基于混沌映射的半脆弱图像水印算法

李东勤[1],林克正[2]
(1.安徽财经大学 信息工程学院,安徽 蚌埠 233041;
2.哈尔滨理工大学 计算机科学与技术学院,黑龙江 哈尔滨 150080)

摘 要:水印的安全性、抗常规图像处理的鲁棒性和篡改检测能力的矛盾、计算复杂度等是现有基于半脆弱水印技术的图像认证算法需克服的主要问题。提出了一种基于混沌映射的自适应半脆弱水印算法,选取图像小波变换的低频信息作为图像特征并利用混沌映射对初值的敏感性产生两种水印,采用块均值量化调制小波系数的方法完成水印信息的嵌入。实验结果表明,该算法具有一定的鲁棒性,可将JPEG压缩等常规信号处理与恶意篡改相区分,并能准确定位篡改区域。

关键词:图像认证;半脆弱水印;混沌映射;离散小波变换
中图分类号:TP391 **文献标识码**:A **文章编号**:1673-629X(2008)11-0156-03

Semi-fragile Image Watermarking Algorithm Based on Chaotic Map

LI Dong-qin[1], LIN Ke-zheng[2]
(1. College of Information Engineering, Anhui University of Finance & Economics, Bengbu 233041, China;
2. College of Computer Science and Technology, Harbin Univ. of Science and Tech., Harbin 150080, China)

Abstract: How to ensure watermark security, how to cancel out the contradiction between robustness to common image processing and fragility to malicious tamper, and how to reduce the computational complexity are the main issues to be solved in the existing image authentication algorithms based on semi-fragile watermarking technique. Presents a new chaos-based adaptive semi-fragile watermarking algorithm which extracts features from the low frequency domain and uses the high sensitivity on initial value of chaotic mapping to generate two watermarks, then embeds them back into the image by mean-quantization and modulating the wavelet coefficients. Experimental results show that the algorithm can identify intentional content modification and incidental tampering and also indicate the location where a modification takes place.

Key words: image authentication; semi-fragile watermark; chaotic map; discrete wavelet transform

0 引 言

多媒体内容的完整性认证,尤其是图像的完整性验证,近几年来随着网络技术的发展已引起了人们的高度重视,其解决方案主要集中在脆弱水印技术上。根据水印识别篡改的能力可将脆弱水印划分为完全脆弱水印和半脆弱水印:完全脆弱水印能够检测出任何对图像像素值改变的操作或图像完整性的破坏操作,即图像中有一个比特的信息被改变,认证都将无法通过[1,2];半脆弱水印则可将常规信号处理与恶意篡改区别对待,是在一定程度上的完整性检验。半脆弱水印由于同时具有脆弱水印和鲁棒性水印两种功能,近年来受到了越来越多水印研究者的关注[3~6]。

文中提出了一种基于混沌映射的自适应半脆弱水印算法,利用图像特征产生两种水印信息,并采用块均值量化调制小波系数的方法将其嵌入到图像小波变换的中频区域。水印的产生和嵌入都基于宿主图像本身,因此认证时无需原始图像和水印的参与,实现了盲检测功能。

收稿日期:2008-02-28
基金项目:黑龙江省科学技术研究项目(10051054);安徽财经大学信息工程学院青年教师资助项目(xgky2008004)
作者简介:李东勤(1981-),女,江苏盐城人,讲师,硕士,研究方向为信息安全、数字图像处理、数字水印技术;林克正,博士,教授,研究方向为图像处理与计算机视觉、多媒体信息编码、数字水印等。

1 基于混沌映射的半脆弱水印算法

1.1 混沌映射

Logistic映射是一类非常简单却被广泛研究的混沌动力系统,可用非线性差分方程来描述:

$$z_{i+1} = \lambda z_i(1 - z_i)\ \lambda \in [0,4]\ i = 0,1,\cdots \quad (1)$$

给定初值 $z_0 \in (0,1)$ 和迭代次数 $n-1$,就可得到长度为 n 的混沌序列 $Z^n = \{z_1, z_2, z_3, \cdots, z_n, z_i \in (0,$

1)}。根据初值 z_0 和控制参数 λ 的不同，可以生成不同的序列。文献[7]取 $z_0 = 0.25$，而文献[8]取 $z_0 = 0.75$，事实上这两个初值没有区别，因为它们之和为 1。因此，只需考虑初值在(0, 0.5) 或(0.5, 1) 范围内即可。

定义如下量化函数：

$$V = Q(Z^n, d) \tag{2}$$

其中，$V = \{v_1, v_2, v_3, \cdots, v_d \mid v_i \in \{0,1\}\}$，$d$ 表示返回{0,1} 比特的个数。

1.2 水印信息的产生

对任意一幅 $m \times n$ 的图像 I，先对其进行 3 级 Haar 小波变换，得到编号为 $LH_1, HL_1, HH_1, LH_2, HL_2, HH_2, LL_3, LH_3, HL_3, HH_3$ 的各个子带，选取 LL_3 为特征子带生成水印信息。该子带包含了图像的主要能量，同时对常规图像操作(JPEG 压缩、平滑滤波等) 具有一定的鲁棒性。选定阈值

$$a = \mathrm{Max}(LL_3)/3 \tag{3}$$

定义二值水印信息 $W_L(i,j)$：

$$W_L(i,j)\begin{cases}1 & LL_3(i,j) \geqslant a \\ 0 & LL_3(i,j) < a\end{cases} \tag{4}$$

$$0 \leqslant i \leqslant (m/8) - 1, 0 \leqslant j \leqslant (n/8) - 1$$

设映射 C_0 满足 $C_0(LL_3(i,j)) \in (0,0.5)$，混沌迭代初值 $z_{i,j}(0)$ 为：

$$z_{i,j}(0) = C_0(LL_3(i,j)) \tag{5}$$

水印信息 $W_A, W_A(i,j) \in \{0,1\}$ 由式(6) 产生：

$$W_A(i,j) = Q(Z^n_{i,j}, 1) \tag{6}$$

这样，就得到了大小为 $(m/8) \times (n/8)$ 的待嵌入水印信息 W_L 和 W_A。

1.3 水印的嵌入

灰度值的平均值(期望值) 是图像的一个统计特征，对常规图像处理而言，块均值的变化范围比较小，主要集中在区间[0, 2] 内，说明图像块均值比较稳定。因此，采用块均值量化调制小波系数的方法，将水印信息嵌入到小波变换的中频子带 LH_2、HL_2 和 HH_2 内，具体步骤如下：

1)将 LH_2、HL_2 和 HH_2 划分成大小为 2×2 互不重叠的图像子块(每个图像子块内仅嵌入 1 个比特的水印信息)。

2)利用密钥 K 随机选择要嵌入水印信息的图像子块 X_i，计算 X_i 所含元素(系数) 的均值 $\bar{x}$，然后用 q 对其进行量化，根据量化结果修改图像子块内元素值，以完成水印信息的嵌入。如果 $\mathrm{mod}(\bar{x}_q, 2) = w_i$，小波系数不变，否则改变小波系数为：

$$x'_i = x_i + \bar{x}_q - \bar{x} + q \tag{7}$$

其中，$x_i, x'_i (i = 1,2,3,4)$ 分别为嵌入水印前和后的小波系数，w_i 为待嵌入的水印信息，q 为量化步长，且

$$\bar{x} = \frac{1}{4}\sum_{i=1}^{4} x_i \tag{8}$$

$$\bar{x}_q = \mathrm{floor}(\bar{x}/q) \tag{9}$$

3) 用含有水印信息的小波系数 x'_i 代替 x_i 并结合未修改的小波系数进行 3 级逆 Haar 小波变换，便可得到嵌入水印后的图像 I_w。

1.4 水印提取及篡改认证

1)认证水印的提取。

在水印提取前，首先利用待测图像生成参考水印信息，并参与水印的双重认证工作。待测图像参考水印生成过程与原始图像水印生成步骤一致，将待测图像进行特征提取、混沌映射后，得到参考水印 W'_L(对应于 W_L) 和 W'_A(对应于 W_A)。

得到参考水印后，进一步在待测图像中提取认证水印。水印的提取过程是水印嵌入过程的逆步骤。对待测图像进行 3 级 Haar 小波变换后，提取中频子带 LH_2、HL_2 和 HH_2，并对其进行互不相交的分割，分块大小为 2×2。利用密钥 K 选择嵌入了水印信息的图像子块 $\hat{X}_i$，计算其所含元素的均值 $\hat{\bar{x}}$ 并量化，分别提取水印信息 $\hat{W}'_L$ 和 $\hat{W}'_A$，见式(10) 和(11)：

$$\hat{\bar{x}} = \frac{1}{4}\sum_{i=1}^{4} \hat{x}_i \tag{10}$$

$$\hat{w}_i = \mathrm{mod}(\mathrm{round}(\hat{\bar{x}}/q), 2) \tag{11}$$

其中，$\hat{w}_i$ 为提取的水印信息比特，q 为量化参数。

2) 篡改认证。

在文中，定义两个认证矩阵 $\boldsymbol{D}_L$ 和 $\boldsymbol{D}_A$ 以及块篡改检测函数 r_L 和 r_A。

$$\boldsymbol{D}_L = \hat{W}'_L \oplus W'_L \tag{12}$$

$$\boldsymbol{D}_A = \hat{W}'_A \oplus W'_A \tag{13}$$

$$r_L = \frac{64\sum_{i=1}^{m/8}\sum_{j=1}^{n/8} \boldsymbol{D}_L}{m \times n} \tag{14}$$

$$r_A = \frac{64\sum_{i=1}^{m/8}\sum_{j=1}^{n/8} \boldsymbol{D}_A}{m \times n} \tag{15}$$

为了反映篡改的程度和强度，引入检测阈值 τ，定义如下判断规则：

(1) $r_L = r_A = 0$ 图像未经任何处理。

(2) $r_L < \tau$ and $r_A < \tau$ 图像已经处理但无篡改。

(3) $r_L < \tau$ and $r_A > \tau$ 图像已被篡改。

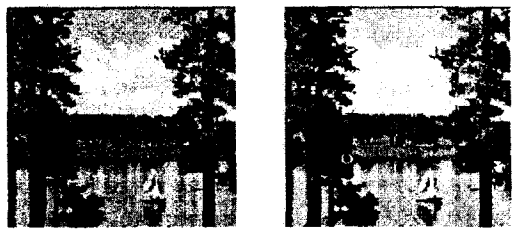
(4) $r_L > \tau$ and $r_A > \tau$ 图像已被严重篡改。

检测阈值 τ 的选取可以根据用户对图像质量的要求而设定，如果要求越高，则 τ 的取值就越小。

2 实验结果和分析

实验以 256×256×8bit 标准灰度图像 careman 和 lake 作为实验图像来测试文中算法的性能。检测阈值 τ 定为 0.45，量化因子 $q = 12$，公钥 $K(i)$ 是一伪随机序列，Logistic 映射的控制参数 $\lambda = 3.93$，迭代次数 $n = 29$。水印信息的嵌入如图 1 所示，其中 a)和 c)分别为原始图像 careman 和 lake，b)和 d)为含水印图像。测得峰值信噪比(PSNR)分别为 40.16dB 和 41.25dB。PSNR 值和主观视觉效果都证实了文中算法实现的水印具有不可感知性，隐藏效果好。

a) 原始 careman 图像　b) 含水印图像



c) 原始 lake 图像　d) 含水印图像

图 1 水印信息的嵌入

2.1 对常规图像处理的鲁棒性

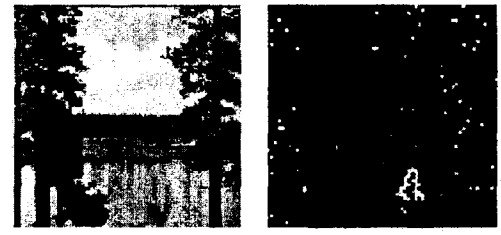
为了测试算法的鲁棒性，对含水印 careman 图像(图 1 b)分别进行了 JPEG 压缩、叠加噪声、平滑滤波等常规信号处理，并计算块篡改检测率 r_L 和 r_A，表 1 给出了部分测试结果。从表中可以看出，所有的 r_L 和 r_A 都小于给定的阈值 $\tau(\tau = 0.45)$，表明图像内容没有发生改变。

表 1 常规图像处理后的检测结果

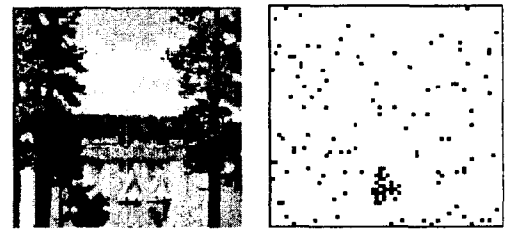
攻击方式	参数	r_L	r_A
JPEG	压缩比为 90	0.09	0.09
	压缩比为 70	0.16	0.16
	压缩比为 40	0.38	0.37
JPEG2000	压缩比率为 0.70	0.10	0.11
	压缩比率为 0.60	0.17	0.17
	压缩比率为 0.30	0.32	0.33
均值滤波	均值滤波 3×3	0.08	0.08
中值滤波	中值滤波 3×3	0.10	0.11
椒盐噪声	椒盐噪声 1%	0.12	0.12

2.2 对恶意篡改的脆弱性

为了测试算法对恶意篡改的脆弱性和对篡改区域的定位能力，对含水印的 lake 图像(图 1 d)先作 70% JPEG 压缩后，再进行局部修改，具体方法如下：(1)将其中的小船移走(如图 2 a)所示)，图 2 b)为其对应的认证矩阵 $\boldsymbol{D}_A$，其中块篡改检测率 $r_L = 0.138$，$r_A = 0.531$，表明图像已被篡改；(2) 添加一个小船(如图 2 c)所示)，图 2 d) 为其对应的认证矩阵 $\boldsymbol{D}_A$，块篡改检测率 $r_L = 0.135$，$r_A = 0.525$，表明图像内容也已发生了改变。实验结果显示，该算法对图像篡改具有很好的检测和定位能力。



a) 篡改图像　b) 检测结果



c) 篡改图像　d) 检测结果

图 2 恶意篡改的检测结果

3 结束语

提出了一种基于混沌映射和小波变换的半脆弱水印算法，主要介绍了水印的嵌入和提取策略。首先选取小波变换低频信息作为图像特征产生两种水印：一种用于检测对图像内容的篡改，一种用于定位篡改区域；然后采用块均值量化调制小波系数的方法将其嵌入到中频区域。为增强水印的安全性和提高篡改检测的准确性，引入了混沌置乱算法。水印的产生和嵌入都基于宿主图像本身，因此认证时无需原始图像和水印的参与，实现了盲检测功能。实验表明本算法具有一定的鲁棒性，可将 JPEG 压缩等常规信号操作与恶意篡改相区分，并能准确定位篡改区域。

参考文献：

[1] 丁 科，何 晨，王宏霞. 一种定位精确的混沌脆弱数字水印技术[J]. 电子学报，2004，32(6)：1009－1012.

[2] 甘艳芬，郑胜林，潘保昌. 基于超混沌加密的脆弱数字水印技术[J]. 计算机技术与发展，2006，16(10)：145－148.

[3] 李赵红，侯建军，宋 伟. 混沌映射的半脆弱图像数字水印算法[J]. 北京交通大学学报，2007，31(2)：52－56.

(下转第 175 页)

Defragment。Rts 帧为控制帧，无需重组，直接以消息 RxIndicate 的形式发送给 Rx_Coordination。Rx_Coordination 在 RxC_Idle 状态下收到 RxIndicate 后，检查帧类型为 rts 帧，则生成一个用于交换的 cts 帧，按协议规定，需等待一个短帧帧间隔后向 Data_Pump 发送 TxRequest，然后进入 Wait_TxDone，即等待 cts 帧发送完成的状态。

```
ValidateMpdu is running!
PHY has transmited PhyRxEndindicationM to ValidateMpdu!
ValidateMpdu is running!
ValidateMpdu has received PhyRxEndindication from PHY!
ValidateMpdu has received rts Frame,reset Trts!
ValidateMpdu has transmit UseDifs to ChannelState!
channelstate has received UseDifs!
ValidateMpdu has transmit RxMpdu to FilterMpdu!
FilterMpdu has transmit PsIndicate(sta_active)!
Mlme has received PsIndicateM message ,it's powermanagemode is 0
The macaddr is :6 7 8 9 a b
FilterMpdu has transmit RxMpdu to Defragment!
The type of the Frame is control or management,no need to defrag!
RxIndicate is Transmitted!
RxC has received RxIndicate
pdu is rts
RxC is running!
Wait_Sifs!
post TxRequest to DataPump
Data_Pump has received TxRequest message !
c4 0 63 0 6 7 8 9 a b
Data_Pump has transmitted TxConfirm!
DataPumptask is running!
RxC is running!
Wait_TxDone!
```

图 4　接收运行过程图

如图 5，收到 TxConfirm 后，Rx_Coordination 模块重又跳转到 Rx_Coordination 状态，任务挂起，直到队列中有可用消息。PHY 层通知 MAC 层信道空闲，Channel_State 模块跳转到 Wait_Ifs 状态，一个帧间间隔后，向 Data_Pump 发送消息 Idle，之后跳转到 noCs_noNav 状态，并每隔一个时隙时间，就向 Data_Pump 发送消息 Slot，以便发送模块完成退避规程[7]。

通过对测试结果分析证明接收 rts 帧后的处理和标准的流程要求一致，另对输入 beacon 帧和数据帧的测试结果也与标准一致，此处不再给出截图。

4　结束语

在 Windows 操作系统中，利用移植到 VC++6.0 上的 μC/OS-II，实现了 MAC 层接收模块的基本功能，即数据功能和信道状态控制，并通过了调试。IEEE802.11 无线局域网以其灵活性和可移动性，作为宽带有线接入网的延伸和补充，有极好的应用前景。

```
Wait_TxDone!
RxC has received TxConfirm
RxC is running!
RxC_Idle!
Defragment is running!
DefragState is DefragIdle!
FilterMpdu is running!
PHY has transmitted PhyCcaindicationM(idle) to ChannelState!
PHY is running!
channelstate has received PhyCcaindication(idle)!
channelstate is running!
MediaState is Wait_Ifs!
ValidateMpdu is running!
Tifs or noTifs!
Idle!
Data_Pump has received Idle!
DataPumptask is running!
channelstate is running!
MediaState is NoCs_NoNav!
Slot!
Data_Pump has received Slot!
DataPumptask is running!
channelstate is running!
MediaState is NoCs_NoNav!
Slot!
```

图 5　接收处理完成图

参考文献：

[1] Brenner P. A Technical Tutorial on the IEEE 802.11 Protocol [R]. [s. l.]: Breezecom Wireless Communications, 1997: 3-22.

[2] LAN MAN Standards Committee of the IEEE Computer Society. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications [S]. IEEE-SA Standards Board. ANSI/IEEE Std 802.11, 1999.

[3] 阮加勇，黄本雄. IEEE 802.11 DCF 延迟性能分析[J]. 华中科技大学学报：自然科学版，2006，34(4)：27-29.

[4] 金　纯，陈林星，杨吉云. IEEE 802.11 无线局域网[M]. 北京：电子工业出版社，2004.

[5] Labrosse J J. 嵌入式实时操作系统 uCOS-II[M]. 第 2 版. 邵贝贝，等译. 北京：北京航空航天大学出版社，2006.

[6] Kernighan B W, Ritchie D M. C 程序设计语言[M]. 第 2 版. 徐宝文，李　志译. 北京：机械工业出版社，2004.

[7] 宫洪运，徐金娣，李德敏. 无线局域网 802.11 协议的分析及其 MAC 层实现[J]. 东华大学学报：自然科学版，2004，30(4)：32-36.

(上接第 158 页)

[4] 王艳辉，王相海. 基于提升方案小波的半脆弱水印图像认证算法[J]. 计算机工程与设计，2007，28(20)：4955-4958.

[5] Maeno K, Sun Q, Chang S F. New Semi-Fragile Image Authentication Watermarking Techniques Using Random Bias and Nonuniform Quantization[J]. IEEE Transactions on Multimediam, 2006, 8(1): 32-45.

[6] 王向阳，陈利科. 一种新的自适应半脆弱水印算法[J]. 自动化学报，2007，33(4)：361-366.

[7] Yen Jui-Cheng. Watermark Embedded in Permuted Domain [J]. IEEE Trans. Electronics Letters, 2001, 37(2): 80-81.

[8] Yen Jui-Cheng. Watermarks embedded in the permuted image[C]// Proc of 2001 IEEE International Conference on Circuits and Systems: Symposium. Sydney, NSW: IEEE, 2001: 53-56.