一种有效识别正版视频的 TDIA 算法

周国瑞[1)] 王文江[2)] 孙世新[1)]

[1)](电子科技大学计算机科学与工程学院 成都 610054)

[2)](龙旗科技(上海)有限公司工程部 上海 200233)

摘 要 结合视频压缩标准、脆弱数字水印及视频通信技术,文中提出一种有效识别正版视频的 TDIA 算法.它包括嵌入算法和识别算法两部分.为消除通信干扰对水印的影响,将迭代方法引入识别算法.基于盗版操作与通信干扰的本质不同,研究讨论了迭代方法的性能.最后,基于迭代结果,借助 Chernoff Bound 理论,分析了 TDIA 算法的识别误差.对于码流 *BER*(Bit Error Rate)$\leq 10^{-3}$、视频 I 帧总数 $n \geq 360$ 的 Mpeg2 编码视频,该算法识别误差小于 10^{-18}.

关键词 脆弱数字水印;正版视频;盗版视频;录制盗版;Mpeg2 编解码器

中图法分类号 TP391 **DOI 号**: 10.3724/SP.J.1016.2010.00175

An Efficient Genuine-Video Identification Algorithm: TDIA

ZHOU Guo-Rui[1)] WANG Wen-Jiang[2)] SUN Shi-Xin[1)]

[1)](*School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu* 610054)

[2)](*Engineering Department, Longcheer Co. Ltd, Shanghai* 200233)

Abstract An efficient genuine-video identification algorithm named as TDIA is proposed, which based on integration of video compression standards, fragile watermarking and video communication technology. It includes two parts: embedding algorithm and identification algorithm. Iterative method is introduced on the identification algorithms to eliminate the communications interference for the impact of watermarking. The performance of the iterative method is investigated according to the difference of nature between piracy operation and communications interference. Finally, the identification errors of TDIA algorithm are analyzed based on the results of iteration and by dint of the theory of Chernoff Bound. The total identification error of the algorithm is less than 10^{-18} when *BER*(Bit Error Rate) of encoded video stream is not more than 10^{-3} and the total number of I-frames of Mpeg2 encoding video is more than 360.

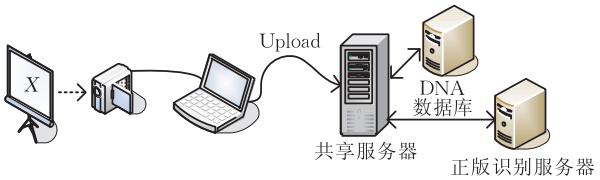
Keywords fragile watermarking; genuine-video; pirated-video; camcorder piracy; Mpeg2 codec

1 引 言

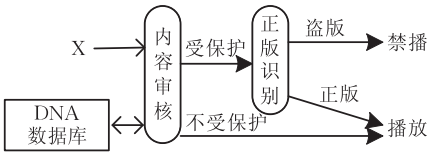
保护正版视频版权关键要做好传输及终端消费两个环节的安全[1].传输安全包括链路安全及接入安全,目前技术较为成熟,主要由网络协议(如 SSL、RTP、ATM 等)加上应用层的 CA(Conditional Access)[2] 技术来实现.理论上,传输安全保证了授权用户才能消费正版视频,未授权用户由于无法获得或解密正版视频,不可能进行消费.终端消费安全就是规范终端授权用户的行为,阻止其非法拷贝及对非法拷贝的散播,目前,主要采取主动禁止及被动防

收稿日期:2008-07-14;最终修改稿收到日期:2009-07-19.**周国瑞**,女,1974 年生,博士研究生,主要从事数据压缩、小波理论、数字水印与版权保护等技术的研究.E-mail: mimi5988@126.com. **王文江**,男,1974 年生,高级工程师,主要从事图形图像、3G 移动通信等技术研究. **孙世新**,男,1940 年生,教授,博士生导师,主要从事信息压缩、网络计算、并行/分布式计算、数值计算与组合算法等领域的研究.

御两种措施.主动禁止是用技术手段主动阻止非法copy,比如,在消费电子装置中配置copy保护,根据CCI(Copy Control Information)进行copy控制[3-4],主动禁止可以阻止点到点copy[5],但无法阻止用户用录像机等外设对着正在播放的视频屏幕进行视频录制盗版(camcorder piracy),见图1(a),这种威胁源于analog hole[5].被动防御旨在禁止对非法拷贝的使用和散播,它是在盗版发生之后,对盗版视频版本的禁播、追踪或进一步对肇事者进行的追踪,从而威慑授权用户不要进行散播侵权.被动防御的主流技术有视频指纹(video fingerprinting[6-7]或VideoDNA①)及抗共谋数字指纹技术(anti-collusion fingerprinting)[8-10];两者都要求鲁棒性,即只要视频的视觉内容没有被改变,前者认为其中的VideoDNA没有被改变,后者认为嵌入其内的代表授权用户信息的数字水印(数字指纹)依然存在;因此,利用前者可以进行视频内容检索,利用后者可以进行肇事者追踪.而两者都不区分视频是正版还是盗版,但这种区分是必要的;鉴于此,本文提出了正版视频识别算法,它与这两种技术的有效结合,能推动被动防御的进展.



(a) 外挂攻击及视频过滤过程



(b) 对受保护视频的盗版禁播示意图

图1 正版视频识别技术应用模型示意图

在本文,版权所有者持有的视频版本为正版视频,不妨记为A;由A仅遭受正常通信信道干扰后形成的视频版本也是正版视频.盗版视频指通过基于analog hole[5],用录屏方式获得的视频,但盗版者为规避检测,可能对其进行修改加工.在主动禁止实现后,录屏是唯一的盗版方式,目前,也很流行[11].

本文所提TDIA(Disturbance-tolerant Identification Algorithm)算法旨在判定视觉内容一致的视频[12]集中,哪些是正版哪些是盗版.应用模型见图1,图1给出了所提算法与VideoDNA技术结合实现盗版过滤及禁播功能的示意.首先通过VideoDNA技术提取待审核视频的DNA,并到DNA database库中查询,若找到与之相匹配的,则说明待审核视频含受版权保护的内容,因此,需要启动正版视别程序进行正版识别并根据识别结果做出相应处理.图1(a)为视频共享网站(如YouTube[13]、优酷、土豆网等)对Upload视频审查过滤示意图.图1(b)为网络终端对受保护视频的盗版禁播示意图.

另外,由于当前在IPTV、3G视频通信中常使用RTP/UDP/IP传输协议[14],而UDP并不保证可靠性和顺序性,所以前端数据并不能保证无误差地传送到终端,终端播放器常利用差错探测、差错控制及差错复原机制来屏蔽所接收视频流中的误码及丢包,尽量给人以流畅的视频感受.在这种环境中,终端播放的视频与前端下发的视频常存在一定的数据差异,并且该差异由通信时信道状况决定.有线信道的通信干扰远小于无线信道,采用足够FEC(Forward Error Correction)[5]及interleaving技术的无线信道通信干扰相当于*BER*(Bit Error Rate)在$10^{-4}\sim10^{-3}$范围的BSC(Binary Symmetric Channel)信道[15].TDIA算法在设计时考虑了对正常通信信道干扰的容忍.

本文第2节介绍录屏盗版的特点、数字水印及盗版视频识别算法现状;第3节给出基于脆弱数字水印技术,能容忍正常通信信道干扰的TDIA算法;第4节对TDIA算法性能进行整体测试;第5节全文小结.

2 相关技术分析

录屏盗版分为外置和内置两种方式.外置指用摄像机、照相机、手机等外设对着正在播放视频的屏幕进行的录制.由于录制时所采用的坐标系[16]、颜色空间、空间和时间采样率都难以保证与播放视频相同,因此同原视频相比,录制的视频存在如下变化:(1)由仿射变化及投影变换[16-17]导致的几何型变,(2)帧率变化,(3)像素值变化.内置指在播放视频的设备上安装录屏软件,使用录屏软件录屏.像Camtasia Recorder、Screensnap等计算机录屏软件可以实现录制时的坐标系、空间及时间采样率与所播放的视频相同,仅存在由D-A和A-D转换带来的像素值损失.因此,外置比内置录制效果差,但是

① Vobile announces landmark deployment of VideoDNA?content indentification and management system. http://www.vobile.cn/files/mediacoverage/2008.09.22-CNBC.pdf

目前外置录屏效果已经具备一定的观赏价值[11].

当正版视频与这些录制的盗版视频混在一起的情况下，如何识别出正版和盗版视频呢？借助文献[4]的思想，可以用不可见鲁棒水印“illegal cogy”标识盗版.正版视频在嵌入该标记后播放，这样，如果录屏盗版，则该标记一并被录制到盗版视频中.通过识别“illegal cogy”标识，来识别盗版.该思想存在如下不足：

(1)播放的视频是叠加了鲁棒水印的视频.同脆弱数字水印相比，鲁棒水印对视频质量影响较大.

(2)在 camcorder piracy 等录屏盗版下，鲁棒水印的存活和检测是个难题；

(3)不同的视频，叠加了相同的鲁棒水印(“illegal copy”)，难以抵制移去攻击.

TDIA 算法，基于脆弱数字水印[18]标识正版，弥补了这些不足.

3　TDIA 算法

TDIA 算法分为水印嵌入及水印提取正版识别两部分.结合视频编码标准、对盗版操作脆弱、视频相依、密钥级安全以及保证一定的水印嵌入量，设计了 3.1 节嵌入算法.3.2 节分析了信道干扰对水印的影响，3.3 节给了排除影响的迭代算法，3.4 节给出了盲识别算法.

3.1　嵌入算法

在 Mpeg2、H.264 视频编解码标准中，DCT 变换以像素块(Block)[19-20]为单位进行，I 帧亮度分量的 MB(Maroblock)[19]中每 4 个这样的 Block 组成 1bit 水印承载单位 WB(Watermark Block).以编码时 WB 中 4 个 Block 的量化后 DCT 系数[19-20]为基础，嵌入水印，并压缩编码成正版视频.水印嵌入算法基本步骤如下：

1.寻找各个 WB 的水印嵌入点.

判定在 WB 最后编码的 Block 中，按照 zigzag 扫描顺序第 T_{embed}(阈值)个扫描系数之后的系数中是否存在非零值 AC 系数；如果有，则选择该扫描顺序最后的非零值 AC 系数(Ac_{last})作为水印嵌入点，转步 2；否则在这个 WB 不进行水印嵌入；

2.计算水印.

记 WB 的 4 个 DC 系数值分别为 $Dc_0,\cdots,Dc_3$，令

$$a=(|Dc_0|+|Dc_1|+|Dc_2|+|Dc_3|)/4;$$

$$b=\max\{|Dc_0|,|Dc_1|,|Dc_2|,|Dc_3|\};$$

$$x_0=\begin{cases}(a/b+k_1)/2, & b\neq 0\\ k_1/2, & b=0\end{cases} \tag{1}$$

其中 $k_1\in(0,1)$为水印密钥，显然 $x_0\in(0,1)$.

将 x_0 及 $\lambda=4$ 作为初值和参数，代入 logistic[21]映射迭代式(2)；并根据密钥 k_2，按式(3)计算水印 w：

$$x_{n+1}=\lambda x_n(1-x_n) \tag{2}$$

$$w=floor(x_{k_2}+0.499999\cdots) \tag{3}$$

其中，$floor(\cdot)$为向下取整函数.

3.嵌入水印.

当 $w=0$ 时，Ac_{last} 需为偶数，不为偶数时按下式进行更改：

$$Ac_{\text{last}}=\begin{cases}Ac_{\text{last}}+\text{sign}(Ac_{\text{last}}), & |Ac_{\text{last}}|=1\\ Ac_{\text{last}}-\text{sign}(Ac_{\text{last}}), & |Ac_{\text{last}}|\neq 1\end{cases} \tag{4}$$

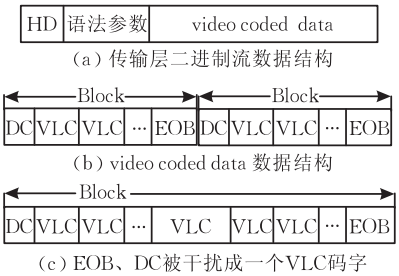
当 $w=1$，Ac_{last}需为奇数，不为奇数时按式(4)进行更改.

水印嵌入时机之所以选择量化后 DCT 系数(亦是解码时反量化前 DCT 系数)，是为了减少量化操作对水印的改变以及避免量化步长的错误对水印检测的影响.考虑到 VLC 编码规则，式(4)在设计上尽量使$|Ac_{\text{last}}|$变小，以便水印的嵌入不增加视频码长.

由 $\lambda=4$ 的 logistic 混沌序列性质[21]，式(3)中 w 等于 0 或 1 的概率各为 50%，对整个视频来说嵌入 0 或 1 的总量基本相等.使用 k_1、k_2两个水印产生密钥，由混沌映射对初值具有敏感性，导致水印难以被统计估计，即使在嵌入算法公开的情况下，安全系数也比较高.

3.2　信道误码对水印的影响分析

传输层二进制视频流的数据结构见图 2(a)，HD(头信息)及语法参数数据量相对较少，常采用 Reed-Solomon code 等容错编码技术进行保护.Video coded data 占视频比特流的 98%左右[22]，由于数据量大，难以采用保护措施，因此，是信道误码的多发区域.Video coded data 是用 VLC 编码对视频的 DC 值、AC 值、游程长度以及宏块地址增量、宏块类型、块编码模式等进行的二进制编码[19]，图 2(b)给出了其数据结构，为便于说明信道误码的影响，将 VLC 编码的 DC 数据表示为 DC，Block 的结



(a)传输层二进制流数据结构

(b) video coded data 数据结构

(c) EOB、DC被干扰成一个VLC码字

图 2　传输二进制流结构及误码引起的块合并示意图

束表示为 EOB(End of Block). 图 2(c)是图 2(b)中的 EOB 及 DC 被信道误码干扰成另一个 VLC 码字后,引起的块合并示意图.

Video coded data 对信道误码非常敏感,当含有信道误码时,视频解码器在解码时就会遇到以下情况:

(1)无效 VLC 码字. 通信干扰导致 VLC 码字无效.

(2)越界. 通信干扰虽未导致 VLC 码字无效,但导致 VLC 码字分解或合并,从而出现:

DC、AC、量化因子、运动矢量、宏块地址增量等值越界;块解码的 DCT 系数总个数超过允许的最大值;Slice[19] 解码 Block 总数不等于应解码总数,特别非 EOB 被干扰成 EOB 时,块被分割,EOB 被干扰成非 EOB,块被合并(图 2(c)所示).

以上错误统称为语法错误(syntax error)[23],这些错误中,只有当 DC、AC 值越界后,解码器将其修改为默认值,对其它语法错误,标准解码器不对其进行更改,而是直接跳到下一个同步标记处(Slice 头)重新开始解码[19].

另外,在标准解码器正常解码的 slice 中,仍可能存在由信道干扰所致的隐藏错误[24],例如:

(1)某个块或某些块的 AC 系数错误;

(2)DC 系数错误,由于 DC 系数是预测差分值(DPCM)编码,一个块的 DC 系数错误,可以导致基于其进行 DPCM 解码的后继块 DC 系数错,直到同步标志处为止.

因此,信道误码 bit 位发生位置的不确定性,导致了 DC、AC 系数错误率的不确定性. 故在没有原始 video coded data 的情况下,无法找到信道误码率与水印错误率之间的精确关系.

3.3 排除信道误码对水印识别的影响

由 3.2 节分析知,应该避免对信道干扰的 MB(Macroblock)[19] 进行水印提取,但是在没有原始视频的情况下,无误差地找出这些 MB 几乎是不可能的. 目前,可以用标准解码器识别语法错误,而隐藏错误识别是难点. 因此,提出了如下计算每个含水印错误 I 帧最终水印错误率 ε_1 的迭代算法,以消除隐藏错误对水印的影响. 迭代算法基本步骤为

1. 初始化参数

$T_S=T_{So}$, $T_{ac}=T_{aco}$, $T_3=T_{3o}$, $M_{Db}=M_{Dbo}$;

$d_1=d_{1o}$, $d_2=d_{2o}$, $d_3=d_{3o}$, $d_4=d_{4o}$;

2. 赋值

$S=\{MB_i \mid i=1,2,\cdots,N\}$,其中 MB_i 为 I 帧中被标准解码器正常解码的亮度宏块;

$N\_e[0]=S$ 中错误水印总数;

$N\_c[0]=S$ 中水印总数;

$berror[0]=N\_e[0]/N\_c[0]$;

$j=0$;

3. 迭代排除

While ($M_{Db}>0$ && $T_{ac}>0$) && ($N\_e[j]>0$ && $N\_c[j]>10$){

$j=j+1$; $x[j]=0$; $y[j]=0$;

For ($i=1:N$) {

判断 MB_i 是否存在 AC 错误;

If (MB_i 不存在 AC 错误)

判断 MB_i 是否存在 DC 错误;

If (MB_i 存在 AC 错误或 DC 错误){

判定 MB_i 是否含水印;

If (含水印){

$y[j]=y[j]+t_1$;//t_1 为 MB_i 中水印数

If (水印错误)

$x[j]=x[j]+t_2$;//t_2 为MB_i 中错误水印数}

将 MB_i 从 S 中删除; }

}

$N\_e[j]=N\_e[j-1]-x[j]$;

$N\_c[j]=N\_c[j-1]-y[j]$;

If ($N\_c[j]>0$)

$berror[j]=N\_e[j]/N\_c[j]$;

$T_{ac}=T_{ac}-d_2$; $M_{Db}=M_{Db}-d_4$;

$N=length(S)$;//求集合 S 的大小

If ($M_{Db}\le 0 \parallel T_{ac}\le 0$) && ($N\_e[j]>0$ && $N\_c[j]>10$) && ($T_S>0$ && $T_3>0$){

$T_S=T_S-d_1$;

$T_3=T_3-d_3$;

$T_{ac}=T_{aco}$, $M_{Db}=M_{Dbo}$;

}

}

4. 计算 ε_1

If $j<5$

$\varepsilon_1=\min(berror[j])$;

Else

$\varepsilon_1=\min(berror[j],berror[j-1],\cdots,berror[j-4])$.

判断 MB 存在 AC 错误的规则为:MB 各 Block 中若一个 Block 存在 AC 系数错误,则该 MB 存在 AC 错误. 将视频 I 帧亮度分量 VLC 解码并反量化到反 DCT 变换前,对每个 Block 的 AC 系数进行错误检测,具体方法[24]:

记 $S=\sum_{i=1}^{64}|AC_i|$, $AC_{\max}=\max\{|AC_1|,\cdots,|AC_{64}|\}$. 若 $S>T_S$ 且 $AC_{\max}/S>T_{ac}$,则此 Block 存在 AC 错误.

判断 MB 存在 DC 错误的规则为：将 I 帧亮度分量解码到像素层，利用空域平滑特性进行 DC 错误检测[25]. 如图 3 所示，current MB、left MB 和 top MB 分别表示待判断的 MB、与其相邻的左边及上边 MB，P_i^{in}、P_i^{out}分别为 current MB 的第 i 个及其邻块的第 i 个边界像素值. 当 top MB 存在时，current MB 与 top MB 的边界差异 $Db_t=\frac{1}{16}\sum_{i=0}^{15}|P_i^{\text{in}}-P_i^{\text{out}}|$，当 top MB 不存在时，$Db_t=0$；current MB 与 left MB 的边界差异 Db_l 同理计算；令 $\overline{Db}=\frac{1}{K}(Db_t+Db_l)$，若 Db_t 与 Db_l 中之一为零，则 $K=1$；否则，$K=2$. 令 $T_{Db}=u+M_{Db}\rho$，其中，

$$u=\frac{1}{N}\sum_{j=0}^{N-1}u_j,\quad \rho=\frac{1}{N}\sqrt{\sum_{j=0}^{N-1}(u_j-u)^2},$$

N 为 current MB 所在 I 帧中已经检测过且不含隐藏错误的 MB 数目，u_j 为第 j 个无错 MB 的 $\overline{Db}$ 值. 如果 $\overline{Db}>\max\{T_{Db},T_3\}$，则 current MB 中含有 DC 错误.

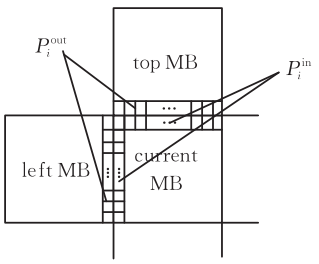


图 3　current MB 的左和上邻块示意图

随着迭代次数的增加，可形成集合$\{berror[j]\}$，$berror[j]$为第 j 步排除完成后 S 的水印错误率，理论上，当 S 中不存在错误 MB 或迭代算法已经没有排除能力后，集合$\{berror[j]\}$表现出收敛特性，即

$$berror[j]=berror[j-1] \tag{5}$$

对于实际问题，严格相等常表现为迭代差异在小范围内波动. 为防止水印过少，而产生迭代结果的剧烈波动，迭代算法要求 $N\_c[j]>10$. 为降低波动的影响，ε_1 为最后 5 次迭代所产生的最小值. 对于正版视频，$\varepsilon_1\in[0,\delta_1]$，对于盗版视频，$\varepsilon_1\in[\lambda-\delta_1,1]$，其中 δ_1 为视频中没有被排除的错误 MB 引起的水印错误率，λ 为盗版视频水印错误率. 迭代算法性能及 ε_1 概率密度函数在第 4.4 节进行测试.

3.4　识别算法

结合 3.1 节的嵌入算法和 3.3 节的迭代算法，提出了如下识别算法，流程图见图 4，基本步骤为

1. 对阈值 T、δ 进行赋值.

2. 初始化参数：$sum=0$，$n=0$.

3. 从 video coded data 中对 I 帧亮度分量进行 VLC 解码，若检测到语法错误，则跳到下一个同步标记处开始重新解码.

4. 计算 I 帧水印错误率 $berror$，$n=n+1$.

根据第 3.1 节嵌入算法的步 1 和步 2，寻找水印承载单位 WB 和 Ac_{last} 上应该携带的水印 w. 提取 Ac_{last} 上实际承载的水印 $\overline{w}$：当 Ac_{last} 为偶数时，$\overline{w}=0$，当 Ac_{last} 为奇数时，$\overline{w}=1$. 如果 $w\neq\overline{w}$，则该 WB 携带的水印错误；否则正确.

根据 I 帧 WB 数目及水印错误数量，计算 $berror$，$berror=I$ 帧错误水印总数/I 帧水印总数.

5. 若 $berror=0$，则检测结束标志，若视频全部 I 帧分析完毕，则视为检测到结束标志，转步 6；否则转步 3，继续解码下一个 I 帧.

若 $berror>T$，则此视频不需进一步判定，识别算法终止，不是正版.

若 $0<berror\leq T$，判断能否迭代，若不能则 $sum=sum+berror$；若能则根据 3.3 节算法迭代算法计算 ε_1，$sum=sum+\varepsilon_1$. 检测结束标志，若检测到结束标志，则转步 6；否则转步 3.

6. 当 $\frac{sum}{n}<\delta$ 时，为正版视频，否则不是正版.

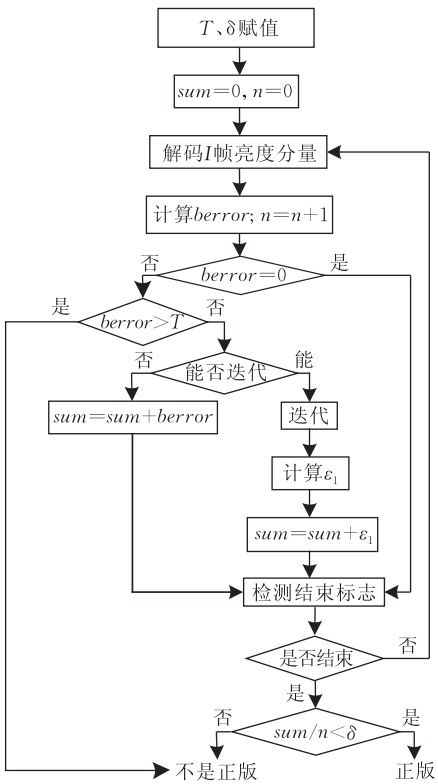


图 4　TDIA 识别算法流程图

在识别算法中，对 δ 的赋值在 4.5 节结合识别误差讨论. 对 T 可采用如下 3 种方式之一赋值：

(1) 令

$$T=\frac{\alpha\times L\times(m/4)}{M} \tag{6}$$

其中,α 为二进制视频码流所面临的比特误码率(bit error rate),L 为视频全部 I 帧在码流中的比特位总长度,M 为视频水印总 bit 数,m 为 1 个 Slice 中包含的 Block 数目. 由于 1bit 错误的最大影响区间为 1 个 Slice[19],因此,T 为在信道干扰下 I 帧最大平均水印错误率. 这样赋值有助于提高识别速度.

(2) 令 T 为正版视频具备观赏价值下可容忍的最大水印错误率,具体可结合错误恢复算法[24-25]进行统计评估. 这样赋值可提高识别速度.

(3) 令 $T=1$. 不出现不需要进一步判断的情形.

4 TDIA 算法性能测试

测试环境:

(1) Intel Pentium CPU:1600MHz,内存 256MB.

(2) Mpeg2 Codec vision 1.2①.

4.1 嵌入算法性能测试

测试内容为:(1) 水印嵌入带来的视频质量下降,用相同码率下,水印嵌入后视频各帧 PSNR 下降的平均值 *mpsnr* 来衡量. (2) 水印嵌入总量,用 w_{total} 表示. (3) 水印嵌入耗时 *e-time*.

令嵌入算法参数 $k1=0.00252$、$k2=100$、$T_{\text{embed}}=30$. 压缩参数为:每个视频时长为 1s、帧率 30 帧/s、$GOP=6$、I/P 帧距为 3. 在 1Mbps、2Mbps、3Mbps、4Mbps 码率下,4 个视频② container、coastguard、foreman、hall_monitor 的测试结果见表 1. 从表 1 中数据可以看出:水印对视频 PSNR 影响微乎其微,水印嵌入量较多,嵌入耗时不大. 一定的水印嵌入量可以保证识别精度以及防止 3.3 节迭代结果因为水印量过少而出现抖动.

表 1 基于 Mpeg2 Codec,水印嵌入算法性能测试结果表

视频	码率/Mbps	*mpsnr*	w_{total}	*e-time*/s
container	1	0.128	1050	6.10
	2	0.117	1685	6.10
	3	0.089	1948	6.61
	4	0.099	2144	7.02
coastguar	1	0.077	971	6.10
	2	0.085	1782	6.10
	3	0.078	2148	7.12
	4	0.072	2259	7.12
hall_monitor	1	0.052	323	6.10
	2	0.051	810	7.02
	3	0.066	1231	7.02
	4	0.057	1585	7.12
foreman	1	0.039	439	5.09
	2	0.077	1206	6.11
	3	0.076	1678	6.11
	4	0.071	1949	7.12

4.2 水印对盗版操作的脆弱性测试

把正版视频解码成帧序列,再把帧序列按如下压缩参数设置方法压缩成盗版:

盗版 1. 压缩参数设置同正版;

盗版 2. 除码率增大外,其它同正版;

盗版 3. 除码率减小外,其它同正版;

盗版 4. 码率增大、I/P 帧距减小,其它同正版.

以 container 正版视频测试这 4 种盗版方式的水印错误率,测试结果见图 5(a)~(d). 图 5 中,*perror* 指盗版视频各 I 帧水印平均错误率. 图 5(a)是将码率分别为 0.6Mbps~8Mbps 的 container 正版分别按盗版 1 盗版的测试结果,图 5(b)是将 0.6Mbps 正版按盗版 2 分别将码率增大到 0.7Mbps~8Mbps 后的测试结果,图 5(c)是将 8Mbps 正版按盗版 3 将码率逐步减少到 7.9Mbps~0.6Mbps 的测试结果. 图 5(d)是将 1Mbps 正版 I/P 帧距减小 1,码率增大到 1.1Mbps~8Mbps 的测试结果. 测试中之所以选择 0.6Mbps 以上视频,是因为当码率小于 0.6Mbps 时,Mpeg2 标准编码器压缩的视频存在明显的马赛克.

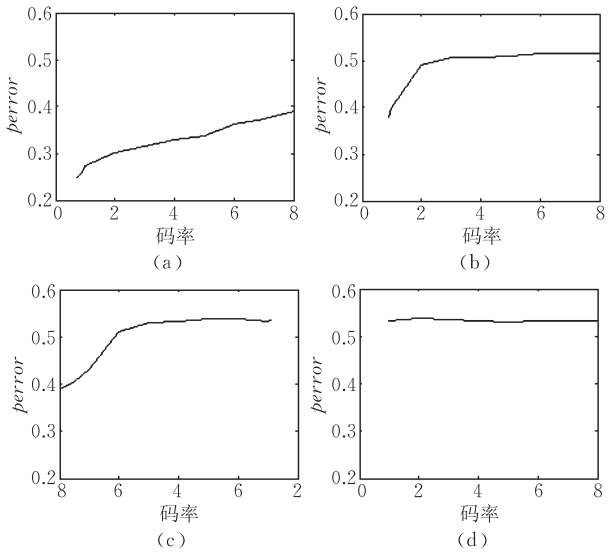


图 5 水印对盗版的脆弱性测试结果图

从图 5(a)~(d)对比可知:盗版视频的 *perror*>0.2,盗版 1 方式是对水印保持最好的方式. 由测试结果可以看出水印对盗版操作脆弱.

① Mpeg-2 source code for version 1.2. http://www.mpeg.org/MSSG

② http://www.cipr.rpi.edu/resource/sequences/sif.html 或 http://see.xidian.edu.cn/faculty/xbgao/html/VIPSL/database_Video.html

4.3　通信干扰对水印影响测试

在没有通信干扰时，正版视频各 I 帧水印错误率为零. 码率为 0.9Mbps 的 8s container 正版视频，码流遭受 $BER=6\times10^{-4}$ 干扰后，各 I 帧水印错误率见图 6(a)，各 I 帧平均水印错误率 $perror=0.1541$. 利用盗版方式 1 对该正版视频进行盗版，在同样信道干扰下，各 I 帧水印错误率见图 6(b). 对比图 6(a)、(b)可以看出，通信干扰使得 container 正版、盗版 *perror* 趋同.

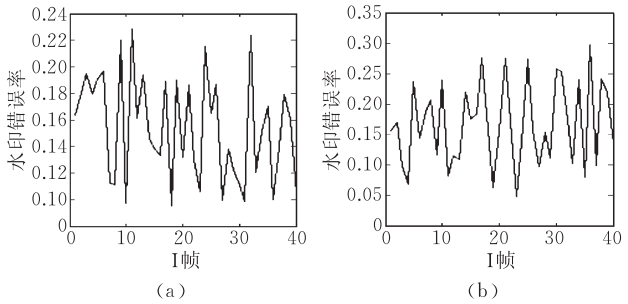


图 6　通信干扰后正版、盗版视频各 I 帧水印错误率示意图

4.4　迭代算法效果测试

遭受信道干扰后，正版视频某 I 帧(见图 7(a))水印错误率为 0.15，盗版视频某 I 帧(见图 7(b))水印错误率也为 0.15. 用 3.3 节迭代算法对两幅图进行干扰排除，图 7(c)、(d)分别绘出了对图 7(a)、(b)进行迭代时，集合 S 的水印错误率变化曲线，横坐标为迭代次数 j，纵坐标为 $berror[j]$. 在图 7(c)中，迭代 16 次，错误全部被排除，在图 7(d)中，迭代 86 次后 *berror* 收敛于 0.25. 迭代算法所使用的参数值为 $T_{So}=100$，$T_{aco}=0.95$，$T_{3o}=10$，$M_{Dbo}=5$；$d_{1o}=10$；，$d_{2o}=0.05$，$d_{3o}=1$，$d_{4o}=0.1$.

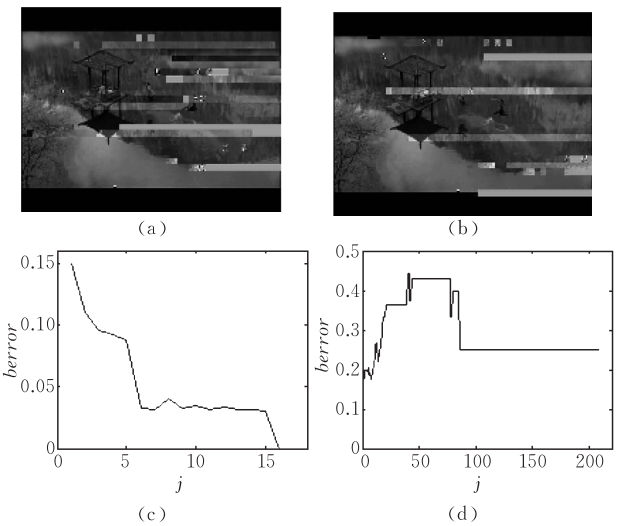


图 7　迭代算法迭代效果图

测试第 3.3 节 ε_1 的概率密度函数，测试样本为遭遇干扰的 *BER* 值为$[10^{-4},10^{-3}]$的正版、盗版 1 方式盗版视频，干扰方式为对视频码流随机加扰，迭代测试结果见图 8(a)、(b)，横坐标为 ε_1，纵坐标为概率 $p(\varepsilon_1)$. 对于正版视频 I 帧，ε_1 的数学期望为 $E(\varepsilon_1)=0.036$；对于盗版视频 I 帧，$E(\varepsilon_1)=0.352$.

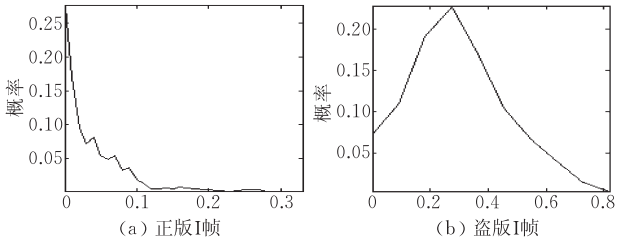


图 8　遭遇干扰的正版、盗版视频 I 帧 ε_1 概率密度函数图

进一步测试表明，当 *BER* 小于 10^{-4} 时，正版视频 I 帧的 $E(\varepsilon_1)\leq0.036$，盗版方式 1 盗版视频 I 帧的 $E(\varepsilon_1)$ 仍为 0.352. 对于其它盗版方式，$E(\varepsilon_1)=0.5$.

4.5　TDIA 算法误识别率分析

Chernoff Bound 定理[26-27]. 如果 $X_1,X_2,\cdots,X_n$ 是独立且 $0\leq X_i\leq1$，$i=1,2,\cdots,n$ 的随机变量，记 $x=E(\sum_{i=1}^{n}X_i/n)$，则对任意 $0<\delta<1$，有

(i) 当 $\delta<x$ 时，$P(\sum_{i=1}^{n}X_i\leq n\delta)\leq2^{-nD(\delta\|x)}$　(7)

(ii) 当 $\delta>x$ 时，$P(\sum_{i=1}^{n}X_i\geq n\delta)\leq2^{-nD(\delta\|x)}$　(8)

其中，$D(\delta\|x)=\delta\log_2\frac{\delta}{x}+(1-\delta)\log_2\frac{1-\delta}{1-x}$.

利用 Chernoff Bound 定理，求识别算法的漏检概率 P_1，即正版视频满足 $sum/n\geq\delta$ 的概率. 由于正版视频每个 I 帧的水印错误率可以看作一个随机变量，这些随机变量独立且取值在$[0,1]$，满足 Chernoff Bound 定理条件，因此，由式(8)，$P_1=P(sum/n\geq\delta)\leq2^{-nD(\delta\|E(\varepsilon_1))}$，$E(\varepsilon_1)$ 为正版视频 I 帧水印错误率的数学期望. 当 $E(\varepsilon_1)\in(0,0.036]$时，$D(\delta\|E(\varepsilon_1))$ 为 $E(\varepsilon_1)$ 的递减函数，因此，对于 $\forall E(\varepsilon_1)\in(0,0.036]$，都有 $D(\delta\|E(\varepsilon_1))\geq D(\delta\|0.036)$，$P_1\leq2^{-nD(\delta\|0.036)}$.

利用 Chernoff Bound 定理，求识别算法的误检概率 P_2，即盗版视频满足 $sum/n\leq\delta$ 的概率，由式(7)，$P_2=P(sum/n<\delta)\leq2^{-nD(\delta\|E(\varepsilon_1))}$，$E(\varepsilon_1)$ 为盗版视频 I 帧水印错误率的数学期望. 当 $E(\varepsilon_1)\in[0.352,1)$时，$D(\delta\|E(\varepsilon_1))$为 $E(\varepsilon_1)$的递增函数，因此，$\forall E(\varepsilon_1)\in[0.352,1]$，都有 $D(\delta\|E(\varepsilon_1))\geq D(\delta\|0.352)$，$P_2\leq2^{-nD(\delta\|0.352)}$.

既不是正版也不是盗版的视频称为无关视频，

这些视频的 I 帧仍是符合 Chernoff Bound 定理的随机变量，且 $E(\varepsilon_1)=0.5$，因此用式(7)可计算把无关视频识别为正版的概率 P_3，$P_3=P(sum/n<\delta)\leq 2^{-nD(\delta\|0.5)}$.

可根据识别误差，对 δ 进行赋值. 当 $T=1$、$\delta=(0.352-0.036)/2=0.158$ 时，$P_1\leq 2^{-0.1728n}$、$P_2\leq 2^{-0.1355n}$、$P_3\leq 2^{-0.3705n}$. 这表明当信道干扰 BER 小于等于 10^{-3} 时，算法漏检率及误检率随着 n 的增加，指数级下降. 当 $n=360$ 时，$P_1\leq 1.88e^{-19}$、$P_2\leq 7.55e^{-18}$、$P_3\leq 7.06e^{-41}$. 通常视频每秒不少于 2 个 I 帧，$n=360$ 相当于不超过 3min 的视频时长.

5 结束语

在分析了版权保护技术现状的基础上，本文提出一种有效识别正版视频的算法：TDIA 算法. 在设计上，它结合了视频编码标准、脆弱数字水印、视频通信技术. TDIA 算法包含两部分：嵌入算法及识别算法. 在 3.1 节描述了嵌入算法，在其设计上考虑了安全性、脆弱性、一定的水印嵌入量以及使所嵌入的水印 0/1 各占 50%，对 Ac_{last} 奇偶性更改概率为 50%，以便保证无关视频 I 帧水印错误率的数学期望为 $E(\varepsilon_1)=0.5$. 基于通信干扰与盗版操作对水印影响的本质不同，在 3.3 节提出了排除干扰的迭代算法，4.4 节测试了其性能. 在 3.4 节提出了识别算法并在 4.5 节基于 $E(\varepsilon_1)$、有界随机变量和的 Chernoff Bound 定理，分析了 TDIA 算法的识别误差. 理论和仿真表明，对于 $BER\leq 10^{-3}$、视频 I 帧总数 $n\geq 360$ 的 Mpeg2 编码视频，TDIA 算法能给出识别误差小于 10^{-18} 的识别结果. 并且随着视频的延长，识别结果指数级下降. 另外，TDIA 算法也可应用于其它编码标准，可用于终端在线检测，也可用于离线检测. 它是一种安全性高、识别准确率高、对通信干扰具备一定容忍性的正版视频识别算法. 将 TDIA 算法与 VideoDNA 技术结合，可实现盗版视频过滤、禁播等.

参 考 文 献

[1] Eskicioglu A M, Town J, Delp E J. Security of digital entertainment content from creation to consumption. Signal Processing: Image Communication, 2003, 18(4): 237-262

[2] GY/Z 175-2001. Specifications of conditional access system for digital television broadcasting. The State Administration of Radio, Film, and Television, 2001(in Chinese)
(GY/Z 175-2001. 数字电视广播条件接收系统规范. 国家广播电影电视总局, 2001)

[3] Eskicioglu A M, Delp E J. An overview of multimedia content protection in consumer electronics devices. Signal Processing: Image Communication, 2001, 16(7): 681-699

[4] Maes M, Kalker T, Linnartz J P M G et al. Digital watermarking for DVD video copy protection. IEEE Signal Processing Magazine, 2000, 17(5): 47-57

[5] Andreaux J P, Durand A, Furon T et al. Copy protection system for digital home networks. IEEE Signal Processing Magazine, 2004, 21(2): 100-108

[6] Radhakrishnan R, Memon N. Multimedia analysis for content identification//Multimedia Content Analysis, Signals and Communication Technology. Springer, 2009: 275-295

[7] Nikolaidis N, Pitas I. Image and video fingerprinting for digital rights management of multimedia data//Proceedings of the International Symposium on Intelligent Signal Processing and Communication Systems. Japan, 2006: 801-807

[8] Trappe W, Wu M, Wang Z, Ray Liu K J. Anti-collusion fingerprinting for multimedia. IEEE Transactions on Signal Processing, 2003, 51(4): 1069-1087

[9] Wu M, Trappe W, Wang Z, Ray Liu K J. Collusion resistant fingerprinting for multimedia. IEEE Signal Processing Magazine, 2004, 21(2): 15-27

[10] Zhou Guo-Rui, Wang Wen-Jiang, Sun Shi-Xin. Research on the realization of anti-collusion fingerprinting. Computer Science, in press(in Chinese)
(周国瑞，王文江，孙世新. 抗共谋数字指纹实现问题研究. 计算机科学，2010，(1)：待发表)

[11] Nakashima Y, Tachibana R, Babaguchi N. Watermarked movie soundtrack finds the position of the camcorder in a theater. IEEE Transactions on Multimedia, 2009, 11(3): 443-454

[12] Ekici Ö, Sankur B, Akcay M. A comparative evaluation of semi-fragile watermarking algorithms. Journal of Electronic Imaging, 2004, 13(1): 209-219

[13] Yoshida K, Murabayashi N. Tiny LSH for content-based copied video detection//Proceedings of the International Symposium on Applications and the Internet. Turku, Finland, 2008: 89-95

[14] Stockhammer Thomas, Hannuksela Miska M, Wiegand Thomas. H.264/AVC in wireless environments. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(7): 657-672

[15] Chen M, He Y, Lagendijk R L. A fragile watermark error detection scheme for wireless video communications. IEEE Transactions on Multimedia, 2005, 7(2): 201-211

[16] Lee M J, Kim K S, Lee H Y et al. Robust watermarking detection against D-A/A-D conversion for digital cinema using local auto-correlation function//Proceedings of the IEEE International Conference on Image Processing. San Diego, CA, USA, 2008: 425-428

[17] Chupeau B, Massoudi A, Lefèbvre F. In-theater piracy: Finding where the pirate was//Proceedings of the SPIE. San Jose, CA, USA, 2008, 6819: 68190T1-68190T10

[18] Lin E T and Delp E J. A review of fragile image watermarks//Proceedings of the Multimedia and Security Workshop(ACM Multimedia'99). Orlando, Florida, USA, 1999: 25-29

[19] Zhong Yu-Zhuo, Wang Qi, Zhao Li, Yang Xiao-Qin. MPEG-2 International Standard for Moving Picture Compression Coding and New Progresses in MPEG. Beijing: Tsinghua University Press, 2002(in Chinese)
(钟玉琢，王琪，赵黎，杨小勤. MPEG-2 运动图像压缩编码国标准及 MPEG 的新进展. 北京：清华大学出版社，2002)

[20] Bi Hou-Jie. The New Generation of Video Compression Coding Standard: H. 264/AVC. Beijing: People's Posts & Telecom Press, 2005(in Chinese)
(毕厚杰. 新一代视频压缩编码标准——H. 264/AVC. 北京：人民邮电出版社，2005)

[21] Li Zhao-Hong, Hou Jian-Jun. DCT-domain fragile watermarking algorithm based on Logistic maps. Chinese Journal of Electronics, 2006, 34(12): 2134-2137(in Chinese)
(李赵红，侯建军. 基于 Logistic 混沌映射的 DCT 域脆弱数字水印算法. 电子学报，2006, 34(12): 2134-2137)

[22] Abdat M, Kachouh Z A, Bellanger M G. Transmission error detection and concealment in JPEG images. Signal Processing: Image Communication, 1998, 13(1): 45-64

[23] Hadar O, Huber M, Huber R. Hybrid error concealment with automatic error detection for transmitted MPEG-2 video streams over wireless communication network//Proceedings of the International Conference on Information Technology: Research and Education, Tel Aviv, Israel, 2006: 106-109

[24] Zhang H H, Wang J, Liu Y Q, Wang J, Gao Y Z. An efficient two-stage error detector based on syntax and continuity. IEEE Transactions on Consumer Electronics, 2007, 53(4): 1276-1280

[25] Wu G L, Chien S Y. Spatial-temporal error detection scheme for video transmission over noisy channels//Proceedings of the 9th IEEE International Symposium on Multimedia. Taichung, Taiwan, 2007: 78-85

[26] Hoeffding W. Probability inequalities for sums of bounded random variables. Journal of the American Statistical Association, 1963, 58(301): 13-30

[27] Hagerup Torben, Christine R U B. A guided tour of chernoff bounds. Information Processing Letters, 1990, 33(6): 305-308

ZHOU Guo-Rui, born in 1974, Ph. D. candidate. Her research interests include data compression, wavelet theory, digital watermarking, and copyright protection technology.

WANG Wen-Jiang, born in 1974, senior engineer. His research interests include graphics & image, and 3G mobile communication technology.

SUN Shi-Xin, born in 1940, professor, Ph. D. supervisor. His research interests include information compression, network computing, parallel & distributed computing, numerical computing, and combinatorial algorithm.

Background

Two key aspects of the copyright protection mechanism are transmission security and consumption security. The transmission security is realized based on network protocol and conditional access technology. The consumption security is realized based on active prevention and passive defense strategies. The active prevention can prevent illegal copy from end to end, but can not prevent the analog hole piracy. In recent years, the problem of analog hole piracy has become more serious due to technical advances in recoding devices. Motion Picture Association claims that over 90% of the pirated movies of new release titles are illegal recordings made by camcorder piracy.

Watermarking is considered as a promising technology to close the analog hole. Some robust watermarking techniques have been proposed for detecting the illegal recordings and traitor tracing. However, the survival of robust watermarking through the analog path is a very tough problem because of spatio-temporal desynchronization and geometric distortions like zooming, translation, rotation, and projection.

This paper presents a TDIA algorithm to identify genuine videos. The TDIA algorithm is designed based on integration of fragile watermarking, video compression standards and video communication technology. The total identification error of the algorithm is less than 10^{-18} when BER (Bit Error Rate) of encoded video stream is not more than 10^{-3} and the total number of I-frames of the Mpeg2 encoding video is more than 360. Pirated video can be filtered based on combination of TDIA algorithm and VideoDNA technology.