一种新的适用于广播监视的安全视频水印算法

刘 丽[1),2)] 彭代渊[2)]

[1)](郑州航空工业管理学院计算机科学与应用系 郑州 450015)

[2)](西南交通大学信息科学与技术学院 成都 610031)

摘 要 在广播监视应用中,需要对视频片段进行认证.使用三维离散小波变换和中值量化方法,提出一种新的利用密钥生成鲁棒视频散列的算法.提出的散列算法对于视频编辑以及有损压缩都具有很好的鲁棒性.并在此基础上提出一种适用于广播监视的安全视频水印方案.该方案利用生成的散列值和版权标识形成待嵌入的水印信息,以实现对视频片段的认证.理论分析和实验结果表明,提出的算法具有较高的安全性和鲁棒性.

关键词 视频水印;视频散列;线性共谋;分集

中图法分类号 TP391 **DOI 号**: 10.3724/SP.J.1016.2009.02239

A Novel Secure Video Watermarking for Broadcast Monitoring

LIU Li[1),2)] PENG Dai-Yuan[2)]

[1)](*Computer Science Application, Zhengzhou Institute of Aeronautical Industry Management, Zhengzhou* 450015)

[2)](*School of Information Science & Technology, Southwest Jiaotong University, Chengdu* 610031)

Abstract Authentication of a video clip via its hash finds application in broadcast monitoring. For broadcast monitoring, a novel algorithm for computing a robust hash from video clips, being secret key based, is proposed based on the 3-D Discrete Wavelet Transform(3D-DWT) and median quantization. The proposed hash algorithm is shown to be remarkably robust against video modifications and lossy compression. On the basis of the video hashing, a secure video watermarking scheme for broadcast monitoring is put forward. In the proposed scheme, the short hash and copyright information are combined to create the embedding watermark. And they are used in the authentication of video clips. Some analyses and experimental results show that the proposed scheme has a good security and robustness.

Keywords video watermarking; video hashing; linear collusion; diversity

1 引 言

许多数字产品都要通过电视广播网进行广播,例如新闻、电影、广告等等.众所周知,广播时段是十分昂贵的.每一个广告客户都需要确认占有全部从广播公司购买的广告时间,作品版权所有者也要确保他们的所有物不会被侵权电台非法转播.对广播监视而言,数字水印显然是鉴别信息的可选方案.水印具有其本身存在于内容之中这一优点,优于广播信号中特定片段的使用,因此它与广播设备的安装基础(A-D、D-A 变换)完全协调一致.

利用数字水印的广播监视技术中,需要考虑 3 个实体:合法广告客户、攻击者(包括非法广告客户)、广播监视设备.合法广告客户在其广告被电视台播放之前,首先将自己的每个广告中都嵌入水印,

收稿日期:2007-10-28;最终修改稿收到日期:2009-06-01.本课题得到国家自然科学基金(60572142)、河南省科技攻关项目(0624220058)、河南省教育厅科技攻关项目(2007520045)、航空科学基金(20095155008)、河南省科技厅基础与前沿技术研究计划项目(092300410043)、河南高等学校青年骨干教师资助计划资助.**刘 丽**,女,1978 年生,博士研究生,讲师,主要研究方向为数字水印、多媒体信息安全等.E-mail: lliulli@163.com. **彭代渊**,男,1955 年生,教授,博士生导师,主要研究领域为密码学、网络信息安全、编码理论等.

然后用广播监视设备对他们已付费的电视台进行监视.而攻击者的目的是扰乱监视设备正常工作,使其鉴别出虚假信息.欧洲的 ESPRIT 项目 VIVA(Visual Identity Verification Auditor)已经证明了把数字水印用在专业的电视广播监视系统中的可行性.著名的 JAWS(Just Another Watermarking System)[1]算法就是成功应用于商业广播监视系统中[2-4]的一种视频水印算法.该算法虽然有鲁棒性好、复杂度低以及实时性高等优点,但是设计者在设计的过程中采用独立于宿主信号且服从正态分布的伪随机序列作为水印模板,仅考虑了水印的鲁棒性.在 2005 年,Su 等人针对 JAWS 算法的不足,提出了一种能够抵抗线性共谋攻击的鲁棒视频水印算法(称为 SLIDE 算法)[5].该算法虽然可以防止攻击者通过线性共谋攻击估计或恶意去除水印,但是设计者仍然采用独立于宿主信号的伪随机序列作为水印模板.JAWS 算法和 SLIDE 算法在设计过程中都采用伪随机序列作为水印,仅考虑了水印的鲁棒性.但如果要把这些算法应用在广播监视技术中还应当考虑算法的安全性.例如,在电视广告中,如果攻击者想办法得到合法广告中嵌入的水印,再将水印拷贝到另外一段非法广告中,即拷贝攻击.非法广告客户为了不向电视台支付广告费用而将自己的广告播出,就会采用这种攻击方法.因此,在设计鲁棒视频水印方案时,不仅要考虑鲁棒性,而且还要考虑具体应用中水印系统对安全性的要求,从而提高系统的安全性.

结合拷贝攻击,针对 JAWS 算法和 SLIDE 算法在广播监视应用中的不足,本文提出一种适用于广播监视的安全视频水印方案.首先,提出一种新颖的鲁棒视频散列算法,然后采用视频的散列值作为水印的一部分,以达到认证的目的,从而提高水印系统的安全性.水印的嵌入和提取则利用通信分集技术来提高水印的鲁棒性.

2 鲁棒视频散列算法

文献[6]中给出了一种基于三维离散余弦变换(3D-DCT)的视频散列算法,本文提出一种基于三维离散小波变换(3D-DWT)的视频散列算法.因为小波变换不仅具有时间-频率定位能力,具有局部时频特性的小波基更能捕捉视频图像的非平稳信息,可以获得更高的压缩比,而且它具有与人眼视觉特性相适应的特点,从而可在同样的平均码率下获得视觉质量更好的重建图像.也就是说,针对同一段视频,在要求得到的散列值位数相同的情况下,用小波变换计算的散列值比用余弦变换计算的散列值更能详细、准确地代表这一视频片段.提出的散列提取算法如下.

(1)视频预处理

在对视频序列进行散列计算之前,首先要把输入的视频序列预处理成标准的大小.预处理过程具体可分为两步:第 1 步,先对原始视频序列 $V_{\text{original}}(W,H,F)$ 在时间维上采用一维高斯低通滤波器进行滤波,然后对滤波后的一维信号进行下采样,使其变成 $V(W,H,f)$.也就是说不同的视频帧中相同位置的像素 $V(x,y,i)$,$i=1,2,\cdots,F$ 都可以看成是一个一维信号,然后对这些一维信号分别进行滤波和子采样,使其变成 $V(x,y,j)$,$j=1,2,\cdots,f$;第 2 步,对每个视频帧分别进行二维高斯低通滤波,然后对滤波后的每个视频帧进行下采样.这样,原始的视频序列 $V_{\text{original}}(W,H,F)$,就被预处理成标准的 $V_{\text{normal}}(w,h,f)$,其中 F 是原始视频序列帧数,f 是经预处理后标准的帧数.

(2)三维离散小波变换

三维离散小波变换是可分离的二叉树结构变换,即给定一个三维的视频序列 $V_{\text{normal}}(w,h,f)$,先对它的帧内行方向进行一维小波变换,然后对帧内列方向进行一维小波变换,最后对时间维进行一维小波变换.这样就可以完成该视频序列的一层三维离散小波变换,记为 $V^1_{\alpha,\beta,\gamma}(w,h,f)$,其中 $(\alpha,\beta,\gamma)\in\{L,H\}$,$\alpha$,$\beta$ 和 γ 分别为待处理信号的行、列和时间维.那么多层三维离散小波变换 $V^l_{\alpha,\beta,\gamma}(w,h,f)$,$l>1$ 可以通过对上一层低频子带 $V^{l-1}_{LLL}(w,h,f)$ 进行一层三维离散小波变换得到.

(3)散列计算

首先,对经过预处理后的信号 $V_{\text{normal}}(w,h,f)$ 进行 $n(n\geq 1)$ 层三维离散小波变换 $V^n_{\alpha,\beta,\gamma}(w,h,f)$(其中 n 的取值由散列值的位数决定).然后,选取低频子带 $V^n_{LLL}(w,h,f)$ 的变换系数进行散列值的计算.散列值的计算过程如下:

1.按照一定的扫描顺序将 $V^n_{LLL}(w,h,f)$ 扫描成一维序列 $A_{(i)}$,$i=1,2,\cdots,S$,S 为选取的低频子带的变换系数的个数,然后根据密钥 $key1$、$key2$、$key3$ 对 $A_{(i)}$ 进行混沌置乱[7]得 $AC_{(j)}$,$j=1,2,\cdots,S$,其中 $key1,key2\in(-1.5,1.5)$,$key3\in(0,1)$;

2.对一维序列 $AC_{(j)}$ 进行排序得序列 $C_{(k)}$,$k=1,2,\cdots,S$,并求 $C_{(k)}$ 的中值 m;

3. 计算视频片段 $V_{\text{original}}(W,H,F)$ 的散列值:

$$h_j=\begin{cases}1, & AC_{(j)}\geq m\\ 0, & AC_{(j)}<m\end{cases},\quad j=1,2,\cdots,S \tag{1}$$

以上操作使得散列算法对视频的一系列微小的变化都具有很好的鲁棒性. 而且,如果攻击者不知道 $key1$、$key2$、$key3$,他就不能准确地计算出视频片段的散列值,也就是说,提出的视频散列算法是安全的.

3　适用于广播监视的视频水印算法

在广播监视中应用水印技术,为了防止水印在经过各种处理后被去除,通常采用鲁棒水印技术. 然而,仅仅在设计水印算法的时候考虑鲁棒性是不够的,因为有攻击者也在试图扰乱广播监视设备的正常工作(如伪造攻击),使其鉴别出虚假结果,这必将引发广播电视台与合法广告客户之间的重大纠纷. 为了避免纠纷的发生,我们在设计适用于广播监视的视频水印算法的时候也要考虑到水印的安全性. 为了提高整个系统的安全性,本文的水印不是简单的利用图片或者伪随机序列,而是利用视频散列值和版权信息共同构成水印,以达到广播监视应用中对视频片段进行认证的目的.

3.1　广播监视应用中水印的生成

提出的算法将水印嵌入在视频片段的 Y 分量中,为了使视频散列序列的提取在水印嵌入前后保持同步,采用 YUV 格式的视频序列中的 U 分量来提取视频片段的散列序列. 原始视频片段的 U 分量为 $V(x,y,z)$,它的一层三维离散小波分解为 $V^1_{\alpha,\beta,\gamma}(x,y,z)$,并对其低频子带系数 $V^1_{LLL}(x,y,z)$ 求散列值. 例如:视频序列 foreman(176,144,20),即 20 帧的 qcif 格式的 foreman 序列,其采样格式为 4∶2∶0. 首先,对它的 U 分量进行一层小波分解得其低频子带 $V^1_{LLL}(44,36,10)$,然后用 $V^1_{LLL}(44,36,10)$ 作为鲁棒视频散列的输入. 在计算散列值之前,$V^1_{LLL}(44,36,10)$ 先经过预处理,使其变成标准大小 $V^1_{LLL}(16,16,32)$. 然后再对 $V^1_{LLL}(16,16,32)$ 进行两层三维离散小波变换,最后对变换后的低频系数进行散列值计算. 这样 foreman(176,144,20)序列经过散列以后,得出的是 128 比特的信息,而且这 128 比特的信息中 0 和 1 的个数是相等的.

然后,将计算出的散列序列和版权保护信息连接在一起,即散列序列作为前 128 位,版权保护信息作为后 128 位. 其中版权保护信息只有合法广告客户独自拥有,如 128 位的伪随机序列. 为了避免攻击者能够在提出水印后分离出视频散列值,在水印被嵌入之前,要对这 256 比特的信息进行置乱[7]. 最后对置乱后的 256 比特信息进行升维,使其变为 16×16 的待嵌入的水印信息.

合法广告客户如果将前面已经生成的水印嵌入到自己的广告片段中,再将含水印的广告在他已付费的电视台播放,这样他就可以相信广播监视设备报告的结果了. 然后选用现有鲁棒视频水印的嵌入和提取技术就可以完成在视频中加水印. 但要遵循的一个原则是:利用视频片段的一部分提取散列值,而嵌入过程并不改变这一部分,只将水印嵌入到剩余的部分,这样就可以在水印嵌入前后保持散列值提取的同步. 为了提高水印系统的鲁棒性和水印提取的实时性,本文利用通信分集的思想,采用重复嵌入的水印技术.

3.2　嵌入区域的自适应选择

有关心理视觉的研究表明,人眼对各种环境有不同的敏感度. 例如,人眼对于纹理复杂区域(如边缘)所产生的失真并不敏感,但是在边缘区域嵌入水印鲁棒性会降低;另一方面,视频序列与静止图像的不同在于它包含运动部分,具有变化的特性,而人眼对于高速运动的物体敏感度会有所下降,因此可以在高运动区域嵌入水印. 但是水印嵌入在高速运动物体的一些细节区域(如边缘)时,水印的鲁棒性就会降低. 因此本文选择高运动区域中梯度变化较小的区域嵌入水印.

高运动区域的选取是在相邻帧间利用运动检测器[8],将图像块划分成慢速运动区域和快速运动区域两类,然后在快速运动区域中利用块复杂度选取梯度变化相对较小的一部分区域嵌入水印,即当块复杂度小于 T_g 时,则该块被用来嵌入水印. 块复杂度定义如下:

$$C_{\text{block}}=\sum_{\text{block}}\frac{1}{4}(|d_x|+|d_{-x}|+|d_y|+|d_{-y}|) \tag{2}$$

其中 C_{block} 表示块复杂度,d_x、d_{-x} 分别表示块中当前像素与其在 x 方向和 $-x$ 方向相邻像素的灰度值之差.

3.3　水印的嵌入

整个嵌入过程在空间域进行,并且只将水印嵌入在亮度分量上,嵌入方法采用位平面替换. 为了在鲁棒性和不可见性之间取得很好的折中,所替换的位平面的位置 k 由下式决定:

$$k=int(var(U_j)) \bmod 3+2 \tag{3}$$

其中，$int(\cdot)$表示取整，$var(\cdot)$表示方差，U_j表示原始子帧.

3.4 水印的提取

水印的检测和提取不需要原始视频的参与.具体的提取步骤如下：

1. 每个已嵌入水印的视频帧被分成互不重叠的16×16的块(子帧)，并根据式(2)计算每个块的复杂度.如果计算出的块复杂度小于一给定阈值 $T'_g(T'_g>T_g)$，则将该块归入集合 $S_1:\{U'_1,U'_2,\cdots,U'_{e_n}\}$；

2. 集合 S_1 中的每一个元素 $U'_j,j\in\{1,2,\cdots,e_n\}$ 分别被分解成8个位平面：

$$U'_j=\sum_{l=0}^{7}U'_j(l) \tag{4}$$

由于根据式(3)计算出的 $k\in\{2,3,4\}$，所以分别计算水印信息与第2、3、4个位平面的相关值：

$$r_l=U'_j(l)\otimes w,\quad l\in\{2,3,4\} \tag{5}$$

再将 r_l 与阈值 T_c 进行比较：

$$\begin{cases} r_l\geq T_c, & \text{检测到水印} \\ r_l<T_c, & \text{没有检测到水印} \end{cases}.$$

如果 r_l 大于等于 T_c，则说明检测到水印，并将相应的位平面 $U'_j(l)$ 放入集合 $S_2:\{U'_{1l},U'_{2l},\cdots,U'_{e_m l}\}$；

3. 在集合 S_2 中可以得到 e_m 个16×16的块.那么提取的水印 $\hat{w}$ 可以通过计算 $U'_{1l},U'_{2l},\cdots,U'_{e_m l}$ 的加权和求得：

$$\hat{w}=round\Big(\sum_{k=1}^{e_m}\alpha_k U'_{kl}\Big),\quad \sum_{k=1}^{e_m}\alpha_k=1 \tag{6}$$

其中，

$$\alpha_k=\frac{D_{E_k}}{\sum_{j=1}^{e_m}D_{E_k}},\quad k=1,2,\cdots,e_m \tag{7}$$

$$D_{E_k}=\frac{\langle U'_{kl},w\rangle}{\langle w,w\rangle} \tag{8}$$

将最后得到的加权和转化为二值信息即得最后提取的水印.

4 安全分析

4.1 线性共谋攻击

视频水印不同于图像水印的一个特点是攻击者可利用更多的数据，这些数据具有高度的相关性，即使在每个图像帧内做空间不相关样本的假设，典型的视频序列在时间轴上依然具有很强的相关性.攻击者可以利用该相关性对含水印视频进行恶意攻击，这种类型的攻击被称为线性共谋攻击[5].

线性共谋攻击是当前视频水印研究中的一个重要问题.线性共谋攻击分为两类[5]：如果水印嵌入者在大量的视觉上相异的视频帧中通过线性组合嵌入相同的水印，那么攻击者就可以估计出水印信息，这种攻击就是第1类线性共谋攻击，该类型的攻击可以看作是未经授权的检测；如果水印嵌入者在大量的视觉上相同的视频帧中通过线性组合嵌入不同的水印，那么攻击者就可以估计出原始视频信息，这种攻击就是第2类线性共谋攻击，该类型的攻击可以看作是未经授权地去除.Furon等人在文献[9]中明确指出：水印安全的范围很广，它不仅包括水印的去除，而且还包括未经授权的嵌入和检测.由此看来线性共谋攻击应该用来衡量水印的安全性.

上述的线性共谋攻击可由如下数学模型来描述：给定一个嵌入水印的视频序列

$$Y_k=X_k+\alpha_k W_k,\quad k=1,2,\cdots,n,$$

其中，X_k 是原始视频帧，Y_k 是嵌入水印后的视频帧，α_k 是嵌入强度，W_k 是水印信息.线性共谋是从嵌入水印后的视频序列中选取 $m(m\leq n)$ 帧(不一定是连续的)，并对这 m 帧形成一个线性组合的过程：

$$\overline{Y}=\sum_{i=1}^{m}\beta_i Y_i=\sum_{i=1}^{m}\beta_i X_i+\sum_{i=1}^{m}\beta_i\alpha_i W_i \tag{9}$$

其中 $\overline{Y}$ 表示水印或宿主视频信号的最佳均方误差估计.如果 $\overline{Y}$ 是水印的最佳均方误差估计，则表示遭受了第1类线性共谋攻击；如果 $\overline{Y}$ 是宿主信号的最佳均方误差估计，则表示遭受了第2类线性共谋攻击.令 $\beta_i=1/m$，那么就得到视频水印中的帧平均.

视频帧 X_i 和 X_j 在视觉上相同是指它们在均方意义上相似，即

$$E[(X_i-X_j)^2]\approx 0 \tag{10}$$

或 X_i 和 X_j 的相关系数

$$\rho(X_i,X_j)\approx 1 \tag{11}$$

如果

$$\rho(X_i,X_j)=1 \tag{12}$$

则 X_i 是 X_j 的最佳均方误差估计.

如果含水印的视频遭受到第1类线性共谋攻击，即式(9)中 $\overline{Y}$ 是水印的最佳均方误差估计，则有

$$\rho(\overline{Y},\overline{W})=1 \tag{13}$$

其中 $\overline{W}=\sum_{i=1}^{m}\beta_i\alpha_i W_i$.令 $\overline{X}=\sum_{i=1}^{m}\beta_i X_i$，则有 $\overline{Y}=\overline{X}+\overline{W}$，

$$\rho^2(\overline{Y},\overline{Y})=1=\rho^2(\overline{Y},\overline{X})+\rho^2(\overline{Y},\overline{W}) \tag{14}$$

由式(13)和式(14)可得

$$\rho(\overline{Y},\overline{X})=0 \tag{15}$$

如果含水印的视频遭受到第2类线性共谋攻击，即式(9)中 $\overline{Y}$ 是原始视频信号的最佳均方误差估计，则有

$$\rho(\overline{Y},\overline{X})=1 \tag{16}$$

那么,根据式(15)和式(16),如果

$$\rho(\overline{Y},\overline{X})\neq 0 \text{ 且 } \rho(\overline{Y},\overline{X})\neq 1 \tag{17}$$

成立,则两种线性共谋都不可能发生.

如果令嵌入水印的方差大于 0,则有

$$0<\rho(Y_i,X_i)<1,\ \forall i\in\{1,2,\cdots,m\} \tag{18}$$

那么,如果

$$\rho(\overline{Y},\overline{X})=\rho(Y_i,X_i),\ \forall i\in\{1,2,\cdots,m\} \tag{19}$$

成立,则式(17)满足,即线性共谋不可能发生. 由式(19)可知

$$\rho(Y_i,X_i)=\rho(Y_j,X_j),\ \forall i,j\in\{1,2,\cdots,m\} \tag{20}$$

成立.

如果把同一个水印模式嵌入到各视频帧中,即

$$W_i=W_j,\ \forall i,j\in\{1,2,\cdots,m\} \tag{21}$$

令水印的均值为 0,且水印信息独立于尺度因子和视频帧,则

$$\rho(Y_i,X_i)=\rho(Y_j,X_j) \tag{22}$$

式(22)成立的充分必要条件是

$$\frac{E\alpha_i^2}{E\alpha_j^2}=\frac{var(X_i)}{var(X_j)} \tag{23}$$

由式(21)和式(23)可以看出,在设计视频水印方案的时候,如果采用同一水印模式,且水印信息均值为 0,方差大于 0,使嵌入强度自适应于相应的原始视频帧的方差,那么攻击者就很难利用视频序列在时间轴上的强相关性对含水印视频进行恶意攻击. 提出的水印方案正好符合这一设计要求,因此攻击者很难利用线性共谋攻击对水印进行恶意去除或未经授权地提取,大大提高了算法的安全性.

4.2　拷贝攻击

在广播监视应用中,假设攻击者知道算法,那么他可以提取广告客户的水印,并且把提取的水印嵌入到他的广告中,然后代替合法广告客户的广告播出,即拷贝攻击. 但是利用提出的视频水印算法,攻击者很难达到他拷贝攻击的目的. 因为合法的广告客户嵌入的水印是具有认证能力的水印,即在水印中加入了广告片段的视频散列值. 广播监视设备只需根据密钥 $key1$、$key2$ 和 $key3$ 解码提取的水印信息,以得到水印信息中的视频散列序列,然后把提取的散列序列和嵌入水印的广告片段产生的散列序列进行比较,如果比特错误率小于某一给定的阈值,那么广播监视设备就可以断定合法广告客户的广告已经在其购买的广告时段被播出了.

如果攻击者想解码嵌入的水印信息,从而用他的广告片段的散列序列代替合法客户水印中的散列序列,那么他们就必须能够估计出 $key1$、$key2$ 和 $key3$. 但是想通过蛮力攻击来估计出 $key1$、$key2$ 和 $key3$,几乎是不可能的. 因为 $key1$、$key2$ 和 $key3$ 的密钥空间分别大于 10^{12},10^{15} 和 10^{16},而整个混沌置乱算法的密钥空间大于 10^{43}[7],这大大降低了攻击者利用蛮力攻击来解码水印信息的可能性,从而有效提高了算法的安全性. 表 1 显示了提出的算法、JAWS 算法、SLIDE 算法分别应用在广播监视中的安全性.

表 1　3 种算法安全性比较

算法	安全性	
	拷贝攻击	线性共谋攻击
JAWS	差	差
SLIDE	差	高
提出算法	高	较高

5　实验结果

实验采用 qcif 格式的视频序列“foreman.yuv”,帧数为 20 帧,采样格式为 4∶2∶0.

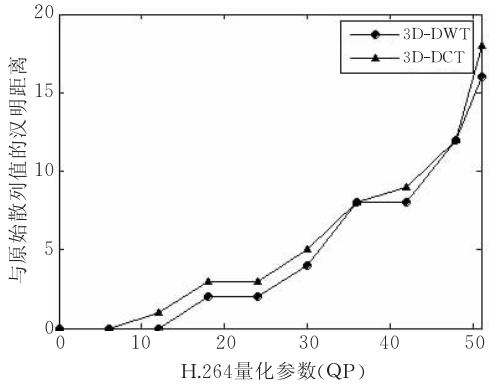
5.1　提出的散列算法的鲁棒性测试

图 1 分别显示了文献[6]和本文提出的视频散列算法的鲁棒性. 空间帧旋转是指视频的每一帧被分别旋转 1°,3°,5°和 7°;帧内像素循环移动是指视频帧内像素纵向循环移动,例如第 1 列的像素移动到最后 1 列,行位置不变,原来第 2 列的像素变为第 1 列,依次类推,参数设置分别为移动行像素点的 1%,3%,5%和 7%;随机帧抖动:在有损信道中,为了使被损坏的视频序列帧数始终与原始文件中帧数保持一致,随机选择掉帧的位置,并用该位置周围现存的帧的线性内插来代替已丢失的帧,抖动率分别取 20%,40%,60%和 80%. 由此可以看出,针对同一段视频,在取得相同长度的散列序列的情况下,提出的视频散列算法比文献[6]中的算法鲁棒性更高.

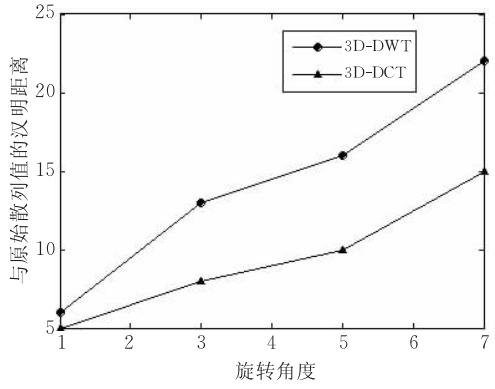
5.2　提出的水印算法的性能测试

图 2 显示了 foreman 序列的连续 3 帧,其中(a)为原始视频帧,(b)为嵌入水印后相应的视频帧. 图 3 显示了 foreman 序列嵌入水印后的 $PSNR$ 值(由于视频序列的第一帧没有嵌入水印,所以其 $PSNR$ 值为 0). 由此可以看出嵌入的水印具有很好的不可见性.

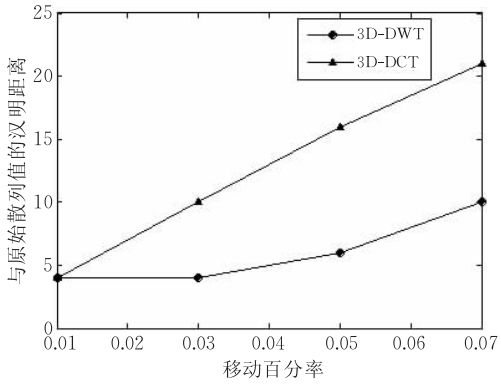
表 2 显示了提出的水印算法经过不同的鲁棒性攻击后提取水印的正确率.



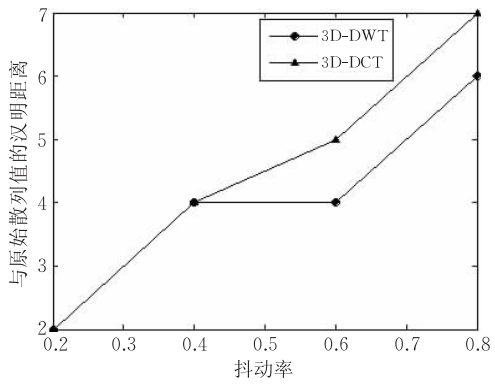
(a) 不同比特率下H.264压缩的影响



(b) 空间帧旋转的影响



(c) 帧内像素循环移动的影响



(d) 随机帧抖动的影响

图 1 不同攻击下的汉明距离

(a) 原始视频

(b) 含水印视频

图 2 “foreman.yuv”视频序列中的连续三帧

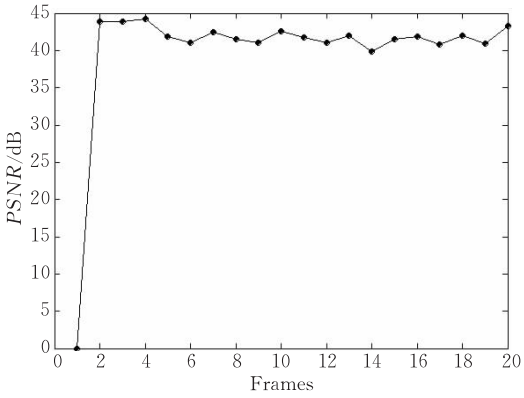


图 3 嵌入水印后“foreman.yuv”序列的 *PSNR* 值

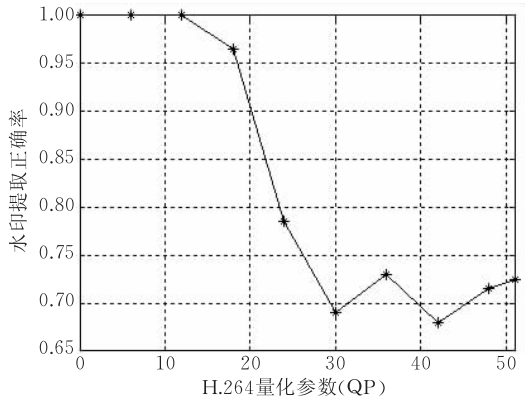


图 4 不同比特率下 H.264 压缩后提取水印的正确率

表 2 不同鲁棒性攻击后的测试结果

鲁棒性攻击	水印提取的正确率/%	鲁棒性攻击	水印提取的正确率/%	鲁棒性攻击	水印提取的正确率/%
中值滤波	94.92	帧去除	100	随机帧抖动(0.4)	100
剪切	100	帧插入	100	帧内像素循环移动(0.03)	99.22
加性噪声	74.22	帧重组	100	空间帧旋转(3°)	74.22

由于视频通常是以压缩格式存储的,因此有必要测试一下算法针对有损压缩的鲁棒性.本文利用 H.264/AVC JM-12[①] 实现视频的编解码过程.实验对连续的 20 帧视频序列进行压缩,帧率为 25 帧/s.图 4 显示了经不同比特率下 H.264/AVC 压缩后提取水印的正确率,其中 $0 \leq QP \leq 51$,由实验结果可以看出提出的算法针对 H.264/AVC 压缩攻击有较好的鲁棒性.

在 matlab7.0 环境下分别对 JAWS 算法和本文算法进行仿真,在提取水印的同时,记录了水印提取的时间.商业中常用的 JAWS 算法从连续的 20 帧中提取出水印的时间为 3.115s;本文提出的算法从连续的 20 帧中提取出水印的时间为 3.357s,从含水印视频序列中提取散列值再与提取的水印中的散列值进行匹配测试的时间为 2.721s,合起来共花费 6.078s.

理论分析和实验结果表明针对广播监视应用,提出的方案不仅具有很好的不可见性和鲁棒性,而且还有较高的安全性和实时性.

6　结　论

在广播监视应用中,仅对水印提取的实时性要求较高,而提出的算法是在空域利用通信分集技术进行水印的提取,这大大提高了水印提取的实时性和正确性.

文章基于三维离散小波变换和中值量化提出一种新颖的用于认证的鲁棒视频散列算法.提出的视频散列算法不仅针对一般的视频编辑和有损压缩具有很好的鲁棒性,而且在广播监视应用中可以用来对广告片段进行认证.并在此基础上给出了设计适用于广播监视的安全视频水印算法所要遵循的一个原则,根据此原则提出一种安全视频水印算法.理论分析和实验结果表明,提出的算法针对广播监视应用具有很好的安全性和鲁棒性.

参　考　文　献

[1] Kalker Ton, Depovere Geert, Haitsma Jaap, Maes Maurice. A video watermarking system for broadcast monitoring//Proceedings of the SPIE, San Jose, CA, USA, 1999: 103-112

[2] Depovere Geert, Kalker Ton, Haitsma Jaap, Maes Maurice, De Strycker Lieven, Termont Pascale, Vandewege Jan, Langell Andreas, Alm Claes, Norman Per, O'Reilly Gerry, Howes Bob, Vaanholt Henk, Hintzen Rein, Donnelly Pat, Hudson Andy. VIVA project: Digital watermarking for broadcast monitoring//Proceedings of the 1999 International Conference on Image Processing (ICIP' 99). Kobe, Japan, 1999: 202-205

[3] Termont Pascale, De Strycker Lieven, Vandewege Jan, Op de Beeck M, Haitsma Jaap, Kalker Ton, Maes Maurice, Depovere Geert. How to achieve robustness against scaling in a real-time digital watermarking system for broadcast monitoring//Proceedings of the 2000 International Conference on Image Processing (ICIP 2000). Vancouver, BC, Canada, 2000: 407-410

[4] Termont Pascale, De Strycker Lieven, Vandewege Jan, Haitsma Jaap, Kalker Ton, Maes Maurice, Depovere Geert, Langell Andreas, Alm Claes, Norman Per. Performance measurements of a real-time digital watermarking system for broadcast monitoring//Proceedings of the 1999 6th International Conference on Multimedia Computing and Systems—IEEE ICMCS'99. Florence, Italy, 1999: 220-224

[5] Su K, Kundur D, Hatzinakos D. Spatially localized image-dependent watermarking for statistical invisibility and collusion resistance. IEEE Transactions on Multimedia, 2005, 7(1): 52-66

[6] Coskun B, Sankur B. Robust video hash extraction//Proceedings of the IEEE 12th Signal Processing and Communications Applications Conference, SIU 2004. Kusadasi, Turkey, 2004: 292-295

[7] Xie Ling, Zhang Jiashu, He Hongjie. A novel robust audio watermarking scheme based on nonuniform discrete Fourier transform. Chinese Journal of Computers, 2006, 29(9): 1711-1721(in Chinese)
(谢玲,张家树,和红杰.一种基于非均匀离散傅立叶变换的鲁棒音频水印算法.计算机学报,2006,29(9):1711-1721)

[8] Lu Zheming, Ge Qingming, Niu Xiamu. Robust adaptive video watermarking in the spatial domain//Proceedings of the 5th International Symposium on Test and Measurement (ISTM'2003). Shenzhen, China, 2003: 1875-1880

[9] Furon T et al. Security analysis. European Project IST-1999-10987 CERTIMARK, Deliverable D.5.5, 2002

[10] Darmstaedter V, Delaigle J-F, Nicholson D, Macq B. A block based watermarking technique for MPEG2 signals: Optimization and validation on real digital TV distribution links//Proceedings of the European Conference on Multimedia Applications, Services and Techniques. Berlin, Germany, 1998: 190-206

① H.264/AVC Joint Model 12 (JM-12) Reference Software. Available: http://iphome.hhi.de/suehring/tml/, 2007

LIU Li, born in 1978, Ph. D., lecturer. Her research interests include digital watermarking, multimedia information security etc.

PENG Dai-Yuan, born in 1955, professor, Ph. D. supervisor. His research interests include cryptography, network information security and coding theory.

Background

This work is supported by the National Natural Science Foundation of China (No. 60572142), the Science & Technology of Henan province (No. 0624220058) and the Science & Technology of the education department of Henan province of China (No. 2007520045), etc.

In recent years, watermarking security has emerged as a new subject in the watermarking area. And it brings new challenges to the design of watermarking systems. This work describes one of the major problems for robust video watermarking in the application of broadcast monitoring, which is security. For broadcast monitoring, authentication of a video clip via its hash find application can solve the problem. At the same time, linear collusion is a critical issue in the current study of video watermarking, and the attack is traditionally in the watermarking literature concerned with robustness assessment. However, according to what Furon et al. said, linear collusion attack should be used to assess security.