一种基于抖动和混沌技术的数字图像篡改检测及修复算法*

王兴元† 张继明

(大连理工大学电子信息与电气工程学部, 大连 116024)

(2014 年 5 月 12 日收到; 2014 年 6 月 22 日收到修改稿)

本文提出了一种基于抖动和混沌技术的数字图像篡改检测及修复算法. 该算法使用小波变换后的低频子图和抖动技术生成图像的认证及修复信息, 在有效减少水印数据量的同时, 将水印嵌入小波变换后的高频子图, 从而达到水印的不可见性. 运用混沌技术完成水印的嵌入和加密, 并结合中国余数定理, 进一步减少水印嵌入对图像质量的影响. 实验证明, 该算法兼顾了水印的不可见性和鲁棒性, 并且能够一定程度修复篡改图像, 在图像认证和修复方面具有较高的实用意义.

关键词: 图像认证, 图像修复, 抖动, 混沌

PACS: 07.05.Pj, 05.45.Gg **DOI:** 10.7498/aps.63.210701

1 引 言

数字信息技术的发展为当今社会生活带来了深刻的变革. 在我们享受信息技术高效便利的同时, 也面临对数字信息安全性的挑战. 有效地验证数字信息, 对数字信息的篡改进行检测是目前研究的重点. 基于水印的数字图像认证技术可以被应用于法庭实证、新闻图片、商业票据、视频监视[1]等场合. 为达到这些目的, 许多鲁棒水印算法[2−5]被应用于图像保护. 但是这些算法很难抵御一些对图像的恶意篡改. 因此, 对篡改敏感的脆弱水印算法被提出并广泛研究. 如Kundur和Hatzinakos[6]提出了基于脆弱水印技术的图像完整性认证算法. Lu等[7]提出了一种基于矢量量化的脆弱水印技术. 基于离散余弦变换(DCT)和矢量量化技术的水印系统也被应用于数字图像的篡改检测和内容认证[8]. 这些算法能够检测图像的扭曲或者篡改, 但对JPEG压缩等常规操作却不能正确识别. 因此, 允许图像的常规操作并对图像恶意篡改敏感的半脆弱水印被提出[9,10]. 除了以上认证技术, 目前还有很多具有图像修复功能的数字水印技术被提出[11−13]. Piva等[14]提出的认证算法不能进行篡改定位. 类似的算法[15]可以进行精确定位, 但却不能进行修复. Chamlawi等[16]提出了一种可以精确检测篡改, 并且能够恢复图像的算法, 但却牺牲了安全性和不可见性. 一些算法[17,18]将图像经过小波变换的近似子图信息引藏于其他子图中, 具有较高的安全性, 但再加入图像的修复信息后[19]图像质量受到一定影响. 混沌系统作为典型的非线性系统近年来得到了广泛的应用[20,21], 因为其具有极端的初值敏感性和伪随机等特性, 也常被应用于图像加密和认证[22−27]. 本文提出了一种基于抖动和混沌技术的数字图像篡改检测及修复算法, 在保证水印安全性的同时兼顾了水印的不可见性和鲁棒性, 并且能够修复篡改图像.

* 国家自然科学基金(批准号: 61370145, 61173183, 60973152)、高等学校博士学科点专项科研基金(批准号: 20070141014)、辽宁省高等学校优秀人才支持计划(批准号: LR2012003)、辽宁省自然科学基金(批准号: 20082165)和中央高校基本科研基金(批准号: DUT12JB06)资助的课题.

† 通讯作者. E-mail: wangxy@dlut.edu.cn

2 图像抖动

抖动技术简单的说就是用较小数量的颜色去模拟更多数量的颜色, 如用16位色显示24位色图像, 为了达到或者接近24位色图像的效果, 就要进行抖动, 如图1所示.

Floyd-Steinberg抖动法是一个比较经典的基于误差扩散的抖动算法. 这里的误差就是转换前后像素颜色的差别值, 具体扩散的方法如下:

1) 为每个像素寻找最接近的新色彩. (a) 如果是灰度图到黑白图的抖动, 则进行简单的阀值操作. (b) 如果是更复杂的如24位色到16位色, 应该将RGB分别处理, 为每个分量分别寻找最接近的值.

2) 计算新色彩与原色彩间的误差. 误差 = 原色彩值 – 新色彩值, 不取绝对值.

3) 分割误差成多份, 并把他们添加到与当前像素邻近且未访问过的像素上去.

具体分割误差方法如下, 推荐按照

$$\begin{bmatrix} \blacksquare & X & 7 \\ 3 & 5 & 1 \end{bmatrix}$$

来进行分割误差, ■是已经访问过的像素, X 是指当前像素, 误差被分成了 $(3+5+1+7)=16$ 份, 分别添加到左下、下、右下、右像素上去. 当水平扫描像素时, 就存在从左向右扩散与从右向左扩散两种选择. 在本文中交叉来进行, 也就是一行从左到右, 下一行从右到左,

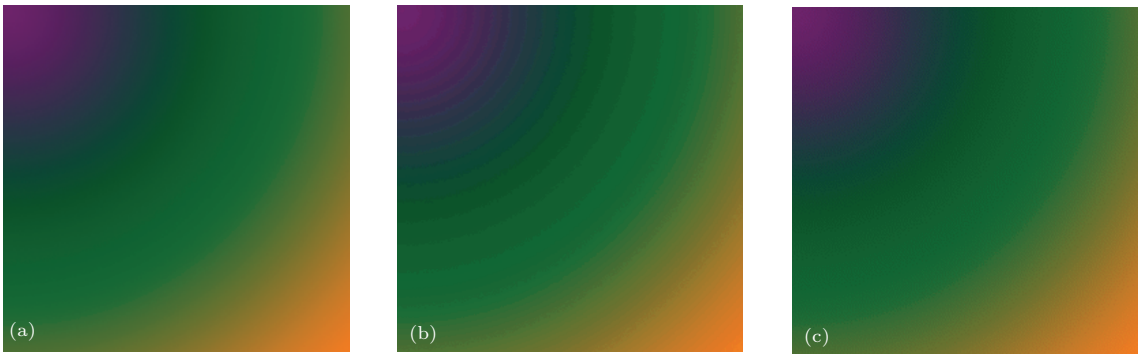
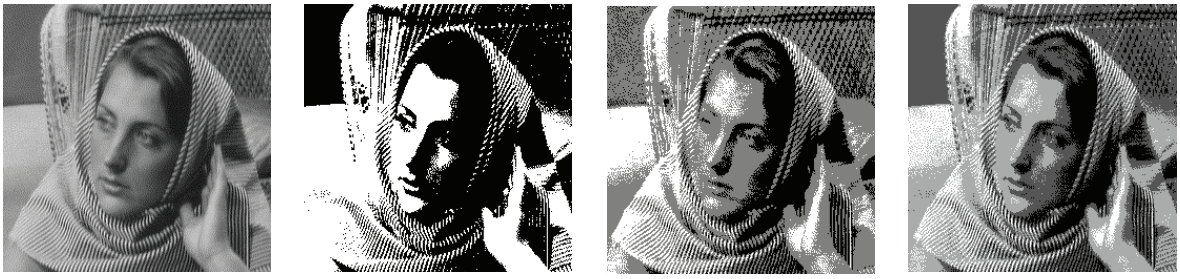
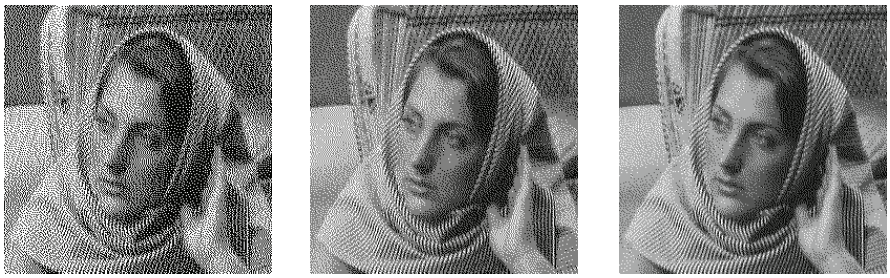


图1 (网刊彩色) 16位抖动图 (a) 24位原图; (b) 16位图 (无抖动) (c) 16位抖动图



(a) 灰度原图 (b) 二值图 (c) 三值图 (d) 四值图



(e) 抖动后二值图 (f) 抖动后三值图 (g) 抖动后四值图

图2 Woman图

$$\begin{bmatrix} 7 & X & \blacksquare \\ 1 & 5 & 3 \end{bmatrix}$$

这样可以有效防止产生流水效应(两行像素因为色彩太接近, 在同向扩散时一些色彩较突出的像素会出现在同一列附近).

用黑白色也就是二值图像模拟256阶灰度就是通常我们所熟知的早期黑白报纸印刷所采用的半影调技术, 是抖动技术的特殊形式. 图2是Woman图的二值图、三值图、四值图的简单映射及应用抖动技术后的图像. 从图2可以看出, 抖动后的三值图和四值图比较半影调技术有更好的视觉效果和细节保留.

3 算 法

图像水印信息的提取和嵌入过程如图3所示. 首先将图像进行小波变换, 得到其低频近似子图L, 将L抖动变换为四值图像生成W, 然后将W嵌入混沌置乱后的小波变换的其他高频子图, 反置乱后与L子图进行小波逆变换生成水印图像.

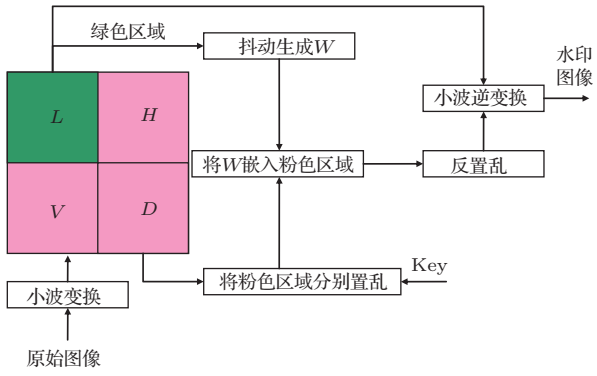


图3 (网刊彩色) 水印生成和嵌入

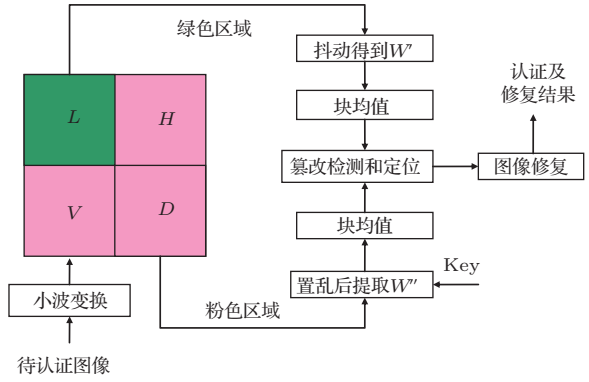


图4 (网刊彩色) 水印提取和认证

图像认证时, 首先将待认证图像进行小波变换, 由近似子图L进行抖动处理得到W', 与从待认证图像其他小波子图中提取的水印W''进行比较, 从而进行篡改定位和图像修复, 如图4所示.

3.1 水印的生成

首先将一个大小为$2m \times 2n$的图像进行小波变换, 将变换后大小为$m \times n$的近似子图L抖动为四值图像, 取值为[0,1,2,3], 从而得到W. 图5显示了变换前后的Women图, 及L子图抖动后得到的水印W.

(a) Woman 图

(b) 小波变化

(c) 水印 W

图5 Woman图小波变换及水印

3.2 水印的嵌入

首先, 将小波变换后的其他高频子图结合分段线性映射(PWLCM)进行混沌置乱. 分段线性映射公式为

$$x_{n+1} = F(x_n, \varepsilon) = \begin{cases} x_n/\varepsilon, & 0 \leqslant x_n < \varepsilon, \\ (x_n - \varepsilon)/(0.5 - \varepsilon), & \varepsilon \leqslant x_n \leqslant 0.5, \\ F(1 - x_n, \varepsilon), & 0 < x_n \leqslant 0, \end{cases} \quad (1)$$

其中 $x_n \in [0,1)$, $\varepsilon \in (0,0.5)$. 可以证明PWLCM映射不仅是混沌映射, 而且 x_n 在区间[0,1)上还具有均匀的不变分布[28].

置乱的方法是根据密钥, 由PWLCM映射生成3个随机序列 $\{x_i^H|i=1,2,\cdots,m\times n\}$, $\{x_i^V|i=1,2,\cdots,m\times n\}$, $\{x_i^D|i=1,2,\cdots,m\times n\}$, 然后根据随机序列分别将 H, V, D 子图置乱. 置乱时, 将每个子图中第 i 个元素和第 j 个元素调换, 即 $p_i \Leftrightarrow p_j$. 其中

$$j = \lfloor x_i \times (m \times n) \rfloor. \tag{2}$$

为保证置乱后的随机性, 可以根据情况进行多次置乱.

结合中国余数定理(chinese remainder theorem, CRT)进行水印信息的嵌入. 中国余数定理是中国古代求解一次同余式组的方法, 是数论中一个重要定理, 又称中国剩余定理, 被广泛应用在不同的工程问题中, 如层次访问控制的密钥分配问题、隐秘图像共享和余数系统等. 其基本思想可分为两个部分: 正向CRT和逆向CRT运算.

正向CRT运算是在已知除数和余数情况下求出大整数. 设 Z 是大整数, μ 是 n 个互素整数的集合, 表示为 $\mu = \{M_1, M_2, \cdots, M_n\}$, 设 r 是 n 个余数的集合, 表示为 $r = \{R_1, R_2, \cdots, R_n\}$, 其中 R_i 可由下式计算:

$$Z \equiv R_i (\mathrm{mod} M_i), \quad 1 \leqslant i \leqslant n. \tag{3}$$

Z 可用下式得到:

$$Z \equiv \left(\sum_{i=1}^{n} R_i \frac{M}{M_i} K_i \right) \pmod{M}, \tag{4}$$

其中

$$M = M_1 \times M_2 \times \cdots \times M_n,$$

$$0 < Z \leqslant M - 1,$$

K_i 可通过下式计算得出:

$$K_i \frac{M}{M_i} \equiv 1 \bmod M_i. \tag{5}$$

例如, 给定除数对 $\mu = [6,11]$, 余数对 $r = [4,8]$, 使用(3)式可得出 $K_1 = 5$, $K_2 = 2$, 利用(4)式即可得出 $Z = 52$.

逆向CRT运算是在已知除数和大整数的情况下求出余数. 同样设除数对 $\mu = [6,11]$ 和 $Z = 52$, 则利用(3)式可得出余数对 $r = [4,8]$.

将 W 置入小波变换后的子图时, 将置乱后的子图中每个元素的值作为大整数 Z, 形成三个序列, 即 $\{Z_i^H|i = 1,2,\cdots,m\times n\}$, $\{Z_i^V|i = 1,2,\cdots,m\times n\}$ 和 $\{Z_i^D|i = 1,2,\cdots,m\times n\}$, 设定互素的除数对为 $\mu = [6,11]$, 并作为解密密钥一部分. 水印嵌入分为以下步骤:

1) 对 Z_i^H, Z_i^V 和 Z_i^D 分别应用(3)式求出余数对 r_H, r_V 和 r_D.

2) 每个余数对中如果 $R_1 > R_2$, 则记作1, 否则记做0, 从而得到 w_H, w_D 和 w_V.

3) 如果 $w_i \neq w_H + w_V + w_D$, 则调整 Z_i^H, Z_i^V 和 Z_i^D 的值, 使 $w_i = w_H + w_V + w_D$.

4) 调整 Z_i^H, Z_i^V 和 Z_i^D 数值时, 遵循最小代价原则. 即对每个数值分别进行循环加1和循环减1运算, 直到产生要求的余数对. 比较两种运算, 从加和减的运算中选取对数值改变最小的方式.

5) 比较改变 Z_i^H, Z_i^V 和 Z_i^D 每个数值的代价, 从代价最小的数据开始调整, 直到满足 $w_i = w_H + w_V + w_D$, 从而完成水印嵌入.

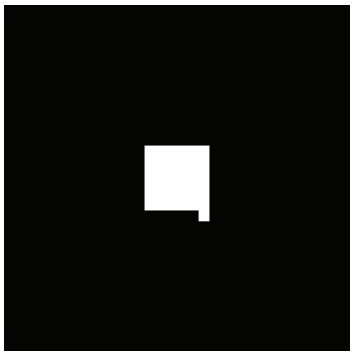
3.3 图像的篡改定位和修复

图像认证时首先将认证图像进行小波变换, 由低频近似子图抖动后得到 W'. 以嵌入过程中的相同秘钥, 结合中国余数定理, 对高频子图进行置乱后, 用水印嵌入时相同的方法计算得到 W''. 按照设定的大小 s 分别对 W' 和 W'' 进行分块得到 $\{w_i'|i = 1,2,\cdots,\lfloor m/s \rfloor \times \lfloor n/s \rfloor\}$ 和 $\{w_i''|i = 1,2,\cdots,\lfloor m/s \rfloor \times \lfloor n/s \rfloor\}$, 对每个图像块求块均值得到 $\{A_i'|i = 1,2,\cdots,\lfloor m/s \rfloor \times \lfloor n/s \rfloor\}$ 和 $\{A_i''|i = 1,2,\cdots,\lfloor m/s \rfloor \times \lfloor n/s \rfloor\}$, 如果满足下式:

$$|A_i' - A_i''| > q, \tag{6}$$

则认为该区域被篡改. q 为检测敏感性参数. 由于图像篡改时同样改变了高频信息, 所以篡改检测可能产生误判. 基于图像篡改具有一定面积及相对集中的假设, 检测过程中如果一个单独区域的所有相邻区域都未检测出篡改, 则认为该区域未篡改, 反之如果它的所有相邻区域都检测出篡改, 则认为该区域也被篡改. 用 W'' 替换近似子图中检测出篡改的区域, 然后用逆向小波变换得到的图像修复篡改图像. 图6显示了 $s = 4$, $q = 18$ 时, 篡改检测及修复结果.

(a) 篡改图



(b) 篡改检测结果

(c) 修复图

(d) 水印 W'

(e) 水印 W''

图 6 Woman 篡改图及检测修复结果

4 实验结果分析

峰值信噪比 (peak signal to noise ratio, PSNR) 被广泛应用于水印图像质量的客观评价, 其值越高, 表示视觉性能越好. 由于算法使用了抖动技术减少了水印的数据量, 并使用中国余数定理降低水印嵌入对图像质量的影响, 所以具有较高的视觉性能. 表 1 是本文算法对几个典型图像嵌入水印后的 PSNR 值及和参考文献的对比. 从表 1 可以看出本文算法的水印图像有良好的视觉质量, 大幅优于参考文献.

表 1 PSNR 值对比

图像	本文算法	Ref[12]	Ref[13]	Ref[19]
Lena	47.91	44.82	41.97	39.28
Peppers	47.83	44.97	41.96	40.01
Woman	47.92	44.87	41.96	39.23

本文在水印嵌入时选择除数对 $\mu = [6, 11]$, 选择其他的除数对时 ([9,17], [11,21], [21,41], [41,81],), 对 Woman 图嵌入水印后的 PSNR 值如图 7 所示. 从图 7 可以看出, 采用除数对的数值越大, 对图像视觉质量的影响越大, 而且运算速度变慢, 本文实验中都采取文献 [6, 11] 除数对.

图像认证过程中分组大小 s、敏感性参数 q 及篡改区域的占比大小, 对篡改检测的准确性都有较大影响. 如图 8 所示, 随着 q 值的改变, 其检测准确性也不断改变.

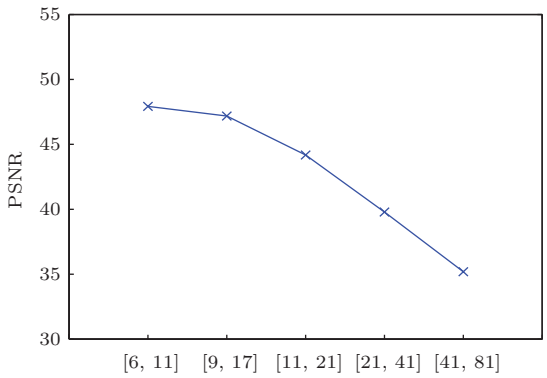
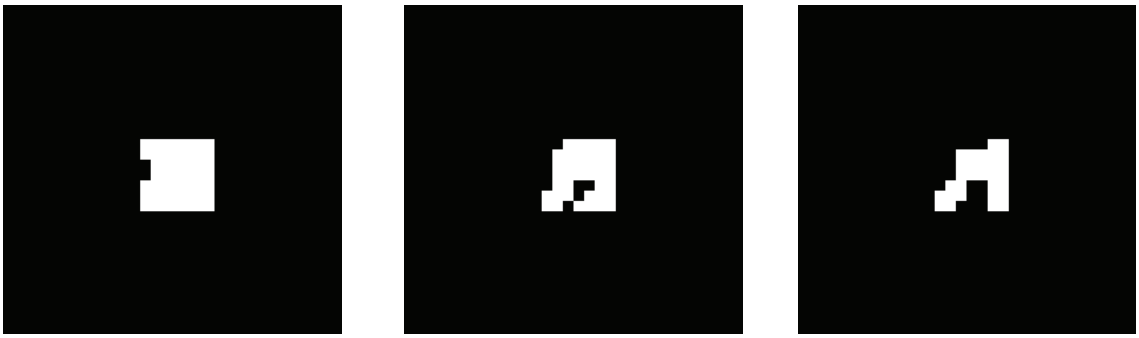


图 7 采用不同 μ 值时的 PSNR

令检测的篡改结果中不是真正篡改区域的比例为错检率 WP, 没有检测出的篡改区域的比例为漏检率 LP. 图 9 分别显示了对于图 8 (a) 篡改图 (篡改区域的长宽占原图的 20%) 的检测, 在 s 取值为 2 至 5 时 WP 及 LP 的变化情况. 通过图 9 可以看出, 随着分组大小的不断增加, 其发生误检的概率不断下降, 而发生漏检的概率不断增加, 需要在实际应用中灵活运用.

(a) 篡改图 (b) $q=10$ (c) $q=15$



(d) $q=20$ (e) $q=35$ (f) $q=40$

图 8 $s=4$ 时不同 q 值的篡改检测结果

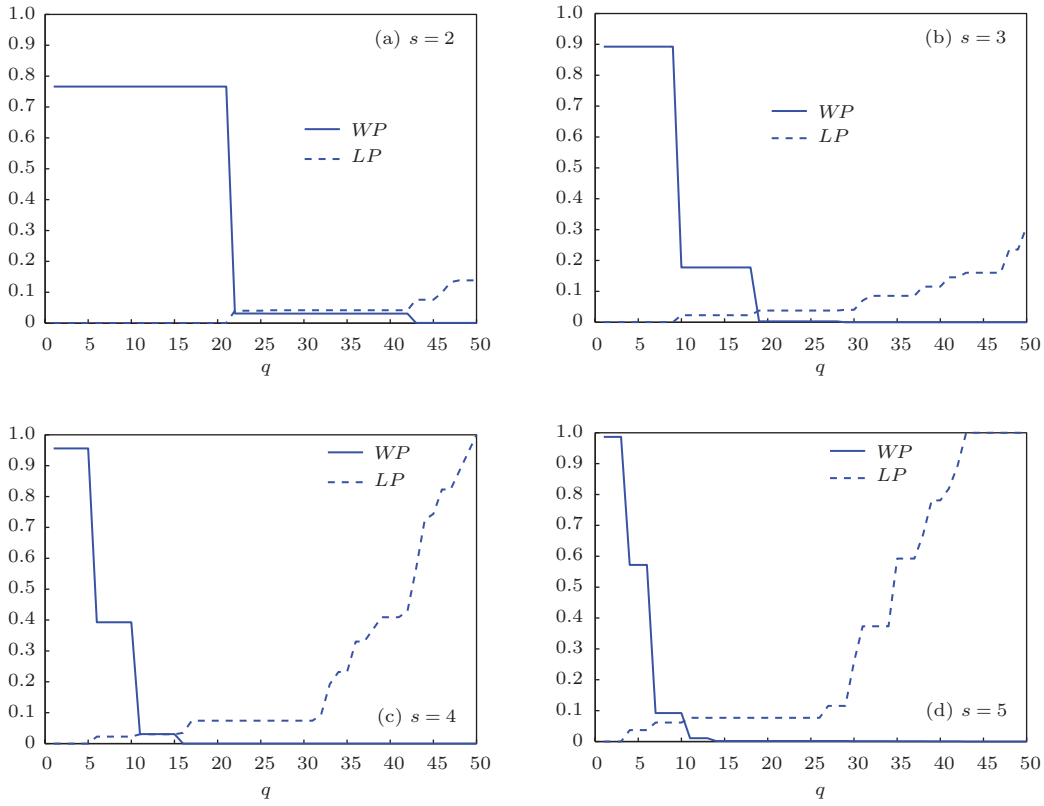


图 9 (网刊彩色) 取不同分组大小的算法性能

篡改区域的大小占比对算法图像检测和恢复的性能也有直接影响. 图10是$s=4$时, 篡改区域长宽分别占原图10%, 30%, 50%, 70%情况下的算法性能. 从图10可以看出随着篡改区域的占比不断扩大, 算法性能也随之下降.

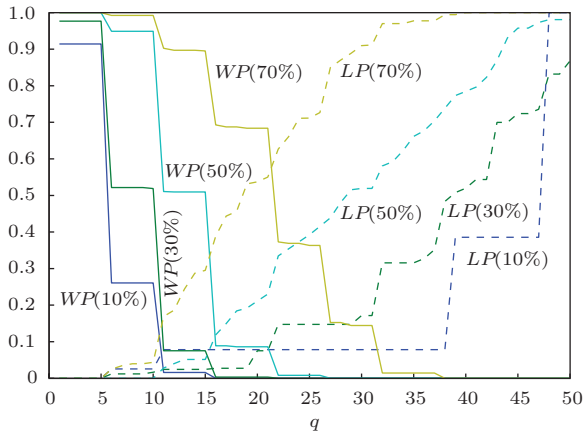


图10 (网刊彩色) 不同篡改大小对算法性能的影响

图11是篡改区域长宽占比50%, 即面积占比25%时, 修复篡改区域后的图像. 从图11可以看出即使篡改面积较大, 算法仍然能够在一定程度上修复图像.

图11 篡改面积达到25%时的修复性能

图12 进行90% JPG压缩后提取的水印W''

图12是对水印图像进行质量因子为90%的JPG压缩后提取的水印W'', 从图12中可以看出, 算法对于JPG压缩具有一定的鲁棒性, 但对性能影响较大, 需要在下一步研究中改善.

5 结 论

本文提出了一种基于抖动和混沌技术的图像篡改检测和修复算法, 在完成图像认证的同时可以进行图像的修复. 通过使用小波变换提高算法的适应性, 并在小波变换中选择低频子图生成水印, 并经过抖动有效减少水印的数据量. 选择高频子图嵌入水印, 在提高水印不可见性的同时兼顾了水印的鲁棒性. 结合中国余数定理和抖动技术有效减少水印嵌入对图像质量的影响. 实验结果证明, 该算法在数字图像认证领域具有一定的应用价值.

参考文献

[1] Fei C, Kundur D, Kwong R H 2006 *Ieee T. Inform. Foren. Sec.* **1** 43
[2] Maity S P, Kundu M K, Maity S 2009 *Comput. Electr. Eng.* **35** 415
[3] Khan A, Tahir S F, Majid A, Choi T S 2008 *Pattern Recogn.* **41** 2594
[4] Khan A, Mirza A M 2007 *Inform. Fusion* **8** 354
[5] Lu W, Sun W, Lu H 2009 *Comput. Electr. Eng.* **35** 183
[6] Kundur D, Hatzinakos D 1999 *P. Ieee* **87** 1167
[7] Lu Z M, Liu C H, Xu D G, Sun S H 2003 *Electron. Lett.* **39** 35
[8] Wang F H, Yen K K, Jain L C, Pan J S 2007 *Inform. Sciences* **177** 2522
[9] Qi X J, Xin X 2011 *J. Vis. Commun. Image R.* **22** 187
[10] Liu F, Leung H Y, Cheng L M, Ji X 2012 *Chin. Phys. B* **21** 040204
[11] Ho C K, Li C T 2004 *International Conference on Information Technology Coding and Computing* Las Vegas, USA, April 5–7, 2004 p7
[12] Hung K M, Chen T W, Su W K, Kao C N 2012 *International Conference on Information Science and Digital Content Technology* Jeju Island, South Korea,June 26–28, 2012 p730
[13] Patra B, Patra J C 2012 *IEEE International Symposium on Intelligent Signal Processing and Communication Systems Tamsui,* New Taipei City, Taiwan, November 04–07, 2012 p430
[14] Piva A, Bartolini F, Caldelli R 2005 *International Journal of Image and Graphics* **5** 149
[15] Liu H J, Steinebach M 2006 *Second International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution* Leeds, UK, December 13–15, 2006 p143

[16] Chamlawi R, Khan A, Idris A 2007 *J. Comput. Sci. Technol.* **22** 795
[17] Ishihara N, Koki A 2007 *Ieice T. Fund. Electr.* **E90**-A 1045
[18] Holliman M, Memon N 2000 *Ieee T. Image Process.* **9** 432
[19] Chamlawi R, Khan A, Usman I 2010 *Comput. Electr. Eng.* **36** 578
[20] Ma T D, Jiang W B, Fu J 2012 *Acta Phys. Sin.* **61** 090503 (in Chinese) [马铁东, 江伟波, 浮洁 2012 物理学报 **61** 090503]
[21] Ma T D, Jiang W B, Fu J, Xue F Z 2012 *Acta Phys. Sin.* **61** 100507 (in Chinese) [马铁东, 江伟波, 浮洁, 薛方正 2012 物理学报 **61** 100507]
[22] Song W, Hou J J, Li Z H, Huang L 2009 *Acta Phys. Sin.* **58** 4449 (in Chinese) [宋伟, 侯建军, 李赵红, 黄亮 2009 物理学报 **58** 4449]
[23] Cao G H, Hu K, Tong W 2011 *Acta Phys. Sin.* **60** 110508 (in Chinese) [曹光辉, 胡凯, 佟维 2011 物理学报 **60** 110508]
[24] Zhou W J, Yu M, Min Y S, Jiang G Y, Ge D F 2012 *Acta Phys. Sin.* **61** 080701 (in Chinese) [周武杰, 郁梅, 禹思敏, 蒋刚毅, 葛丁飞 2012 物理学报 **61** 080701]
[25] Wang X Y, Liu L T 2013 *Chin. Phys. B* **22** 050503
[26] Wang X Y, Bao X M 2013 *Chin. Phys. B* **22** 050508
[27] Sun F Y, Liu S T, Lü Z W 2007 *Chin. Phys.* **16** 3616
[28] Li S J, Mou X Q, Cai Y L, Ji Z, Zhang J H 2003 *Comput. Phys. Commun.* **153** 52

A novel image authentication and recovery algorithm based on dither and chaos*

Wan Xing-Yuan† Zhang Ji-Ming

(*Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China*)

(Received 12 May 2014; revised manuscript received 22 June 2014)

Abstract

This paper presents a digital image tamper detection and recovery algorithm, which uses the dither and chaos technology. Certification of generated image and the repair information gained by low frequency sub-diagram and dither technology after wavelet transform can effectively reduce the amount of data. At the same time, the watermark is embedded in high frequency sub-diagram, so as to make the watermark invisible. Chaos technology is used to complete watermark embedding and encryption; and combined with the Chinese remainder theorem, the impact on the image quality can further be reduced. Experimental results show that the algorithm's watermark has high invisibility and robustness, and also can repair tampered images. So it has a high practical significance in the image authentication and recovery.

Keywords: image authentication, image recovery, dither, chaos

PACS: 07.05.Pj, 05.45.Gg **DOI:** 10.7498/aps.63.210701

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61370145, 61173183, 60973152), the Doctoral Program Foundation of Institution of Higher Education of China (Grant No. 20070141014), the Program for Liaoning Excellent Talents in University, China (Grant No. LR2012003), the Natural Science Foundation of Liaoning Province, China (Grant No. 20082165), and the Fundamental Research Funds for the Central Universities, China (Grant No. DUT12JB06).

† Corresponding author. E-mail: wangxy@dlut.edu.cn