基于混沌映射的视频数字水印算法

马 洁 李建福
(重庆教育学院学生处 重庆 400067) (重庆教育学院计算机科学系 重庆 400067)

摘 要 为了更好地保护视频数据的版权,提出了一种基于混沌映射的视频水印算法。在该算法中,原始视频数据被分割成等帧数的视频组,利用MPEG-7的轮廓编码计算每个视频帧的主要物体轮廓坐标点集合;然后通过傅立叶变换得到该帧轮廓点形状不变量,利用哈希的方法计算水印信号和这些不变量的有效值作为密钥之一;再对整个视频组的轮廓点进行傅立叶变换,得到其时间轴上的有效不变域,并将水印信号嵌入在这个不变域的中频部分,采用混沌技术,提高了水印的嵌入量和算法的鲁棒性。在水印提取阶段,通过对水印的多重校验,确保水印信号的可靠性。实验结果表明,该算法对大部分的视频攻击都具有良好的鲁棒性。

关键词 视频水印,混沌映射,傅立叶变换,MPEG-7

Novel Video Watermarking Algorithm Based on MPEG-7 Contour Description

MA Jie LI Jian-fu
(Student Affairs Department, Chongqing Education College, Chongqing 400067, China)
(Department of Computer Science, Chongqing Education College, Chongqing 400067, China)

Abstract For the copyright protection of digital video, a novel video watermarking algorithm based on MPEG-7 contour description was proposed. The original video is spitted into a series of frame groups, for each frame in the group, the points of contour shape are described by MPEG-7, and taking advantage of hash function to calculate the Keys between those points in the 1D-DFT transform domain and the watermark signals. Then, decomposes all those contour points of each frame in one group through 2D-DFT transform and obtains the invariant domain of the time axis and the contours, and then embeds the watermark signals into this domain to ensure the watermark reliability and robustness. And in the process of watermark extracting, it is performed multiple watermark verification to keep it accuracy. Experimental results show that the watermarked frames are indistinguishable from the original frames subjectively and the proposed video watermarking algorithm is robust against the attacks of additive Gaussian noise, frame dropping, frame averaging and lossy compression.

Keywords Video watermarking, Logistic, DFT, MPEG-7

1 引言

数字水印技术作为一种新的可以用来解决版权保护问题的有效途径,近年来已成为信息安全领域的研究热点。在各类数字水印技术中,数字视频水印技术由于其自身的研究价值和潜在的经济利益而备受各国学者的关注。根据实现过程的不同,原始视频水印算法可以分为空间域水印算法[1,2]和变换域水印算法[3-5]。由于在变换域嵌入水印,可以综合利用人类视觉特性、视频序列固有的时间和空间特性来提高水印的鲁棒性,因此这一直是人们研究的热点。Swanson等[3]利用时域小波变换和频率掩蔽特性相结合,提出了一种多分辨率的视频水印算法。Deguillaume等[4]提出将扩频水印嵌入视频序列的三维傅立叶变换的中频系数上。张立和等[5]将视频看作三维信号,隐藏水印在视频信号三维Gabor变换系数的幅度上。

本文提出了一种基于混沌映射的MPEG-7轮廓描述编码视频水印算法。在该算法中,原始视频数据被分割成等帧数的视频组,利用MPEG-7的轮廓编码计算每个视频帧的主要物体轮廓坐标点集合;使用混沌映射Logistic,生成混沌水印信号;然后通过傅立叶变换得到该帧形状轮廓的不变量,利用哈希的方法计算水印信号和这些不变量的有效值作为密钥之一;再对整个视频组的轮廓点进行傅立叶变换,得到其时间轴上的有效不变域,并将水印信号嵌入在这个不变域的中频部分,确保了水印的有效性和鲁棒性。在水印提取阶段,通过对水印的多重校验,确保水印信号的可靠性。实验结果表明,该算法对大部分的视频攻击都具有良好的鲁棒性。

2 相关知识

2.1 MPEG-7形状描述编码相关知识

1998年10月,MPEG(运动图像专家组)组织就着手制定

到稿日期:2009-10-25 返修日期:2010-01-05 本文受重庆市教委项目(No. kj091502)资助。

马 洁(1979-),女,硕士生,讲师,主要研究方向为计算机应用技术;李建福(1975-),男,博士生,讲师,主要研究方向为模式识别、计算机视觉、图像处理。

MPEG-7 标准，称为“多媒体内容描述接口”(Multimedia Content Description Interface)[6]。MPEG-7 中定义了 3 种形状描述符[7]：区域的形状(Region Shape)、轮廓的形状(Contour Shape)和 3-D 形状(Shape 3D)。使用 MPEG-7 的基于轮廓的描述符可以很好地描述轮廓所包容的形状特征，这个描述符在 CSS(Curvature Scale-Space)算法的基础上对物体的轮廓形状、轮廓上的离心率和环状值进行了良好的表征。在 CSS 算法产生的三维的 CSS 图像上，Z 坐标用来匹配和表征峰值最突出点的高度值，而在 X,Y 轴构成的水平坐标系上刻画的是原始图像所有在该轮廓上的坐标，采用 CSS 算法来描述视觉的形状轮廓特征具有相当好的效果[8]。

2.2 混沌水印信号

由于人类视觉系统对纹理具有极高的敏感性，因此所嵌入的水印信号一般不能具有纹理特性，而应该是不可预测的随机信号。本文采用 Logistic 映射[9,10]将原始水印信息映射成混沌序列。Logistic 映射的定义如下

$$x_{n+1}=\mu \cdot x_n(1-x_n) \tag{1}$$

式中，$x_n\in(0,1)$，当 $\mu\in(3.5699456,4]$时，该参数区间被称为混沌区域，是 Logistic 映射工作与混沌状态(除去某些特殊点，如临界点)，即由不同初始状态 x_0 生成的两个序列是非周期、不收敛和不相关的。

设 $W=\{w(i,j)\mid 0\leqslant i\leqslant m,0\leqslant j\leqslant n,w(i,j)\in\{0,1\}\}$为水印图像，用密钥 K 生成长度为 $m\times n$ 的 Logistic 混沌序列对 W 进行置乱，置乱后的水印信息设为 Wt，则 Wt 具有不可预测性和不相关性，从而保证了视觉对嵌入水印的不敏感性，同时，在不知道密钥 KEY 的前提下，攻击者很难恢复原始水印。

3 算法描述

3.1 水印嵌入

根据上文的介绍，在 MPEG-7 的编码层，利用形状轮廓特征描述，将原始的物体的轮廓进行重构，具体算法如图 1 所示。

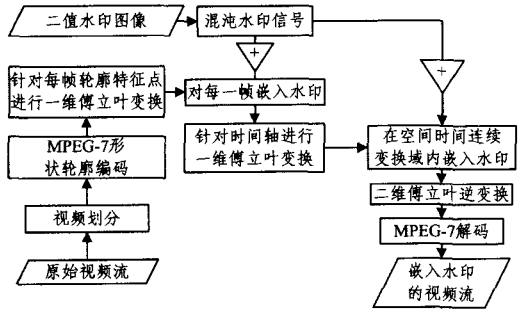


图 1 基于 MPEG-7 的水印嵌入基本过程

Step1 首先，对一个原始视频进行视频帧的划分，按 m 帧对视频序列进行划分。在这里采用 $m=15$ 作为划分标准来划分一组水印嵌入单元，记为 $G(ii)$，其中 $0<ii\leqslant\lfloor sum(frames)/m\rfloor$，在这里 $m=15$。

Step2 将该视频帧序列组 $G(ii)$进行 MPEG-7 的形状轮廓编码，即对 $G(ii)$的每个帧 $Frame(j)$，$0<j\leqslant m$，$m=15$，进行 CSS 轮廓特征点的提取，每个帧提取的 CSS 特征点坐标集合记为 $CSS_{fr}(n)$，其中 $CSS_{fr}(n)=\{(x_{ni},y_{ni})\mid(x_{ni},y_{ni})\in Frame(j)\}$，同时可以得到形状轮廓所有连续 15 帧特征点的集合 $SetCSS$，其中 $SetCSS=\{CSS_{fr}(1),CSS_{fr}(2),\cdots,CSS_{fr}(15)\}$。

Step3 通过 logistic 混沌映射将二值水印图像构造成水印序列并得到 W。对在每个视频帧 $Frame(j)$的 CSS 形状轮廓特征点坐标集合 $CSS_{fr}(n)$做一维傅立叶变换得到 $fftCSS_{fr}(n)$，选择变换域中能量最大的前 $m\times n$ 个向量 $V(m,n)$，利用 Hash 散列算法式(2)，生成包含水印信息的二值逻辑序列 Key，即

$$Key=V\oplus W \tag{2}$$

式中，Key 是由向量 V 和水印 W，通过密码学常用的 HASH 函数生成的。保存 Key，在下面提取水印时要使用到。

Step4 对于该视频帧序列组 $G(ii)$，此时 $ii=1$ 中的 CSS 形状轮廓特征点的集合按照时间轴方向进行一次一维傅立叶变换，即同时对连续 15 帧视频图像的 CSS 特征轮廓点的傅立叶变换域 $fftCSS_{fr}(n)$再进行一维傅立叶变换得到二维傅立叶变换域 $fftCSS$；在变换域 $fftCSS$ 的中频部分即 $\alpha<M_{fftCSS}(x,y)<\beta$ 中嵌入水印，在这里 α 和 β 为中频能量区间，在该区间内按照中频能量的大小选择 $m\times n$ 个位置，应用式(3)进行水印嵌入

$$M'_{fftCSS}(x,y)=M_{fftCSS}(x,y)(1+aW_i) \tag{3}$$

从而得到嵌入有水印的新的变换域 $fftCSS'$。

Step5 将嵌入有水印信号的 $fftCSS'$进行二维傅立叶逆变换，将 $fftCSS'$还原到视频中。

Step6 重复执行 Step2－Step5，直到视频序列结束，实现水印信号完全嵌入到视频。

3.2 水印提取

视频水印提取无需原视频流，同样是在视频 MPEG-7 编码过程中，利用形状轮廓特征 CSS 特征图像的描述，对嵌入水印的视频帧图像区域进行定位，从而对水印进行提取，具体过程如图 2 所示。

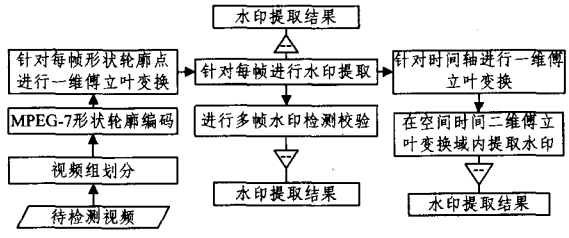


图 2 基于 MPEG-7 的水印提取基本过程

Step1 和水印嵌入的算法类似，首先，对一个原始视频进行视频帧的划分，按 m 帧对视频序列进行划分。在这里采用 $m=15$ 作为划分标准来划分一组水印嵌入单元，记为 $G(ii)$。

Step2 将该视频帧序列组，$G(ii)$进行 MPEG-7 的形状轮廓编码，即对 $G(ii)$的每个帧 $Frame(j)$，$0<j\leqslant m$，$m=15$，进行 CSS 轮廓特征点的提取，每个帧提取的 CSS 特征点坐标集合记为 $CSS_{fr}(n)$，其中 $CSS_{fr}(n)=\{(x_{ni},y_{ni})\mid(x_{ni},y_{ni})\in Frame(j)\}$，同时可以得到 CSS 形状轮廓所有连续 15 帧特征点的集合 $SetCSS$。

Step3 对在每个视频帧 F 的 CSS 形状轮廓特征点坐标集合进行一维傅立叶变换得到 $fftCSS'_{fr(n)}$，选择变换域中能量最大的前 $m\times n$ 个向量 $V'(m,n)$，使用式(4)，利用二值逻辑序列 Key 和待测傅立叶变换域中的向量 V'，提取出水印

W'

$$W'=V'\oplus Key \tag{4}$$

式中，根据在嵌入水印时生成的 Key 和 V'，利用 Hash 散列的性质就可以得到待测帧图像所含的水印信号 W'。再根据 W 和 W' 的相关程度式(5)来判别是否有水印嵌入，并将其还原成二值水印图像。

$$\mathrm{sim}(W,W')=\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(w_{ij}\times w'_{ij})}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}(w'_{ij}\times w'_{ij})}} \tag{5}$$

Step4　再对该视频帧序列组 G 中的 CSS 形状轮廓特征点的集合按照时间轴方向进行一次一维傅立叶变换，在变换域中频部分即 $\alpha<M'_{ffCSS}(x,y)<\beta$ 中，α 和 β 为中频能量区间，在该区间内按照中频能量的大小选择 $m\times n$ 个位置，应用式(6)计算是否含有水印信号。

$$S=\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(w_{ij}\times M'_{ffCSS}(i,j))}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}(M'_{ffCSS}(i,j))^2}} \tag{6}$$

Step5　同时，利用对每 m 帧图像中(此时 $m=15$)是否嵌入水印的相关程度判断，实现对水印提取的校验。当有超过 $M=\lfloor m/2\rfloor$ 帧的水印相关判别为 1 时，则该视频含有水印；否则不包含水印。即

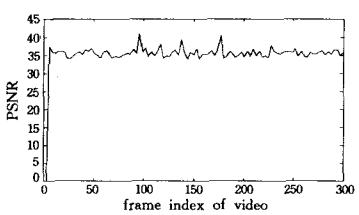
$$J=\begin{cases}1, & \text{if } \sum\mathrm{Sim}(Frame(n))>M\\ 0, & \text{else}\end{cases} \tag{7}$$

式中，$ii<n<ii+m$，$M=\lfloor m/2\rfloor$。

4　实验结果

实验采用一幅 32×32，位深度为 8 位的二值灰度图像作为水印信号。采用标准的视频测试序列 Akiyo 进行实验。图 3 分别给出了原始视频某一帧、相应的嵌入水印的视频帧以及全视频的 PSNR 值分布图。从图 3 可以看出，从人眼视觉感知而言，视频的内容并没有发生太大的变化，水印的嵌入没有对视觉产生明显的降质影响。

(a) 水印图像 (b) 原始视频帧　(c) 嵌入水印的视频帧



(d) 全视频帧的 PSNR

图 3　嵌入水印后视频对比

图 4 到图 8 分别展示了视频经过高斯噪声攻击、帧删除、帧平均、帧旋转以及 MPEG-4 压缩攻击以后的含水印的视频帧图像以及提取的水印信号的图像。

图 4 中嵌入水印的视频帧图像加入高斯噪声后进行水印的检测，平均 PSNR=25.7。从图 4 中可以看到对于这种高频的噪声，水印图像得到良好的还原，因此这种算法具有很好的抗噪声攻击的能力。

图 4　叠加高斯噪声的水印视频帧与提取的水印图像

图 5 展示视频序列经过帧删除后提取水印的图像，由于在嵌入过程中对每一帧都嵌入水印，因此一个帧的删除并不影响别的帧的水印检测。

图 5　帧删除攻击下的视频水印帧与提取的水印图像

在图 6 中将含水印的视频场景亮度分量前后两帧进行帧平均攻击，先攻击一个场景中的图像，然后依次增多，直到所有的视频场景都进行帧平均攻击。图 6(a)展示了对视频进行 50 帧平均的视频图像，PSNR=11.08。实验结果表明，帧平均攻击以后，仍能检测出水印的存在。

图 6　经过帧平均的视频水印帧与提取的水印图像

图 7 展示了对视频图像的每一帧图像进行逆时针旋转 5 度变换，再重组视频，平均 PSNR=10.18。对于视频而言，只要经过一点点的旋转变换，就会令人体视觉感知觉得疲劳，但是，这样的变换并没有改变帧图像内的物体形状轮廓，而根据 MPEG-7 形状轮廓编码生成 CSS 点的集合不会发生太大的变化，同样可以有效地测出水印。

图 7　经过旋转的视频与提取的水印图像

对原始视频进行标准的 MPEG-4 压缩，压缩比特率为 0.2 Mbps，如图 8 所示。实验表明，经过这样的 MPEG-4 压缩，视频帧图像内的物体的形状轮廓没有发生任何变化，采用本文算法同样可以很好地提取出水印信号。

图 8　经过 MPEG-4 压缩的视频与提取的水印图像

由上述实验结果可以看到，这种水印方案对于常见的基于视频的攻击，如帧旋转、帧平均、高斯噪声、MPEG 编码、帧

(下转封三)

生密钥前，通过算法说明书了解算法的弱密钥。密钥产生时，必须防止弱密钥的产生。密钥的传输有很多方式，初期的离线产品不涉及到密钥传输。ANSI X9.17 标准表述了两种密钥：密钥加密密钥和数据密钥。二期的在线产品需要通过网络传输公开密钥，采用密钥加密密钥将数据密钥加密或使用公开密钥密码术体系里的密钥传输协议来传输密钥。公开密钥密码术有一个缺陷，就是如果用户甲的公开密钥被中间人替换了，用户乙是很难发现的。所以在给用户的 Memory 卡中，一定会加上对所有密钥的校验码，就是使用单项散列函数分别对所有密钥进行运算。

PXE 动态分布存储密钥体系通常不采用软件加密（加密算法用软件实现），因其加密过程是在本机内实现的，破坏者可以对内存进行检测，对算法进行分析。如果算法被攻破，后果将是可怕的，故动态分布存储密钥体系通常使用硬件实现算法，加解密都在硬件中进行，无法追踪检测，所以更加安全。在系统中控制密钥的使用方案是：在密钥后面附加一个控制向量，用来标定密钥的使用和限制。对控制向量取单向散列运算，然后与主密钥异或，把等到的结果作为密钥对会话密钥进行加密，再把合成的加密的会话密钥跟控制向量存在一起。恢复会话密钥时，对控制向量取单向散列运算，再与主密钥异或，最后用结果进行解密。另外，密钥在使用完后，会立即从机器中销毁，决不会在磁盘上保存。用户如果想更新密钥，必须先收回旧密钥，在确认旧密钥无误的情况下，为用户提供新的密钥。旧密钥要进行销毁。

结束语 如上所述，PXE 动态分布式无盘网络数据存储安全解决方案的信息安全平台对 SIMS 进行了全面的改进，借鉴了数字签章、无盘网络等相关技术的优点。通过分布存储实现数据异地网络备份，对密钥服务器实现分布式管理，从而提高了数据存储系统整体效率并且提高了系统的安全性。基于 PXE 技术的动态分布式数据存储体系的最终用户为信息化较高的行业：证券、保险、银行、教育、交通、旅游、互联网、电信、大型零售企业、会员制行业以及医药企业的内部信息平台以及电子政务等公众网络信息服务。

数据存储安全是一个关系国家安全和社会稳定的重要问题，涉及网络技术、密码技术、信息安全技术、应用数学、信息论等多种学科。为了保证信息安全的可靠性，开发拥有独立知识产权的安全存储技术系列产品势在必行。本文提供了一种提高网络数据安全的解决方案，方案采用最新的动态分布式存储技术及 PXE 无盘网络技术，将所有网络数据及操作系统集中存放在单个服务器上，从而实现数据的集中存储与集中管理，从网络边界安全、数据传输安全、数据存储安全 3 个方面降低各种数据泄漏风险，从技术上解决可能存在的管理漏洞，为如何有效保证网络数据安全、真正实现数据的安全可靠提供参考。随着成果的普及与行业应用，其经济价值前景可观。

参 考 文 献

[1] Sinha P K. Distributed Operating Systems [M]. IEEE Computer Society Press, 2000

[2] Garrett P. Making, Breaking Codes [M]. Prentice-Hall, 2001

[3] 闵军，等. 最新 PXE\RPL 无盘站和终端[M]. 北京：清华大学出版社，2003

[4] 黄冠利，等. 动态分布式无盘网络数据安全解决方案设计与改进[C]//2009 国际信息技术与应用论坛. 2009

[5] 斯托林斯. 密码学与网络安全[M]. 北京：清华大学出版社，2002

[6] 黄冠利，胡亦，等. 基于 PKI 体系的数字签章安全系统设计[J]. 计算机安全，2008，9：78-80

[7] 钟阿林，许方恒，董方敏. 一种理想的数据库加密方案[J]. 重庆邮电大学学报：自然科学版，2007，19(6)：131-133

（上接第 289 页）

删除等具有较好的鲁棒性。

结束语 经过对视频序列的多次实验测试，本文提出的基于 MPEG-7 形状轮廓编码的视频水印算法，具有以下特点：将视频信号分成一系列的视频组，对视频组中的帧进行 MPEG-7 形状轮廓编码得到一些局部的点，并将这些点作为各种变换域的区域以及水印嵌入的区域，从而避免了全局的计算，降低了算法的运算复杂度；利用 Hash 的思想实现部分水印信号的无损嵌入，在保证不可见性的同时，使水印具有较好的鲁棒性；采用混沌技术，提高了水印的嵌入量和算法的鲁棒性；水印提取时不需要原始视频信号，并可以进行多重水印的校验。

参 考 文 献

[1] Hartung F, Birod B. Watermarking of uncompressed and compressed video[J]. Signal Processing, Special Issue on Copyright Protection and Access Control for Multimedia Services, 1998, 66(3): 283-301

[2] 梁华庆，王磊，双凯，等. 一种在原始视频帧中嵌入的鲁棒的数字水印[J]. 电子与信息学报，2003，25(9)：1281-1284

[3] SwansonM D, Zhu B, Tewfik A H. Multiresolution scene based video watermarking using perceptual models[J]. IEEE Journal on Selected Areas in Communications, 1998, 16(4): 540-550

[4] Deguillarme F, Csurka G, Ruanaidh J O, et al. Robust 3D DFT video watermarking[C]// Proceedings of SPIE. Security and Watermarking of Multimedia Contents. San Jose, California, 1999, 3657: 113-124

[5] 张立和，伍宏涛，胡昌利. 基于三维 Gabor 变换的视频水印算法[J]. 软件学报，2004，15(8)：1252-1258

[6] Martinez J. MPEG-7 Overview(Versions 10) [S]. 150/IECJTCI/SC29/WGl. http://www. chiariglione. org/mpeg/standards/mpeg-7/mpeg-7. htm, 2002

[7] Pereira F, Koenen R. MPEG-7: A standard for multimedia content description[J]. International Journal of Image and Graphies, 2001, 3(1): 527-546

[8] Mokhtarian F, Mackworth A K. A Theory of Multiscale, Curvature-Based Shape Representation for Planar Curves[J]. IEEE transactions on pattern analysis and machine intelligence, 1992, 14(8): 789-805

[9] Lin H B. Staring with parabolas: an introduction to chaotic dynamics[M]. Scientific and Technological Education Publishing House, Shanghai, 1993

[10] 张欣，杨德刚. 一种基于混沌映射的图像加密方法[J]. 重庆工学院学报：自然科学版，2009，23(10)：104-107