文章编号:1673-9469(2010)01-0109-04

一种用于图像篡改定位的半脆弱数字水印算法

潘 伟,庞彦军
(河北工程大学 理学院,河北 邯郸 056038)

摘要:设计并实现了一种用于数字图像内容认证的半脆弱水印方案。算法中,图像块的水印选择 Logistic 映射作为混沌系统从该图像块本身产生一系列混沌序列,作用于水印的嵌入;每个图像块产生的水印按照 Torus,自同构映射嵌入另一个映射块的 LSB(Least Significant Bit),对应关系通过密钥来确定,这样建立起图像块之间的相关性;利用混沌对初值极端敏感性的特点,能够定位检测对加入水印图像的篡改,且水印提取不需要原始图像。实验结果表明,嵌入水印后的图像的视觉好;算法具有图像内容局部篡改检测的有效性、敏感性以及良好的篡改定位能力。

关键词:半脆弱水印;混沌;环面自同构映射;图像认证
中图分类号: TP309 **文献标识码**:A

Semi-fragile digital watermarking algorithm for image tamper localization

PAN Wei, PANG Yan-jun
(College of Science, Hebei University of Engineering, Hebei Handan 056038, China)

Abstract: A new semi-fragile watermarking algorithm for image content authentication based on chaotic mapping is presented. Chaotic sequence generated from the block itself by means of Logistic mapping is used to generate watermarking embedding; then the generated watermarking information is embedded into LSB plane of another image block with Torus Automorphism mapping, which the corresponding relation is determined by the secret key to establish the correlation among the image blocks. The results show that the method could localize the tampered watermarked image by using the high sensitivity on initial value of the chaotic mapping without host image in watermark extraction. Moreover, watermarked images obtained have good subjective quality, precise localization of tampered areas, and the algorithm is simple and safe.

Key words: semi-fragile digital watermark; chaos; torus automorphism mapping; image authentication

数字化技术在为信息处理、复制、传播以及销售提供便利的同时,也随之带来了潜在的安全隐患。数字水印技术通过在数据中嵌入认证信息,能够有效地识别数据所有者并验证数据的真伪,是保证数字媒体真实性与完整性的一种重要手段。文献[1-3]提出基于小波变换的半脆弱水印算法,水印通过量化小波系数嵌入,这些算法能够抵抗一定程度的 JPEG 压缩,但不能将局部很少量像素修改区分开来;文献[4]提出了具有篡改定位能力分级脆弱水印,该算法由于不同级分享同一个 LSB 平面,导致嵌入内容互相包含。

本文在分析现有的定位型算法基础上提出并实现了基于混沌映射的数字水印算法。通过对实验结果的分析,证明该算法保证嵌入水印后图像具有良好的视觉质量;很高的图像篡改定位能力具有较好的实用性。

1 基于混沌映射的半脆弱数字水印算法

1.1 预处理

假设原始图像 X 为 256 灰度级,大小为 $M \times M$,其中 M 为 2 的倍数。对图像进行 2×2 分块,通过 Torus 自同构变换得到块映射序列 $A \rightarrow B \rightarrow C \rightarrow \cdots \rightarrow A$,并进行水印嵌入,序列中每个字母代表

收稿日期:2009-11-16
基金项目:国家自然科学基金项目(60474019);河北省自然科学基金项目(F2005000482) 特约专稿
作者简介:潘 伟(1982-),女,助教,硕士,从事数字图像处理方面的研究。

一个独立的块,即由块 A 生成的认证水印嵌入块 B 中,块 B 的认证水印嵌入到块 C 中,依次类推,以提高算法的安全性。

利用 Torus 自同构映射一维变换公式计算一一映射序列

$$n=[f(m)=(k\times m)\bmod N]+1 \quad (1)$$

其中 $m,n(\in[1,N])$—块序号;$k\in[0,N-1]$—素数,属于私有密钥;$N(\in Z-\{0\})$—图像块总数。

块映射序列生成算法如下:

1)将大小为 $M\times M$ 的原始图像划分为互不重叠的 2×2 图像块,则分块总数为 $N=\frac{M}{2}\times\frac{M}{2}$。

2)按照从左到右从上到下的顺序,对所有分块进行编号,记为 $m,m=1,2,\cdots,N$。

3)任意确定私有密钥 k 值($k\in[0,N-1]$,且为素数)。

4)根据式(1)计算 n,即块 m 的 Toru 自同构映射块。

5)记录所有的 m 和 n。当密钥 k 为素数时,m 和 n 满足一一映射关系,否则为多对一映射关系。表 1 给出了当 $N=16$,$k=7$ 和 $N=16$,$k=8$ 时,m 和 n 映射关系。由表可以发现,当密钥 k 不为素数时,自同构映射最小周期小于 N,为多对一映射关系。

1.2 混沌映射

混沌是非线性系统方程在某些特定条件下的解,其随机输出由一个确定方程(组)决定。考虑一维离散混沌映射

$$f:U\to U,U\in R \qquad z(n+1)=f(\lambda,z(n)),\lambda\in R,z(n)\in U \quad (2)$$

其中,n—迭代次数;λ—控制系统混沌行为的参数。

通过若干次迭代后可以用一个量化函数实现映射:$z(n)\to\{0,1\}$。给定混沌映射两个略微不同的初始值,经过多次迭代后将得到两个截然不同的伪随机序列,这种混沌系统对初值的极端敏感性可以使 $z(n)\to\{0,1\}$ 得映射结果具有高度的随机性[6,7]。一个著名的混沌系统就是 Logistic 系统

$$z(n+1)=1-2z(n)^2,z(n)\in[-1,1] \quad (3)$$

1.3 水印算法设计

具体实现流程如图 1 所示。将原图像分块后的子块其像素灰度值的平均值经量化操作后映射为混沌初值,经若干次混沌映射生成水印比特;把生成的水印比特嵌入到利用环面自同构映射找到与此相对应的图像子块的像素灰度值的 LSB 平面。

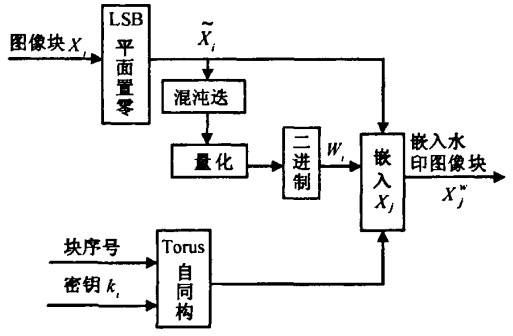


图1 水印嵌入算法框图

Fig. 1 The algorithm of watermarking embedding

水印的产生及嵌入过程如下:

1)将 X 等分为 $N\times N$ 互不重叠的子图像块 X_i 后,使每块 LSB 平面置零得到 $\tilde{X}_i$。

2)求出子块 $\tilde{X}_i$ 的像素值的归一化到[0,1]范围内,得到归一化的标准差并作量化处理,得到混沌初值 $z(0)$。

3)利用式(3),从初值 $z(0)$ 开始迭代,每迭代 1 次得到一个混沌序列值,取其绝对值为混沌终值 $z(n)$。

4)计算出量化序列 Q_{X_i},得到嵌入的水印 $W_i=(w_{i3},w_{i2},w_{i1},w_{i0})$,其中 $w_{ij}(j=0,1,2,3)$满足

表 1 $N=16$ 和 $k=7,8$ 时,m 和 n 映射关系

Tab. 1 Mapping m of and n, when $N=16$ and $k=7,8$

	N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$k=7$	m	8	15	6	13	4	11	2	9	16	7	14	5	12	3	10	1
$k=8$	n	9	1	9	1	9	1	9	1	9	1	9	1	9	1	9	1

$Q_{X_i} = 8w_{i3} + 4w_{i2} + 2w_{i1} + w_{i0}$

5)根据式(1)，利用密钥 k 确定出序号 i 的对应序号 j，把 $\tilde{X}_i$ 生成的水印 W_i 嵌入到 X_j 的 LSB，得到嵌入水印的图像块 X_j^w。至此完成了子块 X_i 的水印嵌入，全部子块处理完毕后得到水印图像 X_w。

1.4 水印检测与图像内容认证

水印检测的过程同时也是对图像内容进行认证的过程。参照水印的嵌入过程 1－4,利用密钥 k 确定子块 $\tilde{X}_W^i$ 要嵌入的位置 $\tilde{X}_W^i(i,j=1,2\cdots N)$，比较 $\tilde{X}_W^i$ 生成的量化序列 $Q_{X_W^i}$ 与映射块 $\tilde{X}_W^i$ 提取 LSB 得到的 Q_j^* 以此来判断图像块是否通过验证，相异则判断为被篡改。定义篡改矩阵 T 以对图像的篡改位置作出标记

$$T_{(i,j)} = \begin{cases} 1 & X_{(i,j)}\text{被篡改} \\ 0 & X_{(i,j)}\text{未被篡改} \end{cases}$$

其中,矩阵 T 中为 1 的点表示原始图像中被篡改的点。

为降低虚警概率引入阈值 $L(L \le 8)$,当图像块 X_i 被标注为已篡改,而其周围被标注为篡改的图像块的个数小于 L 时,则认为图像块 X_i 通过认证。即在含水印图像实际被篡改区域的部分图像块中,若某篡改图像块相邻的最近的 8 个图像块(如图 2 所示)不全被视为篡改区,则该图像块为虚警块,通过认证。

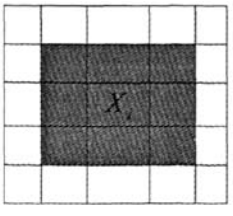


图2 图像块 X_i 及其相邻图像块(包围中心图像块的深色区域所示)

Fig. 2 The image block X_i and adjacent blocks (the shadow areas)

2 案例分析

被测图像为的灰度 Lena, Peppers 和 Rice 图像,有 256 个灰度级,图像质量由峰值信噪比(*PSNR*)来评测。

2.1 不可见性分析

为了衡量嵌入水印的图像质量的好坏,使用数字水印技术中常用的峰值信噪比 *PSNR*,其定义为

$$PSNR = 10 \times \lg\left(\frac{255^2}{\frac{1}{N \times N}\sum_{i=1}^{N}\sum_{j=1}^{N}(X_w(i,j) - X(i,j))^2}\right) \quad (4)$$

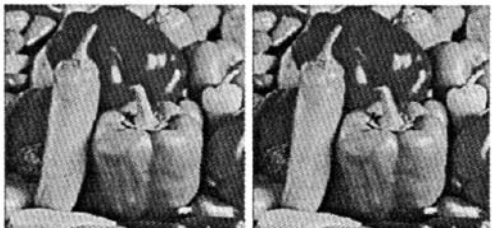
把水印信号只嵌入到图像的 LSB 平面,从理论上分析,当出现最不理想的情况即原图像中所有 LSB 变化时,由式(4)得

$$PSNR_{worst} = 10 \times \lg\frac{255^2}{1^2} = 48.13$$

根据任意性把 0 判成 1 或 1 判成 0 是等可能的,由此得到

$$PSNR = 10 \times \lg\frac{255^2}{\frac{1}{2} \times 1^2} = 51.1411$$

图 3 给出 Peppers 嵌入水印前后的图像,由式(4)计算得出的 $PSNR_{WORST}$ 与原始图像的 *PSNR* 均满足数字水印对不可察觉性的要求,取值和主观视觉效果都证实了本算法实现的水印具有不可感知性,透明性效果好。



(a)原始图像　　(b)嵌入水印后的图像

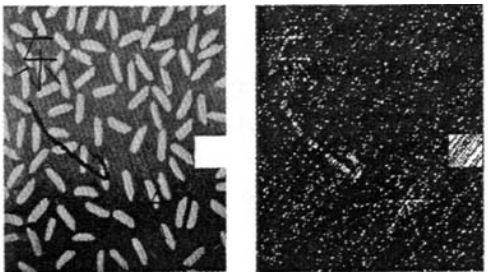
图3 不可见性测试

Fig. 3 The sightless testing

2.2 图像定位能力分析

定位精度的验证分析:对水印图像 Rice 篡改后的图像进行两次认证(图 4),在第一次中,跳过了引入阈值 L 的验证过程(图 4(b));在第二次中,执行了认证算法的所有步骤,引入阈值 L 的验证过程,并且也给出了取不同阈值的检测效果(图(c)、(d)),得出当阈值取 4 时可以达到良好的定位效果。

由图 4 可以看出,引入阈值 L 的验证过程,大大降低了篡改检测的虚警概率;同时对比图中可知篡改区域内部绝大多数的图像块均被正确的检测出篡改,仍然保持着较高的篡改检测概率。

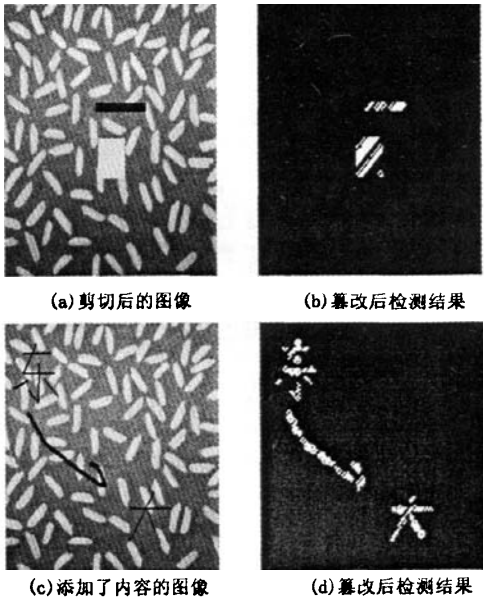


(a)被篡改的含水印的图像 (b) 无阈值处理

(c) 阈值处理 L_{w3} (d) 阈值处理 L_{w4}

图4 恶意篡改及篡改检测的阈值处理操作

Fig. 4 The intentional tamper and threshold processing localization



(a)剪切后的图像 (b)篡改后检测结果

(c)添加了内容的图像 (d)篡改后检测结果

图5 恶意攻击的检测结果

Fig. 5 The testing results of the intentional tamper

局部篡改的定位能力分析:对带有水印图像进行恶意攻击(剪切替换操作、添加物体操作等等),在图5中(a)、(c)表示各种恶意攻击篡改后的水印图像;图5中(b)、(d)是对各自受到修改的篡改定位结果。从而证明本文所提出的算法抵抗恶意攻击的能力很强,水印图像对恶意篡改具有很好的敏感性。

3 结论

1)图像块的水印选择 Logistic 映射作为混沌系统,从该图像块本身产生一系列混沌序列,作用于水印的嵌入,以提高算法的定位精度。

2)每个图像块产生的水印按照 Torus 自同构映射嵌入另一个映射块的 LSB,对应关系通过密钥(必须是素数)来确定,可以保证 Torus 自同构映射是一一映射,提高了算法的安全性,使其能抵抗类似于拼贴攻击这样的伪造攻击。

3)认证时,根据图像块水印被篡改的个数并结合其8个邻域判定该图像块是否被篡改,以提高定位精度和安全性。

参考文献:

[1] KUNDUR D, HATZINAKOS D. Digital watermarking for telltale tamper - proofing and authentication[C]// Proceedings of the IEEE International Conference on Image Processing, Fort Collins, Colorado, 1999. CA: IEEE Computer Society Press, c1999.

[2] FRIDRICH J, GOLJAN M. Images with self - correcting capabilities [C]// Proceedings of the IEEE International Conference on Image Processing, Fort Collins, 1999. CA: IEEE Computer Society Press, c1999.

[3] FRIDRICH J, GOLJAN M, BALDOZA A C. New fragile authentication watermark for images[C]// Proceedings of ICIP, Vancouver, 2000. Canada: [s.n.], 2000

[4] FRIDRICH J. Image watermarking for tamper detection [C]// Proc ICIP, Chicago, 1998. IL: Vieweg Publishing Company, c1998.

[5] 张春田, 张 静. 基于混沌映射的鲁棒性图像水印算法[J]. 电子学报, 2002, 30(1): 69-72.

[6] AKRITAS P, ANTONIOU I E, PRONKO G P. On the torus automorphisms analytic solution computability and quantization chaos [J]. Chaos Solitons and Fractals, 2001(12):2805-2814.

(责任编辑 马立)