digital image watermarking. Signal Processing, 1998, 66(3): 303~317[DOI]

13 Haitsma Jaap, Kalker Ton. A watermarking scheme for digital cinema. In: Proc Int Conf for Image Processing, 2001. 487~489

14 Zhao Y, Lagendijk R L. Video watermarking scheme resistant to geometric attacks. In: Proc Int Conf on Image Processing, 2002, 2: 145~148

15 Cornsweet T N. Visual Perception. New York: Acadmic Press, 1970

16 Depover G, Kalker T, Linnartz J P. Improved watermark detection reliability using filtering before correlation. In: Proc Int Conf for Image Processing, 1998, 430~434

17 Jayant N, Noll P. Digital Coding of Waveforms. Prentice Hall, 1984