

一种基于混沌和汉明码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)

(2013年8月29日收到; 2013年9月24日收到修改稿)

提出了一种基于混沌映射和汉明码的数字图像篡改检测及修复算法. 该算法采用了目前在信道编码中广泛使用的编组码汉明码, 将差错控制应用于图像认证和修复, 并使用混沌映射保证算法的有效性和安全性. 分析及实验表明: 该算法在保证良好的视觉效果, 嵌入较少认证信息的前提下, 可以有效地进行数字图像篡改检测, 并能够完成一定程度的图像修复.

关键词: 图像认证, 图像修复, 汉明码, 混沌

PACS: 07.05.Pj, 05.45.Gg

DOI: 10.7498/aps.63.020701

1 引言

近年来, 随着互联网技术的发展, 数字媒体的应用越来越广泛, 大量的数字媒体信息依靠网络传播. 但是在传播过程中, 数字媒体信息可能因为在传输过程中丢失数据包^[1], 或者被恶意篡改而遭到破坏. 为解决这个问题, 许多鲁棒水印算法^[2-6]被应用于图像的内容保护, 但这些算法不能恢复被篡改的图像, 因此研究者提出很多数字图像恢复算法. 文献^[7-9]提出了基于脆弱和半脆弱水印的算法, 但这些算法的恢复及认证能力有限. Fridrich等^[10]通过将恢复信息隐藏在离原始块一定距离的图像块中实现图像恢复; Cao和Li^[11]通过丢失块的邻居块来重建丢失块的低频DCT系数, 这些算法的效率很高, 因此被应用于实时系统. Kang和Leou^[12]使用一种边缘吻合向量量化法 (side-match vector quantization, SMVQ)^[13]生成特征值, 然后嵌入相应图像块的DCT系数, 实现错误恢复编码, 这种算法可以很大程度地恢复图像

的丢失块, 但由于需要嵌入太多的信息而牺牲了图像质量. 另外, Lu^[14]提出了一种使用小波变换认证信息的图像恢复算法, 但是其恢复图像的质量偏低; Chamlawi等^[15]使用小波变换可以有效地进行图像认证和恢复, 但其安全性和图像的视觉效果不高; Wang和Tsai^[16]提出了一种基于分形编码的图像自动认证和恢复算法, 这种算法效率较高, 但其处理过程复杂, 并且需要面临“重要区域”(ROF) 选择的问题. 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^[17-19], 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^[20-22]. 在上述研究的基础上, 本文提出了一种基于汉明码和混沌映射的数字图像认证和修复算法. 该算法应用汉明码编码原理, 将图像的高位信息编码后嵌入图像的较低位, 在保证嵌入较少认证信息, 保持图像质量的前提下, 可以同时完成数字图像的篡改检测和图像修复, 并通过混沌系统保证了算法的良好特性和安全性, 且该算法可以灵活采用多种编码和混合编码方式,

^{*} 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)、辽宁省国家自然科学基金 (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

进一步提高适用性.

2 汉明码

汉明码是一种错误校验码码集, 由 Bell 实验室的 Hamming 发明, 是能纠正一位错码的效率最高的分组码^[23]. 与其他的错误校验码类似, 汉明码也利用了奇偶校验位的概念, 通过在数据位后面增加一些比特, 可以验证数据的有效性. 汉明码不仅可以验证数据是否有效, 还能在数据出错的情况下指明错误位置并改正. 它满足:

$$2^r - 1 > n, \quad (1)$$

这里 n 为码元总位数, r 为监督码元位数.

例如: 构造一个信息位 $k = 4$ 的汉明码. 则根据 (1) 式, 可计算出 $r \geq 3$. 现取 $r = 3$, 则 $n = 7$. 用 a_6, a_5, a_4, a_3 表示信息位, 则可得到 a_2, a_1, a_0 三位监督位:

$$\begin{cases} a_2 = a_6 \oplus a_5 \oplus a_4 \\ a_1 = a_6 \oplus a_5 \oplus a_3 \\ a_0 = a_6 \oplus a_4 \oplus a_3 \end{cases}, \quad (2)$$

由 7 个码元按照下列访法运算得到校正子

$$\begin{cases} S_1 = a_6 \oplus a_5 \oplus a_4 \oplus a_2 \\ S_2 = a_6 \oplus a_5 \oplus a_3 \oplus a_1 \\ S_3 = a_6 \oplus a_4 \oplus a_3 \oplus a_0 \end{cases}, \quad (3)$$

不难看出 a_6, a_5, a_4 或 a_2 发生错误时, 校正子 $S_1 = 1$; a_6, a_5, a_3 或 a_1 发生错误时, 校正子 $S_2 = 1$; a_6, a_4, a_1 或 a_0 发生错误时, 校正子 $S_3 = 1$; 否则校正子等于 0. 校正子的取值与错码位置的对应关系如表 1 所示. 经计算可得 (7, 4) 码的全部码字, 如表 2 所示. 上述 (7, 4) 码能纠 1 个错误. 11 位信息位时需要 4 位监督码 ($2^4 > 11 + 4 + 1$), 64 位信息位时就需要 7 位监督码 ($2^7 > 64 + 7 + 1$).

3 图像的视觉冗余

根据图像采用的颜色数, 可以将图像分为 2 位、8 位和 24 位图. 8 位灰度图和 24 位彩色图像每个像素中最不重要的位被称为最低有效位 LSB (least significant bits), 最重要的位称为最高有效位 MSB (most significant bits). 图 1 给出了 Woman 图每一个位平面的二值图像, 图 2 依次给出了将

Woman 图低位全部补 0 的图像. 从结果可以得出 MSB 对图像影响最大, LSB 图像的影响最小, 将图像的低 3 位全部补 0 后, 图像基本看不出改变.

4 算法

算法首先将图像按位进行置乱, 将置乱后图像的高位当做汉明码的信息位, 把计算得到的监督位嵌入置乱图像的低位, 得到水印置乱图像, 然后将水印图像进行反置乱得到水印图像, 过程如图 3 所示.

表 1 校正子与错误位置的对应关系

$S_1 S_2 S_3$	错误位置
000	无错
001	a_0
010	a_1
011	a_2
100	a_3
101	a_4
110	a_5
111	a_6

表 2 (7, 4) 码全部码字

	码 字			码 字	
	信息码元	监督位		信息码元	监督位
0	0 0 0 0	0 0 0	8	1 0 0 0	1 1 1
1	0 0 0 1	0 1 1	9	1 0 0 1	1 0 0
2	0 0 1 0	1 0 1	10	1 0 1 0	0 1 0
3	0 0 1 1	1 1 0	11	1 0 1 1	0 0 1
4	0 1 0 0	1 1 0	12	1 1 0 0	0 0 1
5	0 1 0 1	1 0 1	13	1 1 0 1	0 1 0
6	0 1 1 0	0 1 1	14	1 1 1 0	1 0 0
7	0 1 1 1	0 0 0	15	1 1 1 1	1 1 1

图像认证时, 首先将待认证图像进行置乱, 然后提取汉明码, 验证汉明码的有效性并进行纠错, 得到修复后的置乱图像, 然后将图像进行反置乱, 根据错误位信息进行篡改定位和判断, 并对图像进行二次修正, 最终得到恢复图像, 过程如图 4 所示.

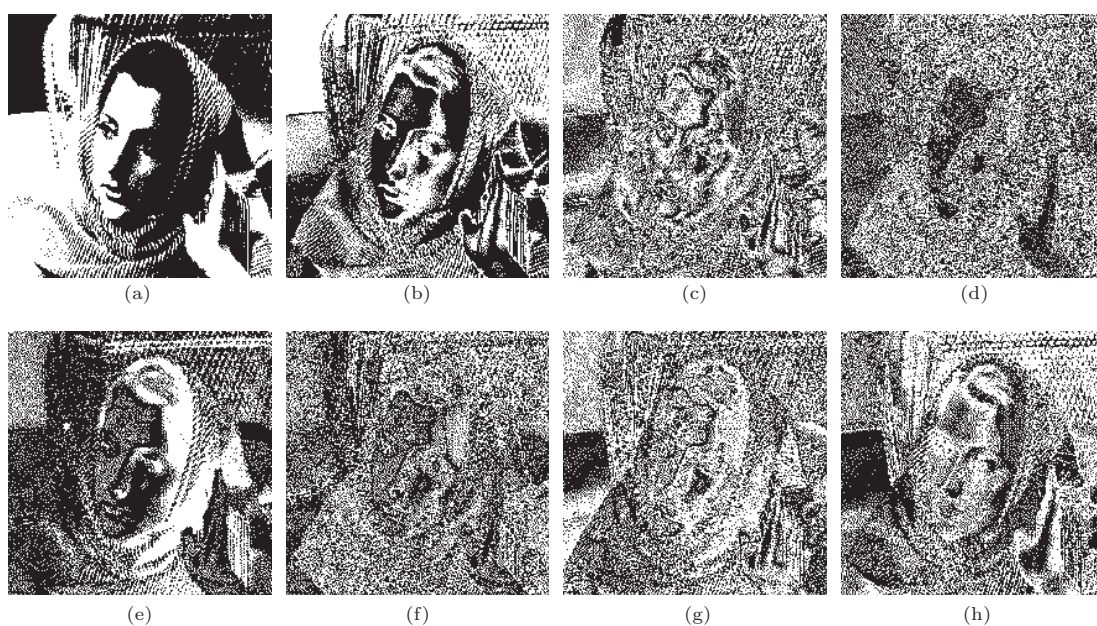


图1 Woman图每个位平面二值图像 (a) 第8位; (b) 第7位; (c) 第6位; (d) 第5位; (e) 第4位; (f) 第3位; (g) 第2位; (h) 第1位

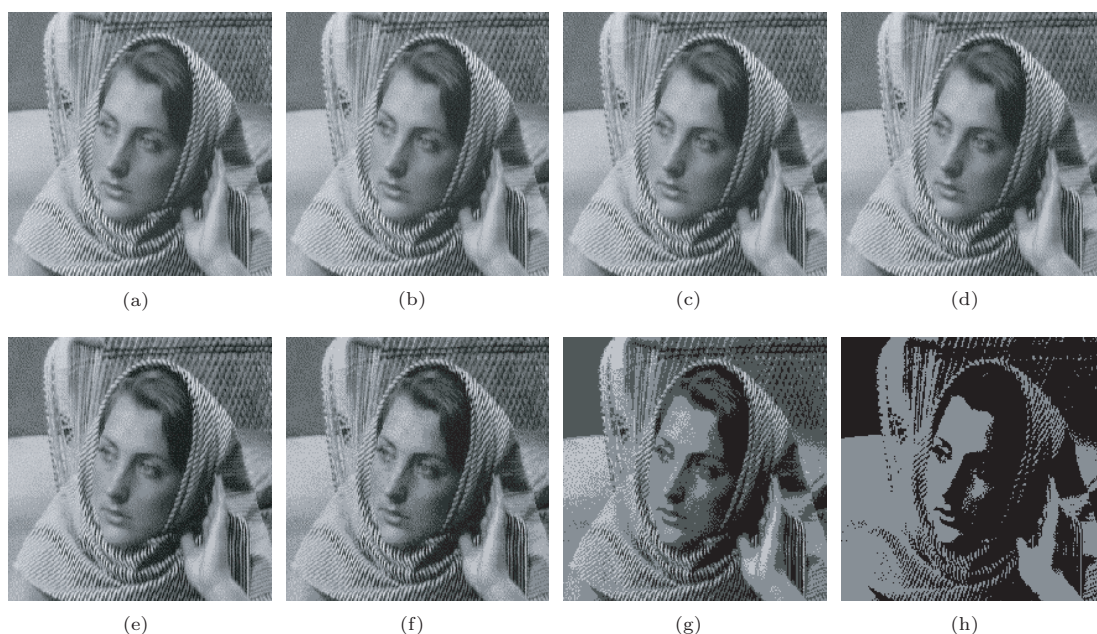


图2 Woman图低位补0图像 (a) 原图; (b) 最低位补0; (c) 低2位补0; (d) 低3位补0; (e) 低4位补0; (f) 低5位补0; (g) 低6位补0; (h) 低7位补0

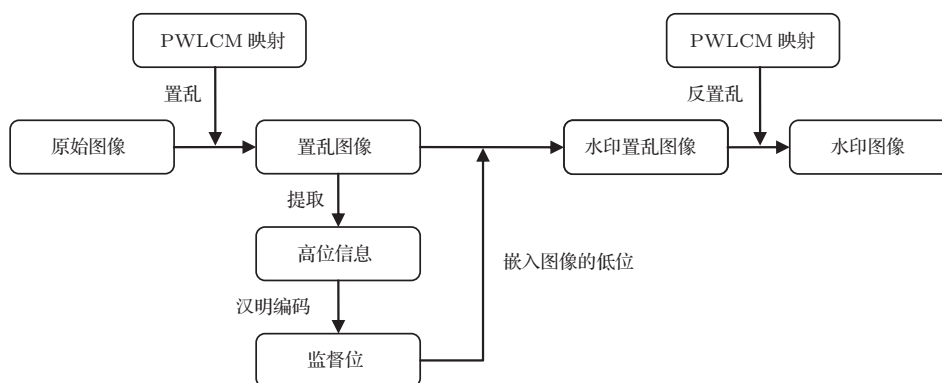


图3 水印的提取和嵌入

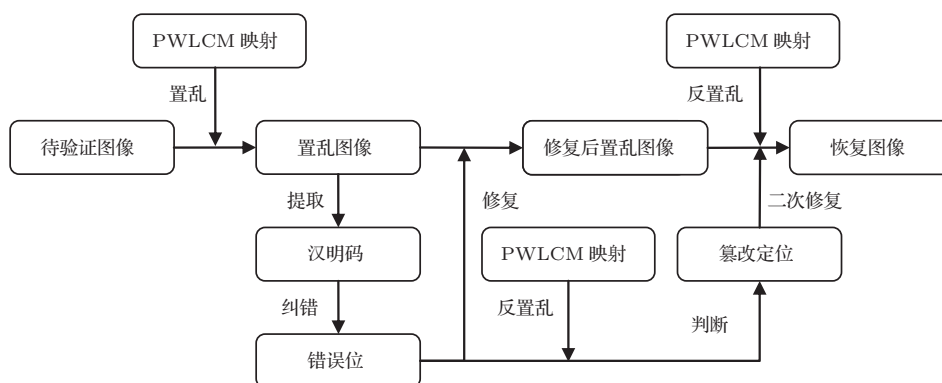


图4 图像的认证和修复

4.1 图像特征信息的提取和嵌入

首先将图像每个像素点的值由十进制转换为二进制, 然后将所有像素的不同位组成8个二进制序列 $P_1, P_2, \dots, P_8$. 若一个大小为 $m \times n$ 的图像, P_i^j 表示第 i 个像素点二进制值的第 j ($j = 1, 2, \dots, 8$) 位的值, 则

$$\begin{aligned} P_1 &= \{p_i^1 | i = 1, 2, \dots, m \times n\}, \\ P_2 &= \{p_i^2 | i = 1, 2, \dots, m \times n\}, \dots, \\ P_8 &= \{p_i^8 | i = 1, 2, \dots, m \times n\}. \end{aligned}$$

然后使用分段线性映射 (PWLCM)^[24], 对8个序列进行置乱操作. 分段线性映射

$$\begin{aligned} x_{n+1} &= F(x_n, \varepsilon) \\ &= \begin{cases} x_n / \varepsilon & 0 \leq x_n < \varepsilon \\ (x_n - \varepsilon) / (0.5 - \varepsilon) & \varepsilon \leq x_n \leq 0.5 \\ F(1 - x_n, \varepsilon) & 0 < x_n \leq 0 \end{cases}, \quad (4) \end{aligned}$$

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^[24]. 置乱的方法是根据密钥, 由 PWLCM 映射生成8个随机序列

$$\begin{aligned} \{x_i^1 | i = 1, 2, \dots, m \times n\}, \\ \{x_i^2 | i = 1, 2, \dots, m \times n\}, \dots, \\ \{x_i^8 | i = 1, 2, \dots, m \times n\}. \end{aligned}$$

然后根据随机序列分别将 $P_1, P_2, \dots, P_8$ 置乱. 置乱时, 每个序列的第 i 个像素和第 j 个像素调换, 如 $p_i^1 \Leftrightarrow p_j^1$,

$$j = \lfloor x_i \times (m \times n) \rfloor. \quad (5)$$

可以根据情况进行多次置乱. 置乱后的序列记做 $P'_1, P'_2, \dots, P'_8$. 图5为 Woman 原图和经过5次

置乱后的图像. 然后根据 $P'_1, P'_2, \dots, P'_8$ 提取汉明码的信息位, 并生成监督位, 然后将监督位嵌入图像. 本文将讨论保护图像的高2位、高3位、高4位三种情况, 并采用 (7, 4) 汉明码和 (15, 11) 汉明码两种编码方案及一种混合编码方案来反映算法的性能. 7种编码方案可以用图6来表示.

根据情况也可选用 (31, 26) 汉明码, 在本文不做讨论. 根据图6的方案, 在完成信息位提取、监督位的计算和嵌入后, 得到的序列分别进行反置乱即可得到水印图像. 图7显示了采用不同编码方案后得到的水印图像. 从视觉上看难以发现改变.

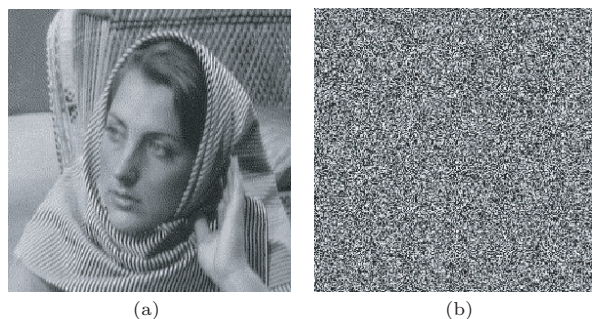


图5 Woman 原图和置乱图 (a) 原图; (b) 置乱图

4.2 图像的篡改定位和修复

图像认证是上述过程的逆过程, 首先将待验证图像的每个像素点的值转换为二进制, 然后以相同的方式和初值进行置乱. 根据采用的编码方案不同, 提取信息位和监督位, 然后验证汉明码的有效性, 并进行纠错. 每进行一次纠错, 就将该点对应置乱前的位置标记为篡改点. 最后将纠错后的序列进行反置乱得到恢复图像. 将 Woman 水印图的中间长和宽为原图1/5的大小的区域全部置0, 图8是各方案修复后的图像和篡改定位结果.

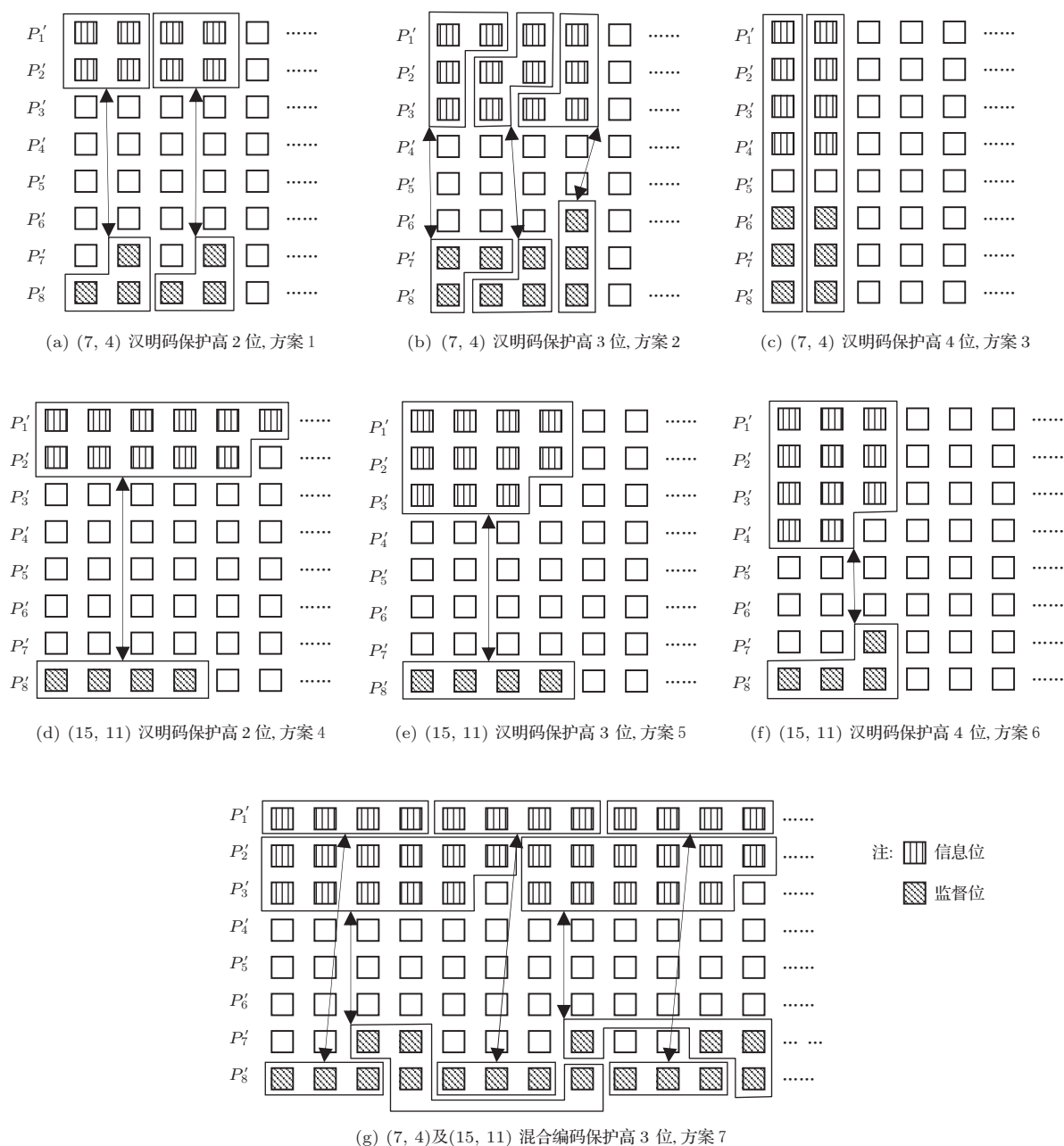


图 6 7 种编码方案

4.3 篡改判断及修正

由于汉明码只能纠正一个错误, 当编码内有两个以上的位被修改后不能正确地进行纠错. 从图 7 中也可以看出, 很多没有被篡改的区域在修复过程中被错误地进行了修改. 因此进行篡改正确性的判断. 由于对图像的篡改一定是有一定面积并且相对集中的, 所以可以进行以下假设.

假设 1 如果一个在首次检测中被认为是篡改点的像素点相邻其他 8 个像素点都没有被篡改,

或者只有 1 个像素点被篡改, 则认为该像素点不是篡改点.

假设 2 如果一个在首次检测中被认为是篡改点的像素点相邻其他 8 个像素点中有以 5 个以上被篡改, 则认为该像素点是篡改点.

图 10 是以上假设的两种示例.

基于以上假设, 我们对图 9 所示的篡改定位结果进行判断和修正, 得到结果如图 11. 从图 11 可以看出, 经过判断和修正, 篡改定位结果非常接近于真实的篡改区域.



图7 水印图像



图8 篡改及恢复图像

4.4 二次修复

如图8所示,首次检测时被认为是篡改点,但判断为非篡改点的像素点称为“错误点”。根据该“错误点”,可以对篡改区域的图像进行二次修复。方法是:

- 1) 查找“错误点”中被错误修改的位;
- 2) 恢复被错误修改的位;
- 3) 查找该位所处的汉明编码的其他所有位;
- 4) 判断其他位是否处于被篡改区域;
- 5) 如果其他位中有大于二个或者小于四个位处于被篡改区域,则全部改变这些位的值。

这样做的原因是:如果一组汉明码不能正确

地纠正错误,则一定是其中两个以上的位发生了改变。而在图像中一定只有在篡改区域内的位才有可能发生改变。因此,在假设篡改区域被如实检测出来的前提下,如果一个“错误点”所处的汉明编码的其他位处于被篡改区域内,则显然是这些位中有两个以上的位发生了改变,从而导致了错误。可以分为以下三种情况:

1) 如果有两个位处于被篡改区域,判定是这两个位都发生了篡改,则改变这两个位的值;

2) 如果有三个位处于被篡改区域,则有可能是两个或者三个位发生了篡改,如果是两个位发生了篡改,同时改变这三个位,错误位从两个变成了一

个; 如果是三个位发生了改变, 篡改被全部纠正;

3) 如果有四个位处于被篡改区域, 则有可能是两个、三个或者四个位发生了篡改, 如果是二个

位发生了篡改, 全部改变后, 错误位仍然保持两个; 如果是三个位发生了篡改, 错误位从三个变成了一个, 如果四个位发生了篡改, 篡改被全部纠正.

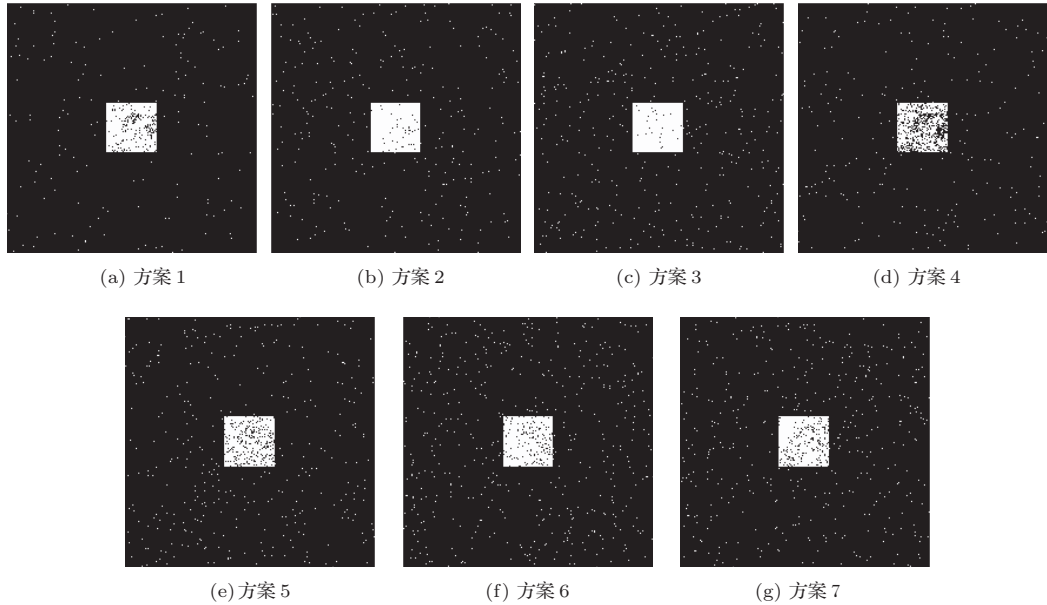


图9 篡改定位结果

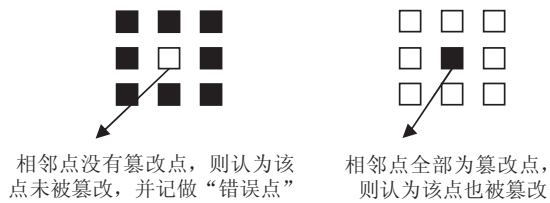


图10 假设示例

进行二次修复, 得到结果如图12. 图12中可以看出, 经过二次修复图像, 恢复图像的质量得到了明显的提高.

5 性能分析

根据以上的二次修复方法, 对图8的恢复图像

因为篡改绝大多数是局部发生的, 而算法使用

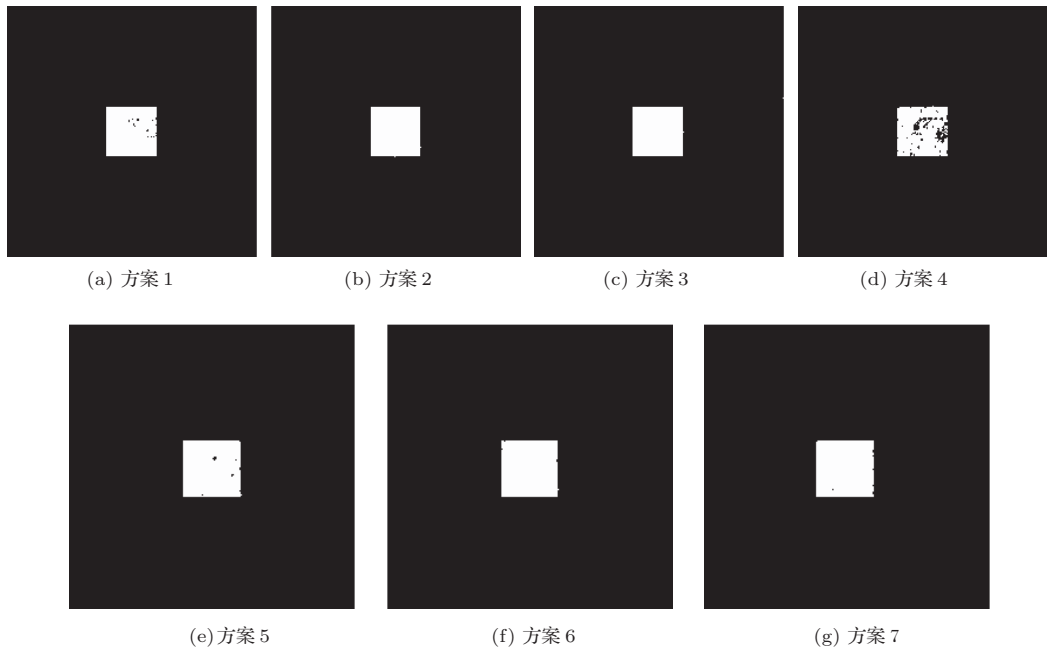


图11 判断和修正后的篡改定位结果

混沌系统对图像位进行了置乱,保证了汉明码的每一组编码在图像中随机分布,可以保证在局部篡改发生时只有个别码被改变,从而可以进行正确的修复.根据本文的算法,只要每一组汉明码中小于四个码被篡改,都可以进行适当的修复.图13显示了算法对于简单图形同样具有良好的恢复能力.

峰值信噪比PSNR (peak signal to noise ratio)被广泛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.表3给出了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3中可以看出,本文算法的水印图像有良好的视觉质量,除方案3以外各方案均优于参考

文献.

从图14中可以看出,采用(15, 11)和混合编码方案,其PSNR值明显好于采用(7, 4)编码的方案.首次篡改检测正确率记为 P_t ,经过判断后的篡改检测正确率记为 P'_t .首次修复后被修复的位的正确率记为 P_r ,二次修复后被修复的位的正确率记为 P'_r .表4和图15为将Lena图的中间长和宽为原图1/5的大小的区域全部置0后,首次修复和二次修复的对比.

从表4中可以看出,经过二次修复,算法的性能有较大的提升.



图12 篡改及二次修复图像

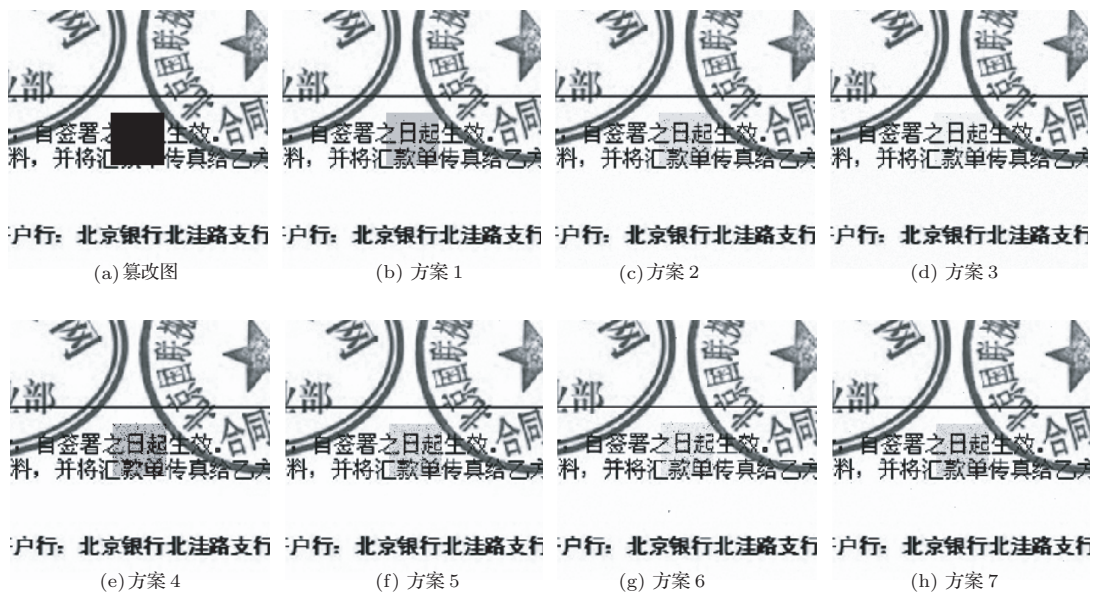


图13 简单图形的恢复

表3 PSNR 值对比

图像	方案1	方案2	方案3	方案4	方案5	方案6	方案7	文献 [25]	文献 [26]
Lena	48.82	44.46	41.32	55.91	54.17	50.52	48.95	44.82	41.97
Peppers	47.96	43.79	41.56	55.73	54.10	50.50	48.98	44.97	41.96
Woman	49.44	45.03	41.47	55.98	54.18	50.57	49.94	44.87	41.96

表4 首次和二次修复对比

参数	方案1	方案2	方案3	方案4	方案5	方案6	方案7
P_t	0.7315	0.7952	0.7917	0.5249	0.6523	0.6566	0.5451
P'_t	0.9048	0.9867	0.9998	0.7179	0.8990	0.9834	0.8759
P_r	0.9659	0.9584	0.9505	0.8982	0.8900	0.8661	0.8804
P'_r	0.9926	0.9896	0.9932	0.9287	0.9425	0.9333	0.9492

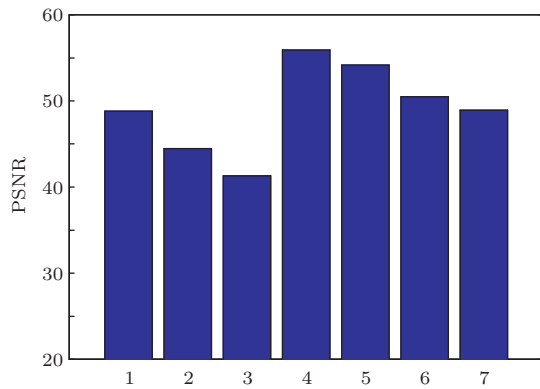


图14 Lena图7种编码方案的PSNR值

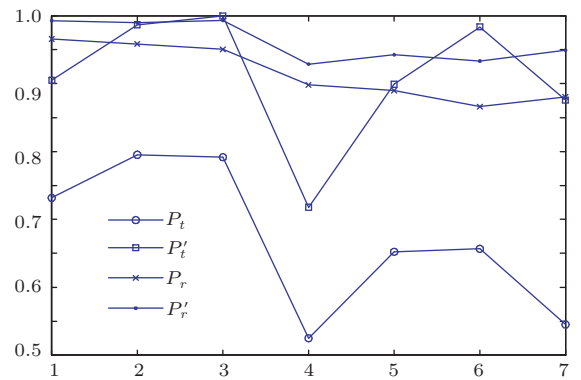


图15 首次和二次修复对比

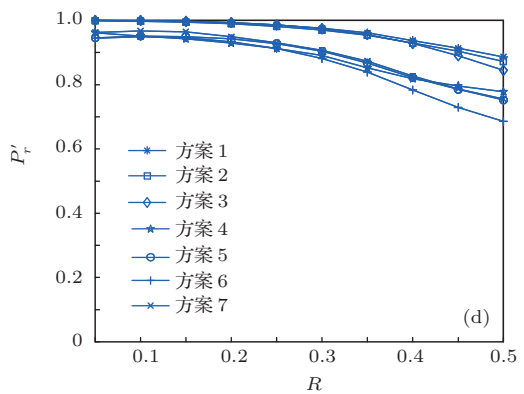
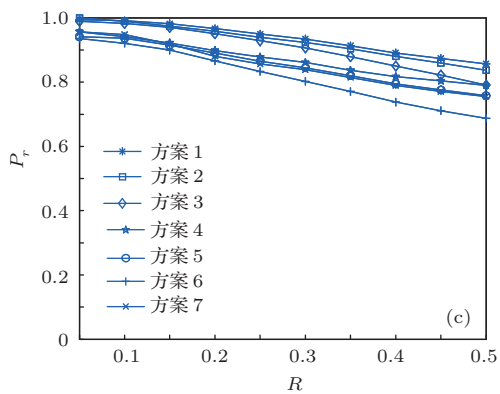
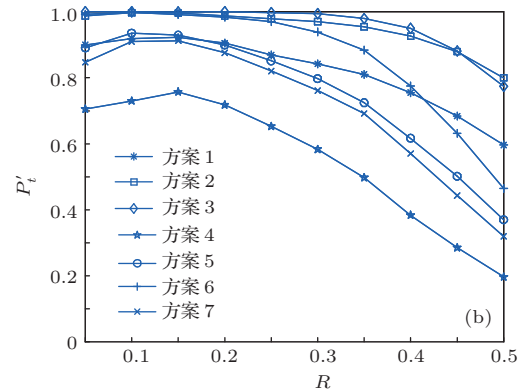
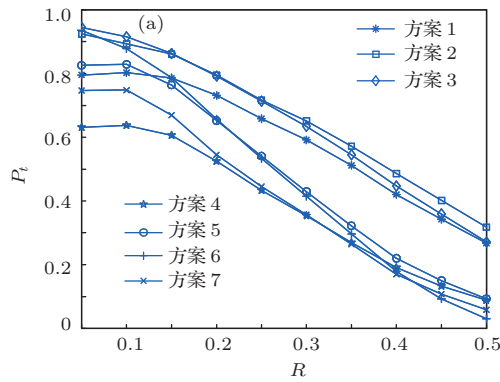


图16 篡改比例与算法性能的关系

把置0区域与原图长和宽的比值记为 R , 图16是 R 从1/20到1/2, P_t , P'_t , P_r , P'_r 的值. 从图16中可以看出, 对图像进行有限面积的篡改, 算法可以有效地进行检测和修复. 但随着篡改面积的扩大, 算法的性能随之下降.

6 结 论

本文提出了一种基于混沌映射和汉明码的数字图像篡改检测及修复算法. 实验证明, 在有限篡改的前提下, 使用汉明码对图像的高位进行编码, 可以在嵌入较少信息的情况下, 有效地对图像进行篡改定位和内容修复, 并通过二次修复进一步提高性能. 通过灵活的编码方案可以得到不同的性能, 应用于不同的场合. 通过混沌系统的使用, 保证了汉明码编组的随机性和系统的安全性. 该算法在数字图像保护及恢复领域具有较强的实用性.

参考文献

- [1] Redmill D W, Kingsbury N G 1996 *IEEE Trans. Image Process.* **5** 565
- [2] Wong P W, Memon N 2001 *IEEE Trans. Image Process.* **10** 1593
- [3] Khan A, Mirza A M 2007 *Inform. Fusion.* **8** 1566
- [4] Khan A, Tahir S F, Majid A, Choi T S 2008 *Pattern Recogn.* **41** 2594
- [5] Lu W, Sun W, Lu H T 2009 *Comput. Electr. Eng.* **35** 183
- [6] Ahmed F, Siyal M Y, Uddin Abbas V 2010 *Signal Process.* **90** 1456
- [7] Lin C Y, Chang S F 2001 *Proceedings of the Ninth ACM International Conference on Multimedia* Ottawa, ON, Canada, September 30–October 05, 2001 p628
- [8] Cheddad A, Condell J, Curran K, Mc Kevitt P 2010 *Signal Process.* **90** 727
- [9] Patra J C, Karthik A, Bornand C 2010 *Digit. Signal Process.* **20** 442
- [10] Fridrich J, Goljan M, Baldoza A C 2000 *Image Processing, 2000, Proceedings 2000 International Conference on* Vancouver, BC, Canada, September 10–13, 2000 p446
- [11] Cao J H, Li F T 2003 *Neural Networks and Signal Processing, 2003, Proceedings of the 2003 International Conference on* Nanjing, China, December 14–17, 2003 p1160
- [12] Kang L W, Leou J J 2006 *J. Vis. Commun. Image R.* **17** 876
- [13] Kim T 1992 *IEEE Trans. Image Process.* **1** 170
- [14] Lu C S 2002 *Multimedia Signal Processing, 2002 IEEE Workshop on* Thomas, Virgin Islands, USA, December 9–11, 2002 p316
- [15] Chamlawi R, Khan A, Idris A 2007 *J. Comput. Sci. Technol.* **22** 795
- [16] Wang S S, Tsai S L 2008 *Pattern Recogn.* **41** 701
- [17] Ma T D, Jiang W B, Fu J, Chai Y, Chen L P, Xue F Z 2012 *Acta Phys. Sin.* **61** 160506 (in Chinese)[马铁东, 江伟波, 浮洁, 柴毅, 陈立平, 薛方正 2012 物理学报 **61** 160506]
- [18] 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]
- [19] Fu J, Yu M, Ma T D 2011 *Chin. Phys. B* **20** 1674
- [20] 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]
- [21] 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]
- [22] Zhou W J, Yu M, Yu S M, 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]
- [23] Hamming R W 1950 *Bell Syst. Tech. J.* **29** 147
- [24] Li S J, Mou X Q, Cai Y L, Ji Z, Zhang J H 2003 *Comput. Phys. Commun.* **153** 52
- [25] Hung K M, Chen T W, Su W K, Kao C N 2012 *Information Science and Digital Content Technology (ICIDT), 2012 8th International Conference on* Jeju Island, South Korea, June 26–28, 2012 p730
- [26] Patra B, Patra J C 2012 *IEEE International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS 2012)* Tamsui, New Taipei City, Taiwan, November 4–7, 2012 p430

A novel image authentication and recovery algorithm based on chaos and Hamming code^{*}

Wang Xing-Yuan[†] Zhang Ji-Ming

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

(Received 29 August 2013; revised manuscript received 24 September 2013)

Abstract

In this article, we propose an image authentication and a recovery algorithm based on chaos and Hamming code. In this algorithm, the Hamming code that is widely used in the channel coding is used, the error control is applied to the image authentication and recovery, and the validity and security of the algorithm are ensured by chaotic mapping. Analytical and experimental results show that the algorithm has a good visual effect and an effectively tampering detection ability with less embedding authentication information, at the same time the algorithm can recover a tampered image to some extent.

Keywords: image authentication, image recovery, Hamming code, chaos

PACS: 07.05.Pj, 05.45.Gg

DOI: 10.7498/aps.63.020701

^{*} 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), Program for Liaoning Excellent Talents in University, China (Grant No. LR2012003), the National 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