Journal of Computer Applications
计算机应用,2013,33(12):3531-3535
ISSN 1001-9081
CODEN JYIIDU
2013-12-01
http://www.joca.cn

文章编号:1001-9081(2013)12-3531-05
doi:10.11772/j.issn.1001-9081.2013.12.3531

面向网关版权保护的抗几何攻击视频水印方法

刘洪滨*,杜　玲,姬红利
(天津大学 计算机科学与技术学院,天津 300072)
(*通信作者电子邮箱 liuhongbin2007@gmail.com)

摘　要:为了解决网关视频的版权保护问题,提出了一种网关视频水印快速嵌入和提取方法。该方法在视频帧内,首先以近线性时间检测和挑选仿射协变区域,然后采用基于最小生成树的区域选择算法消除重叠区域,最后以线性时间在离散小波变换域内嵌入水印;在视频帧间,利用视频场景的连续性基于场景边界仿射协变区域预测场景内部仿射协变区域以达到整体加速的目的。攻击实验表明:对测试序列嵌入水印后,针对几何攻击和格式变换压缩攻击,水印检测准确率分别达到93%和83%以上。仿真实验表明:在400在线主机局域网内,该方法能在10帧以内成功阻断网关水印视频的传输。

关键词:视频水印;场景边界检测;网关过滤;版权保护;最小生成树;特征提取
中图分类号:TP309　　**文献标志码**:A

Fast geometric resistant video watermarking scheme for gateway copyright protection

LIU Hongbin*, DU Ling, JI Hongli
(*School of Computer Science and Technology, Tianjin University, Tianjin 300072, China*)

Abstract: To solve the problem of gateway copyright protection, a new fast approach was put forward for embedding and extracting gateway watermark in digital video. In intra frame watermarking, the method elegantly detected and selected affine covariant regions in nearly linear complexity. Then, the overlapped affine covariant regions were eliminated based on minimal spanning tree. Last, watermark bits were embedded in Discrete Wavelet Transform (DWT) coefficients in linear time. In inter frame watermarking, the method effectively utilized the continuity inside video scenes to predict the affine covariant regions in no-boundary frames based on boundary frame. The attacking experimental results show that under geometric attacks and format conversion attacks, the accuracies of watermark detection are above 93% and 83% respectively. The simulation results show that in local network with 400 online hosts, the proposed method can block gateway watermark video transmission within 10 frames.

Key words: video watermarking; shot transition detection; gateway filtering; copyright protection; minimal spanning tree; feature detection

0　引言

随着万维网的快速发展,通过网络对数字视频内容进行复制、修改和发布变得越来越简单,内容安全和版权保护也变得越来越受重视。在许多点对点(Peer-to-Peer,P2P)网站、用户视频网站存在大量未获得版权许可的多媒体内容。这些内容很大部分是从广告公司、动画公司等内容提供商内部局域网泄露出来的,给版权所有者造成重大经济损失。因此,迫切需要一种有效方法来解决这类版权保护问题。

为防止数字内容的非法传播,提出了许多视频水印技术[1-3]。通常根据水印嵌入载体内容形式不同,将现有视频水印方法分成两大类:1)原始视频水印[4],在视频压缩前嵌入水印;2)比特流水印[5],在视频压缩后嵌入水印。例如一种针对MPEG-4视频流的水印方法[6]从MPEG-4比特流恢复出视频中物体对象的量化系数,然后修改系数嵌入水印。该方法存在的主要问题是水印直接嵌入MPEG-4比特流,一旦采用不同压缩标准(比方说MPEG-2)进行格式转化水印信息就会丢失。为了达到抗格式转换的目的,水印必须在视频压缩前嵌入,即在视频帧嵌入。为此,Barni等[7]通过在视频压缩前修改每一帧物体的小波系数来嵌入水印。该方法的主要缺陷是计算复杂度高,不能用于实时水印嵌入和提取。如果视频载体分辨率低且计算设备性能足够高,尚且可以做到实时水印嵌入或提取。然而在许多应用场景特定硬件设备(如现场可编程门阵列(Field Programmable Gate Array,FPGA)[8],机顶盒(Set-Top Box, STB[9])对计算时间和计算能力有严格的限制。本文方法属于原始视频水印方法,采用视频帧预测突破了网关设备的时间和计算约束。

目前存在许多针对不同应用的视频水印方法。对于版权保护,水印视频必须对各类恶意或非恶意攻击具有鲁棒性。几何攻击因其常见性和复杂性,抗几何攻击水印算法在近几年成为研究热点。现有抗几何攻击水印方法可以分为三大类:参数恢复技术、不变域技术和基于不变特征区域的局部水印技术。第一类方法首先估计几何变换参数,然后根据变换参数恢复出受攻击前水印载体,最后提取水印。该类方法的主要局限在于参数估计的准确性无法保障。在第二类方法中,水印嵌入在几何不变域。尽管几何不变域在一定程度上

收稿日期:2013-06-25;**修回日期**:2013-08-13。　**基金项目**:中国科学院科技先导项目(XDA06030601)。
作者简介:刘洪滨(1989-),男,湖南娄底人,硕士研究生,主要研究方向:图像处理、视频水印;　杜玲(1982-),女,辽宁沈阳人,博士研究生,主要研究方向:多媒体信息安全、数字水印、信息隐藏;　姬红利(1989-),女,山东济宁人,硕士研究生,主要研究方向:计算机视觉、图像处理。

抗旋转和尺度攻击,但受局部几何变换攻击容易损坏。

基于不变特征区域的局部水印技术利用图像特征的可重复性来确定水印嵌入位置,有效解决了水印嵌入和提取过程中的同步问题。当前,最出色的仿射协变特征检测器是尺度不变特征变换检测器(Scale Invariant Feature Transform, SIFT)[10]和最大稳定极值区域检测器(Maximally Stable Extremal Regions, MSER)[11]。SIFT 检测器提取的特征区域对光照和视角变化具有鲁棒性。MSER 检测器则提取图像稳定连通区域作为仿射协变区域。出于时间效率考虑,本文方法的帧内水印算法主要基于文献[7,12]的工作,在 MSER 仿射协变区域的离散小波变换(Discrete Wavelet Transform, DWT)域嵌入水印。

1 帧内水印

1.1 MSER 提取算法

帧内水印需要提取几何不变特征区域用于水印同步。本文选择 MSER 特征区域有两个原因:1)在 Mikolajczyk[13]的特征性能比较中 MSER 表现最好,具有更好的抗几何攻击能力;2)MSER 效率最高。

MSER 最初由 Matas[11]提出用于宽基线匹配,通过判断图片相邻像素间的灰度值变化并以合适的阈值筛选出连通区域。MSER 检测过程由三步构成:1)按灰度值排列像素点并合并连通组件;2)检测极值区域;3)确认最大稳定极值区域。使用桶排序(Bin Sort)算法,像素点排序可以在 $O(n)$ 时间内完成;使用并查集算法,组建合并可以在 $O(n \log\log(n))$ 时间内完成。这说明可以用近线性时间快速检测 MSER。检测出的原始 MSER 如图 1(a)所示。

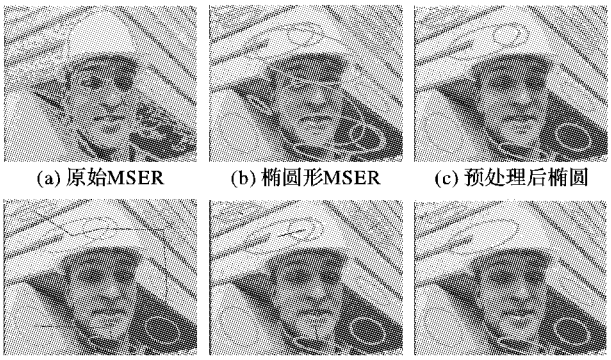
由于原始 MSER 形状不规则难于表示,需要为其构建形状描述符。通过计算原始 MSER 区域的均值和方差将其拟合成椭圆区域。拟合的椭圆形 MSER 如图 1(b)所示。

1.2 MSER 过滤算法

MSER 检测器通常会提取密布整个图片的许多 MSER 区域,拟合后椭圆区域间存在大量重叠,水印在这些重叠区域的重复嵌入会导致提取混乱。因此,在水印嵌入前必须自动去除重叠区域。

基于 MSER 特性,在预处理阶段直接去除面积过大和过小的不稳定区域。选择面积大小下界阈值 τ_1 和面积大小上界阈值 τ_2,过滤掉面积满足 $|R_i| < \tau_1$ 或 $|R_i| > \tau_2$ 条件的 MSER 区域,其中 $|R_i|$ 表示第 i 个 MSER 区域的面积。经预处理后的 MSER 区域如图 1(c)所示。

为过滤重叠区域,首先构建图模型以分类 MSER 区域。每个椭圆区域记为顶点 V_i,各顶点之间互连构成无向完全连通图 G,顶点之间边 e_j 的权重 w_j 等于对应顶点间距离值。构图的目的是剪切 G 中加权边生成无连通森林。森林中的每个连通子图表示一个聚类,每个顶点属于且只属于某个特定的聚类。这里使用最小生成树算法剪切加权边。最小生成树算法倾向于删除权值过大的边,使得相距较远的 MSER 区域更易于分配到不同的聚类。MSER 区域最小生成树如图 1(d)所示。进一步选定阈值 w_τ 删除最小生成树中权值 $w_i > w_\tau$ 的边。如此生成一定数量的聚类,每个聚类包含多个 MSER 区域。MSER 聚类如图 1(e)所示。最后在每个聚类中保留面积最大的 MSER 区域作为最终选择。最终挑选的 MSER 区域如图 1(f)所示。



(a) 原始MSER (b) 椭圆形MSER (c) 预处理后椭圆

(d) 最小生成树 (e) 聚类 (f) 最终挑选区域

图 1 MSER 检测和挑选

MSER 过滤算法总结如下:

1)删除面积过大和过小的 MSER 区域;

2)在完全加权图上使用最小生成树算法生成最小生成树;

3)截断最小生成树生成 MSER 聚类;

4)保留每个聚类中面积最大的 MSER 区域作为最终选择。

1.3 水印嵌入

水印嵌入过程从解码视频比特流成原始帧序列开始,在每一帧使用 MSER 检测器与过滤算法提取和挑选出 MSER 区域,并嵌入相同水印。详细水印嵌入过程如下:

1)按 1.1 节和 1.2 节所述算法提取和选择椭圆区域。

2)归一化每个选择的椭圆区域成预定大小的圆形区域,计算圆形区域的主方向并旋转至正北方向。

3)对每个圆形区域进行离散小波变换生成小波系数。

4)将二值水印图片缩放至 $r \times r$ 大小。记小波变换水平高频竖直低频系数和水平低频竖直高平系数分别为 HL 和 LH,对应系数间差值为 $D(x,y)$。

$$D(x,y) = HL(x,y) - LH(x,y) \tag{1}$$

对于每个水印位,对应修改相同位置的小波系数差值,使其满足条件:

$$\begin{cases} D'(x,y) \geqslant \alpha, & W(x,y) = 1 \\ D'(x,y) < \alpha, & W(x,y) = 0 \end{cases} \tag{2}$$

其中:$D'(x,y)$ 表示在 (x,y) 处修改后的小波系数差;α 表示水印强度。在每一个 (x,y) 位置重复上述过程可将水印信息全部嵌入小波系数域。这里,水印鲁棒性随 α 的增大而增强,但其可见性也相应降低。

对嵌入水印后的小波系数进行反向离散小波变换还原成空间区域,再经反向归一化后替换原视频帧中椭圆区域。

1.4 水印提取

与水印嵌入过程相同,水印提取过程首先使用 MSER 检测器与过滤算法提取和选择 MSER 区域,然后对 MSER 区域经行归一化和主方向旋转。

从小波系数 HL 和 LH 提取水印的方法如下:

$$W'(x,y) = \begin{cases} 1, & D'(x,y) \geqslant 0 \\ 0, & D'(x,y) < 0 \end{cases} \tag{3}$$

其中:$D'(x,y) = HL'(x,y) - LH'(x,y)$,$HL'(x,y)$ 和 $LH'(x,y)$ 分别表示 (x,y) 位置的水平高频竖直低频系数和水平低频竖直高频系数。

提取出所有水印位 W' 后,计算 W 和 W' 间的归一化相关值 z_{nc}:

$$z_{nc} = (W \cdot W') / |W| \tag{4}$$

其中 $|W|$ 表示 W 的长度。如果 z_{nc} 大于特定阈值 τ_{nc},可认为该区域包含水印信息。

如前所述,在每一帧中通常存在多个 MSER 区域。因此,在只要某一帧检测到某个 MSER 区域存在水印即可认为该视频嵌入了水印信息。在多个区域重复嵌入水印使得视频即使经过变形也能提取出水印信息。最终提取出的水印由投票决定。记 $Num_1(x,y)$ 表示在 (x,y) 位置提取到的水印位"1"的数目,$Num_0(x,y)$ 表示在 (x,y) 位置提取到的水印位"0"的数目。最终水印表示如下:

$$W^*(x,y) = \begin{cases} 1, & Num_1(x,y) \geqslant Num_0(x,y) \\ 0, & iNum_1(x,y) < Num_0(x,y) \end{cases} \tag{5}$$

投票水印 $W'(x,y)$ 和原水印 W 间的归一化相关系数 z_{voting} 用于决定水印信息的存在与否。

$$z_{voting} = (W \cdot W^*) / |W| \tag{6}$$

2　帧间水印

鉴于当前商用网关设备有限的计算能力和光纤的高速传输速度,用于局域网版权保护的水印算法必须足够快速而不至于阻碍数据包的传输。然而如引言中提到的,原始视频帧水印算法的逐帧计算方式在时间和资源方面消耗很大。所以降低逐帧计算的计算量非常有意义。

分析第 1 章中所述帧内水印算法可知,其计算量主要集中在 MSER 区域提取、椭圆拟合和重叠区域过滤上。通过观察发现大部分用户视频可以划分为多个独立的时间单元,也即场景,场景内部的视频帧作微小的连续变化。这表明可以在帧间作 MSER 预测,减少帧间冗余的 MSER 提取、拟合和过滤操作。

2.1　场景边界检测

场景边界检测用于将视频分割成多个时间序列。一个场景是由单个相机拍摄的连续相关图片集,表示时空上的一个连续动作。结合网关数据包在线处理,场景边界检测必须在视频完整捕获前完成。这里采用基于局部视频帧变化[14]的场景边界系数模型。

为了度量帧间变化,选取 $2N+1$ 帧的局部窗口,第 i 帧的局部窗口帧差定义为:

$$D_{sw}(i) = \sum_{j=1}^{N} \frac{N-j+1}{K} D(i-j, i+j) \tag{7}$$

其中:$K = \sum_{k=1}^{N} k$;$D(m,n)$ 表示第 m 帧和第 n 帧之间的差值,其计算使用直方图交,如式(8):

$$D(m,n) = 1 - \frac{1}{XY} \sum_{l=0}^{L-1} \min(H(m,l), H(n,l)) \tag{8}$$

其中:X,Y 表示帧宽度和高度,L 表示灰度级,$H(m,l)$ 表示第 m 帧直方图的第 l 个直方柱的值。

局部窗口帧差和帧像素相关,可使用场景边界检测算子归一化成场景边界相似系数(C_{SBS}):

$$C_{SBS}(i) = \frac{\sum_{j=-N}^{N-1} (D_{sw}(i+j) \times O_{sw}(N+j))}{\sqrt{\sum_{j=-N}^{N-1} (D_{sw}(i+j))^2} \times \sqrt{\sum_{j=-N}^{N-1} (D_{sw}(N+j))^2}} \tag{9}$$

其中:$O_{sw}(j)$ 表示场景边界检测算子,$N=3$ 时,算子为(1,3,6,6,3,1)。

通常,C_{SBS} 在场景边界处接近 1,但分布相对集中。为增大分辨力度,使用指数函数定义场景边界系数 C_{SB}:

$$C_{SB}(i) = \exp(-\alpha(1 - C_{SBS}(i))) \tag{10}$$

其中 α 是常量,$\alpha \in [5,15]$,实验中取 $\alpha = 10$。

场景边界系数有两个特性:抗噪声能力强以及对视频运动不敏感,因此与特定阈值结合可用于场景边界检测。

2.2　帧间 MSER 预测

对每个视频场景,我们在场景边界帧使用帧内水印算法嵌入水印,边界后续帧则使用光流算法[15]预测 MSER 的位置,省去 MSER 的检测、拟合和选择过滤操作。同一场景内后一帧 MSER 的位置由前一帧 MSER 移动得到。在每个椭圆区域计算光流中值 (u,v),以此作为 MSER 平移向量。MSER 平移公式如下:

$$(x',y') = (x,y) + (u,v) \tag{11}$$

其中:(x',y') 表示预测帧中新椭圆中心,(x,y) 是对应的前一帧椭圆中心,椭圆方差保持不变。

在嵌入过程中,先进行场景边界检测。如果某帧被检测为边界帧,则使用帧内水印方法嵌入水印;否则,使用帧间 MSER 预测确定 MSER 位置,然后嵌入水印。水印提取按类似方式进行。水印嵌入框架如图 2 所示。

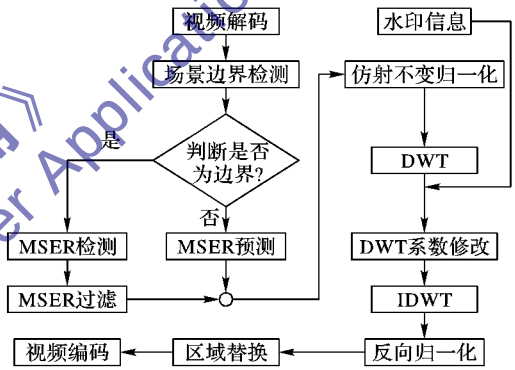


图 2　水印嵌入框架

3　实验结果与分析

3.1　鲁棒性测试

为验证本文方法的有效性,针对水印不可见性、抗格式变换鲁棒性、低比特率压缩和抗几何攻击设计本实验。实验选用 352×288 帧大小,帧率 25 帧/s,H264 编码视频 foreman 作为水印载体;水印图片大小为 64×64,面积大小边界设置为 $\tau_1 = 1000$ 和 $\tau_2 = 5000$;在最小生成树聚类中,w_r 设置为 1/4 帧宽度;水印强度设置为 $\alpha = 0.09$;场景边界系数阈值设置为 0.8。

为分析本文方法对视觉效果的影响,在视频载体的每一帧嵌入相同水印,计算每帧的峰值信噪比(Peak Signal-to-Noise Ratio, PSNR)。视频序列的 PSNR 曲线如图 3 所示。事实上,在静态图片中当 PSNR 值高于 30 dB 时,噪声对人眼不可见。从图 3 可以看出,本文方法的 PSNR 平均值为 43.76 dB,远高于 30 dB,视频可以流畅的播放,且视频水印对人眼不可见。

为测试所提算法对格式转换、低比特率压缩和常见几何变形的鲁棒性,设计攻击实验:1)JPEG 压缩;2)MPEG-4 低比特率压缩;3)中值过滤;4)行-列移除;5)拉伸;6)尺度变化;7)旋转;8)长宽比变化;9)线性变化。在每个检测到的 MSER 区域提取水印并计算归一化相关系数 z_{nc}。对所有视频帧,计算最大归一化相关系数 z_{max}、平均归一化相关系数 z_{mean} 和投票归一化相关系数 z_{voting} 用于性能评价。从表 1 可以看出,本

文方法对所有攻击行为具有很好的鲁棒性。

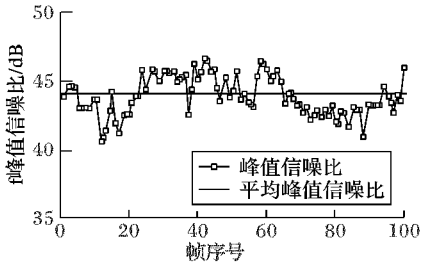


图 3 峰值信噪比曲线

表 1 攻击实验结果

攻击	参数	z_{voting}	z_{max}	z_{mean}
JPEG 压缩	90	0.862	0.774	0.703
	80	0.830	0.701	0.695
	50	0.794	0.726	0.708
MPEG-4 压缩	6 Mb/s	0.729	0.911	0.790
	2 Mb/s	0.924	0.903	0.781
中值过滤	3×3	0.861	0.723	0.699
行-列移除	行 1 列 5	0.939	0.930	0.805
	行 5 列 1	0.940	0.93	0.819
	行 17 列 5	0.939	0.930	0.819
	行 5 列 17	0.939	0.930	0.802
拉伸	x—5%,y—5%	0.939	0.924	0.803
	x—0%,y—5%	0.934	0.928	0.805
	x—1%,y—1%	0.939	0.924	0.802
旋转	5°	0.934	0.883	0.773
	10°	0.935	0.862	0.766
	20°	0.931	0.833	0.764
尺度缩放	0.8	0.929	0.869	0.752
	1.2	0.935	0.928	0.793
	1.5	0.935	0.930	0.798
长宽比	x—1.1,y—1.0	0.925	0.886	0.754
	x—1.0,y—1.1	0.929	0.920	0.749
	x—1.2,y—1.0	0.923	0.893	0.742
	x—1.0,y—1.2	0.916	0.912	0.730
线性变换	[1.007,0.010;0.010,1.012]	0.936	0.885	0.802
	[1.010,0.013;0.009,1.011]	0.914	0.869	0.762
	[1.013,0.008;0.011,1.008]	0.929	0.885	0.789

3.2 性能比较

为了和文献[16]进行对比，将文献[16]中水印方法嵌入本文框架，并分别计算最大归一化相关系数 z_{max}、平均归一化相关系数 z_{mean}。图 4～6 展示了在 foreman 视频载体进行旋转、尺度变换和 MPEG-4 压缩的实验结果。从图中可以看出，本文方法的最大归一化相关系数 z_{max} 和平均归一化相关系数 z_{mean} 均高于文献[16]中对应结果。图 4、5 表明本文方法对几何变形不敏感；图 6 表明对于所有 MPEG-4 压缩比特率，本文仍明显优于文献[16]的方法。

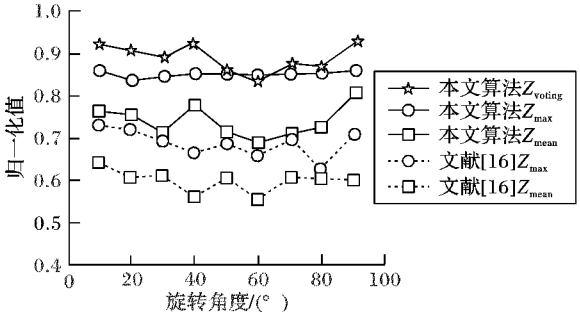


图 4 旋转对比

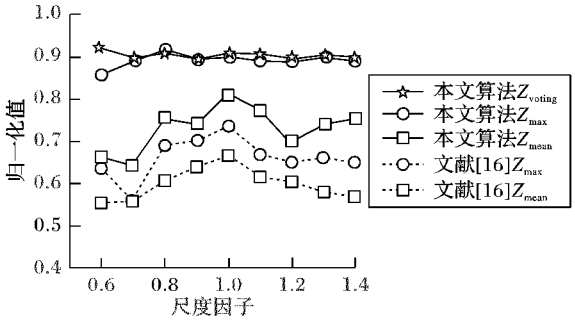


图 5 尺度对比

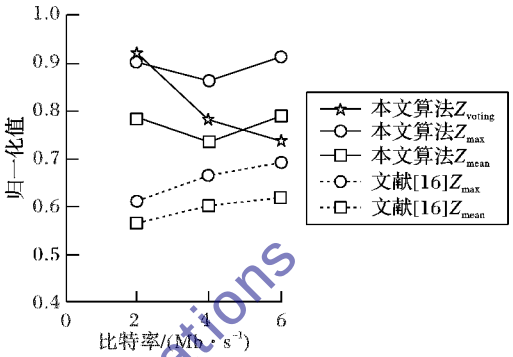


图 6 MPEG-4 压缩对比

为度量帧间水印算法对视频水印的加速效果，在 Intel Core i7- 2600 CPU @ 3.40 GHz 3.40 GHz，8 GB 内存，Ubuntu12.04 64 位系统上进行模拟实验，水印视频载体为 100 帧 foreman.h264，其中包含 4 个场景。在只是用帧内水印算法逐帧嵌入水印的条件下，水印嵌入时间为 3.04 min；结合帧间水印算法，水印嵌入时间减少到 1.27 min。可见帧间预测在消除冗余计算后显著提高了计算效率。

3.3 网关仿真

本文方法在网关设备 Huawei eSpace U1980 上仿真实验。

网关架设在中国科学院信息工程研究所信息安全国家重点实验室的教育网 CERNET 端口上。

使用网络流转包库 Libpcap 在网关设备上设计网络嗅探器。Libpcap 最初由 Network Research Group at Lawrence Berkeley Laboratory 设计开发，具备底层数据包捕获、数据包文件读写功能。对于每个试图通过网关设备由内向外传输的数据包，嗅探器解析数据包协议。如果数据包协议是多用途因特网邮件扩充协议(Multipurpose Internet Mail Extensions，MIME)、实时传输协议(Real-time Transport Protocol，RTP)或者实时流协议(Real-Time Streaming Protocol，RTSP)，说明网络流可能正在传输视频数据，可进行数据包深度检测。当检测到视频数据包时，捕获同一连接中所有数据包并重组成视频比特流。更进一步，视频比特流解码成原视频帧供水印检测。当检测到水印时，立即设置网关阻断连接中所有后续数据包的传送。在仿真实验中，局域网中有 400 台在线主机，约 1% 的外传数据包和视频数据相关。平均情况下，水印视频在传输至第 10 帧时能被成功阻断，能有效达到局域网版权保护的目的。

4 结语

本文提出了一种抗几何攻击、低比特率压缩和格式转换的快速水印方法。帧内过滤算法成功解决了嵌入区域的重叠问题；帧间场景边界检测和区域预测显著加速了水印嵌入和提取过程。实验表明本文方法能适应网关设备有限的计算能

力和光纤快速的传输能力。

参考文献:

[1] LEE M-J, LEE H-Y, LEE H-K, *et al*. Improved watermark synchronization based on local auto-correlation function [J]. Journal of Electronic Imaging, 2009, 18(2): 1 – 11.

[2] CHOI D, DO H, CHOI H, *et al*. A blind MPEG-2 video watermarking robust to camcorder recording [J]. Signal Processing, 2010, 90(4): 1327 – 1332.

[3] WOHLGEMUTH S, ECHIZEN I, SONEHARA N, *et al*. On privacy-compliant disclosure of personal data to third parties using digital watermarking[J]. Journal of Information Hiding and Multimedia Signal Processing, 2011, 2(3): 270 – 281.

[4] DEGUILLAUME F, CSURCA G, O'RUANAIDH J J, *et al*. Robust 3D DFT video watermarking [C]// Proceedings of the 1999 Conference on Security and Watermarking of Multimedia Contents, SPIE 3657. Bellingham: SPIE, 1999: 113 – 124.

[5] HARTUNG F, GIROD B. Digital watermarking of MPEG-2 coded video in the bitstream domain[C]// ICASSP 1997: Proceedings of the 1997 International Conference on Acoustic, Speech, & Signal Processing. Piscataway: IEEE, 1997, 4: 2621 – 2624.

[6] BARTOLINI F, CAPPELLINI V, CALDELLI R, *et al*. MPEG-4 video data protection for multimedia fruition[C]// VSMM 2000: Proceedings of the 6th International Conference on Virtual Systems and Multimedia. Aumsterdam: IOS Press, 2000: 35 – 40.

[7] BARNI M, BARTOLINI F, CAPPELLINI V, *et al*. A DWT-based technique for spatio-frequency masking of digital signatures [C]// Proceedings of the 1999 Conference on Security and Watermarking of Multimedia Contents, SPIE 3657. Bellingham: SPIE, 1999: 31 – 39.

[8] GOPAL K, LATHA M MADHAVI. Watermarking of digital video stream for source authentication[J]. International Journal of Computer Science Issues, 2010, 7(4): 18 – 26.

[9] LEE J-W, OH T-W, LEE M-J, *et al*. Video watermarking on overlay Layer [C]// IIH-MSP 2011: Proceedings of the 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing. Piscataway: IEEE, 2011: 85 – 88.

[10] LOWE D G. Distinctive image features from scale-invariant keypoints [J]. International Journal of Computer Vision, 2004, 60(2): 91 – 110.

[11] MATAS J, CHUM O, MARTIN U, *et al*. Robust wide baseline stereo from maximally stable extremal regions [C]// Proceeding of the 2002 British Machine Vision Conference. Edinburg: BMWA Press, 2002: 761 – 767.

[12] ZHANG X J, CAO X C, LI J J. Geometric attack resistant image watermarking based on MSER [J]. Frontiers of Computer Science, 2013, 7(1): 145 – 156.

[13] MIKOLAJCZYK K, TUYTELAARS T, SCHMID C, *et al*. A comparison of affine region detectors[J]. International Journal of Computer Vision, 2005, 65(1): 43 – 72.

[14] LIU T M, ZHANG H J, QI F H. A novel video key-frame-extraction algorithm based on perceived motion energy model [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(10): 1006 – 1013.

[15] LIU C. Beyond pixels: exploring new representations and applications for motion analysis[D]. Cambridge: Massachusetts Institute of Technology, 2009.

[16] LI L, QIAN J, PAN J. High capacity watermark embedding based on local invariant features [C]// ICME 2010: Proceedings of the 2010 Internal Conference on Multimedia and Expo. Piscataway: IEEE, 2010: 1311 – 1314.

(上接第 3521 页)

有效签名。最后 C' 输出一个伪造签名(V^*, R_1^*, R_2^*, m^*),其中 m^* 未进行 $O_{\text{Ves-Sign}}$ 询问,则 D' 可以从 C' 得到(V^*, R_1^*, R_2^*),并输出同一个签名。因此如果 C' 能成功构造一个普通签名,那么 D' 也能成功伪造一个普通签名。又因为文献[13]中定理 3.1 已经给出详细证明,说明普通签名方案在随机预言模型下是可证安全的,因此在 CDH 问题难解的前提下,D' 不可能成功伪造普通签名。所以本方案是抗恶意仲裁者攻击。

终上所述,本文提出的方案在随机预言模型下是可证安全的。

4　结语

本文结合双线性对、无证书公钥密码体制和可验证加密签名方案,提出一种高效的盲化的无证书可验证加密签名方案,该方案不仅能够间接恢复出消息,抵抗存在性伪造,而且具有更高的安全性,在实际生活中具有重要的应用价值,比如公平交换协议、电子合同等。

参考文献:

[1] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography [C]// ASIANCRYPT 2003: Proceedings of Cryptology, LNCS 2894. Berlin: Spinger-Verlag, 2003: 452 – 473.

[2] GORANTLA M C, SAXENA A. An efficient certificateless signature scheme [C]// Proceedings of the 2005 Computational Intelligence and Security, LNCS 3802. Berlin: Springer-Verlag, 2005: 110 – 116.

[3] 张振峰. 基于身份的可验证加密签名协议的安全性分析[J]. 计算机学报, 2006, 29(9): 1688 – 1693.

[4] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems [J]. Communications of the ACM, 1978, 21(2): 120 – 126.

[5] BONEH D, GENTRY C, LYNN B, *et al*. Aggregate and verifiably encrypted signatures from bilinear maps [C]// EUROCRYPT 2003: Proceedings of the Advances in Cryptology, LNCS 2656. Berlin: Springer-Verlag, 2003: 416 – 432.

[6] HESS F. Efficient identity based signature schemes based on pairing [C]// Proceedings of the 9th Annual International Workshop on Selected Areas in Cryptography, LNCS 2595. Berlin: Springer-Verlag, 2003: 310 – 324.

[7] GU C X, ZHU Y F. An ID-based verifiable encrypted signature scheme based on Hess's scheme [C]// Proceedings of the 1st SKLOIS Conference on Information Security and Cryptology, LNCS 3822. Berlin: Springer-Verlag, 2005: 42 – 52.

[8] ASOKAN N, SHOUP V, WAIDNER M. Optimistic fair exchange of digital signature (extended abstract) [C]// EUROCRYPT'98: Proceedings of the 1988 International Conference on the Theory and Application of Cryptographic Techniques, LNCS 1403. Berlin: Springer-Verlag, 1988: 591 – 606.

[9] CASTRO R, DAHAB R. Two notes on the security of certificateless signature [C]// Proceedings of Provable Security, LNCS 4784. Berlin: Springer-Verlag, 2007: 85 – 102.

[10] 周敏, 杨波, 傅贵, 等. 基于无证书的可验证加密签名方案[J]. 计算机科学, 2009, 36(8): 105 – 108.

[11] 李兵方, 茹秀娟, 张姗姗. 一个高效的可验证加密签名方案[J]. 咸阳师范学院学报, 2010, 25(2): 45 – 48.

[12] 谷利泽, 孙艳宾, 卿斯汉, 等. 新的基于 Shim 签名的可验证加密签名方案[J]. 电子与信息学报, 2011, 33(6): 1271 – 1276.

[13] SHIM K-A. An ID-based aggregate signature scheme with constant pairing computations [J]. Journal of Systems and Software, 2010, 83(10): 1873 – 1880.