Journal of Computer Applications
计算机应用,2015,35(10):2963-2968
ISSN 1001-9081
CODEN JYIIDU
2015-10-10
http://www.joca.cn

文章编号:1001-9081(2015)10-2963-06
doi:10.11772/j.issn.1001-9081.2015.10.2963

基于二维直方图移位的图像认证算法

王 兵*,毛 倩,苏栋骐
(上海理工大学 光电信息与计算机工程学院,上海 200093)
(*通信作者电子邮箱 wangbing6220@163.com)

摘 要:针对如何检测数字图像内容是否完整、有无篡改,提高认证图像质量的问题,提出了一种基于二维直方图移位的图像认证算法。首先,在棋盘格结构中利用两种预测差值计算方法构建原始图像的二维直方图,由预先设定的参数选择可嵌入信道,并确定可嵌入信道峰值点的位置,将可嵌入信道移位。然后结合直方图信息嵌入方法将认证信息嵌入到图像分块中。在篡改检测过程中采用分层篡改检测方法,有效提高篡改检测准确度。实验结果显示,该算法不仅可以抵抗噪声攻击,而且当参数设定为2和4时,认证图像的平均峰值信噪比(PSNR)分别为52.37 dB和50.33 dB,进一步提高了图像质量。实结果表明,所提算法安全性高,可实现可逆水印,并准确定位出篡改区域。

关键词:图像认证;预测差值;脆弱水印;二维直方图移位;篡改检测;分层检测
中图分类号:TP391.41 **文献标志码**:A

Image authentication agorithm based on two-dimensional histogram shifting

WANG Bing*, MAO Qian, SU Dongqi
(*School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai* 200093, *China*)

Abstract: In allusion to the problem that how to detect whether the digital image data is complete, and whether the image is tampered, an image authentication algorithm based on two-dimensional histogram shifting was proposed to improve the quality of the authentication image. Firstly, the two-dimensional histogram of the cover image was structured through two prediction difference value calculating methods. The embeddable channels were chosen by the preset parameters and the embeddable channel peak positions were determined and the embeddable channels were shifted. Then, the anthentication information was embedded into image blocks with histogram shifting method. Hierarchical tampering detection was adopted during the process of tamper detection to effectively improve the accuracy. The experimental results showed that the algorithm could resist noise attack, and the average Peak Signal-to-Noise Ratio (PSNR) of the authentication image was 52.37dB and 50.33dB respectively when the parameter was set as 2 and 4, which improves the quality of images. The resutls prove that the algorithm has high security, and it is able to implement reversible watermarking as well as precisely locationing the tampering region.

Key words: image authentication; prediction difference value; fragile watermarking; two-dimensional histogram shifting; tamper detection; hierarchical detection

0 引言

随着多媒体和网络技术的发展,数字图像的内容很容易受到恶意篡改,因此图像认证技术成为图像处理的一个重要研究课题。近年来,许多学者提出了不同的图像水印方法。根据水印的鲁棒性,这些方法可以分为鲁棒水印[1-3]和脆弱水印。鲁棒水印技术主要用于保护数字图像的所有权[4]1,这类技术需要从数字图像中提取认证数据来判断数字图像的所有者。因此,即使数字图像受到不同程度的篡改,认证数据也要保证完整地提取出来。

另一方面,脆弱水印技术主要用于图像认证中。根据认证数据检测数字图像内容的真实性和完整性,判断数字图像是否被恶意篡改[4]1。目前已经提出了很多用于图像认证算法的研究。文献[5]在位面上的随机排列以及合适的异或操作产生了一个随机的二进制图像,用此二进制图像来替换宿主图像的最低有效位,通过这个方式来完成二进制水印的嵌入。Lee等[6]采用了双重水印进行篡改检测和恢复。该算法将两种类型的水印嵌入到原始图像中,因此,一旦其中一种水印被破坏,还可以根据另一种水印恢复篡改图像。文献[7-8]将水印位嵌入到宿主图像中,以此来检测图像的真实性和完整性,而不需要存储额外的信息。文献[9]利用汉明码原理生成校验位,并根据环面自同构原理[10]将校验位嵌入到其他灰度值中,从而得到水印图像。文献[11]提出了一种基于混沌映射[12]的篡改检测算法,该算法使用分层水印和最低有效位(Least Significant Bit, LSB)嵌入原理提高篡改检测率。在2014年,Lo等[13]提出了基于预测差值直方图移位的图像认证算法。该算法先对图像分块,利用直方图移位的信息隐藏方法将认证信息嵌入到原始图像中,进而得到认证图像。

收稿日期:2015-04-14;**修回日期**:2015-07-03。

作者简介:王兵(1989-),女,山东聊城人,硕士研究生,主要研究方向:图像认证; 毛倩(1978-),女,山东烟台人,博士,主要研究方向:图像处理、信息理论与编码; 苏栋骐(1990-),男,上海人,硕士研究生,主要研究方向:信号与信息处理。

该文献算法能保证较好的图像视觉质量,并能检测出篡改区域;在图像没有被篡改的前提下,能准确恢复出原始图像。

在上述研究的基础上,本文提出了一种基于二维直方图移位的数字图像认证方案。在棋盘格结构中运用信息隐藏技术将水印嵌入到原始图像中,能够有效减少对图像灰度值的修改量,并提高篡改检测率。

1 相关的图像隐藏方案

假设原始图像 X 的大小为 $M \times M$,每个灰度值的大小为 $X_{i,j} \in [0,255](1 \leqslant i \leqslant M,1 \leqslant j \leqslant M)$。

1.1 文献[14]方案

2010年,文献[14]提出了一种基于交叉预测差值直方图移位的可逆信息隐藏方案。在提到的方案中,其中一种预测方法是基于棋盘格结构的,如图1所示。在棋盘格结构中,首先使用式(1)计算白色像素的预测差值,然后再计算黑色像素的预测差值。也就是说,原始图像中的每一灰度值与其上、下、左、右四个相邻灰度值的平均值之间的差值即为该像素的预测差值。

$$D_{i,j} = X_{i,j} - \left\lfloor \frac{X_{i,j-1} + X_{i,j+1} + X_{i-1,j} + X_{i+1,j}}{4} \right\rfloor \tag{1}$$

其中:$\lfloor A \rfloor$ 表示小于等于 A 的最大整数。

1.2 文献[15]方案

2013年,文献[15]提出了一种基于分块预测的直方图可逆信息隐藏方案。在此方案中,原始图像按 $w \times w$ 大小进行不重叠分块,以 2×2 的图像分块为例,如图2(a)所示,将每一个图像分块分为 E_1、E_2、E_3、E_4 四类,对于每一类 $E_i(1 \leqslant i \leqslant 4)$ 的预测差值均为 X_i 与其周围相邻的八个灰度值(图2(b))的平均值之间的差值,如式(2)所示:

$$D_{i,j} = X_{i,j} - \left\lfloor \frac{\sum_{s=-1}^{1}\sum_{t=-1}^{1} X_{i+s,j+t}}{|\{X_{i+s,j+t} \mid -1 \leqslant s \leqslant 1, -1 \leqslant t \leqslant 1\}|} \right\rfloor \tag{2}$$

其中:$|B|$ 表示与 B 相邻的灰度值的个数。

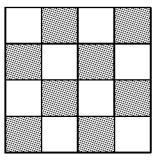
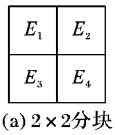
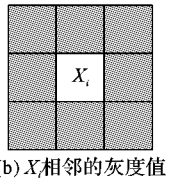


图1 棋盘格结构



(a) 2×2分块



(b) X_i相邻的灰度值

图2 交叉预测结构

1.3 文献[16]方案

2013年,文献[16]在图像隐藏方案中构建了二维直方图。该文献中,用两种差值预测方法计算每一个灰度值的残差值,用 (e_1,e_2) 表示。然后构建残差图像的二维直方图 $H(e_1,e_2)$,二维直方图中有不同的通道分布,如图3所示。其中 $c = e_1 - e_2$ 将二维直方图划分为不同的通道 $c = \cdots, -3, -2, -2,0,1,2,3,\cdots$。每一个通道都类似于一维的直方图 $H_c(e_1,e_2)$,在这些通道中,往往有较高峰值点的通道具有很好的信息嵌入效果,因此这类的通道被选为可嵌入信道(Embeddable Channel, EC)。为了方便区分,将信道 c 的绝对值越小的信道规定为"低信道",也就是说,低信道所在的位置更接近直线 $e_1 = e_2$,而"高信道"所在的位置则距离直线 $e_1 = e_2$ 越远。低信道具有很好的嵌入效果,因此引入一个参数 c_b,用来选择二维直方图中可嵌入信道 EC,而且 $c \in [-c_b, c_b]$。例如,$c_b = 2$,那么信道 -2、-1、0、1、2 均为可嵌入信道 EC。

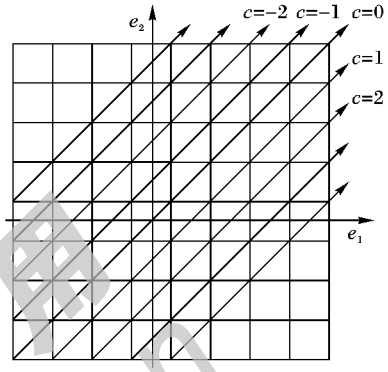


图3 二维直方图的定义

2 本文的图像认证算法

本文利用直方图移位的原理将认证信息嵌入到原始图像中,从而达到检测数字图像是否被篡改的目的。如果认证图像未被篡改,那么根据直方图移位算法的逆运算可恢复出原始图像。

2.1 认证信息嵌入过程

假设原始图像大小为 $M \times M$,$X_{i,j}$ 表示位于 (i,j) 的原始图像灰度值,$X'_{i,j}$ 表示位于 (i,j) 的经预测计算之后的灰度值。每个灰度值的大小为 $X_{i,j}(X_{i,j} \in [0,255],1 \leqslant i \leqslant M,1 \leqslant j \leqslant M)$。$D_{i,j}$ 和 $D'_{i,j}$ 分别表示位于 (i,j) 的预测差值和被嵌入信息之后的预测差值。在信息嵌入算法中,位于白色像素块的灰度值由步骤2 ~ 9进行预测和计算;那么,位于黑色像素块的灰度值由步骤10 ~ 12进行预测和计算。认证信息嵌入算法的具体步骤如下:

步骤1 首先将原始图像的灰度值划分为棋盘格结构,为了方便区分,将白色像素块和黑色像素块分别定义为"半平面 C_1"和"半平面 C_2";并且将原始图像按 4×4 大小进行不重叠分块,分块总数为 $(M \times M)/16$。

步骤2 设定两个种子 S_w 和 S_b,利用伪随机数生成器得到 $(M \times M)/16$ 个随机数 v。使用式(3)将每一个随机数 v 转换为二进制数 n[13]。

$$n = v \bmod 2 \tag{3}$$

步骤3 对于每一个灰度值 $X_{i,j} \in C_1$,分别使用式(1)、(2)计算该灰度值的预测差值。用 d_{w1} 表示由式(1)计算得到的预测差值,用 d_{w2} 表示由式(2)计算得到的预测差值,那么灰度值 $X_{i,j}$ 的残差值对为 (d_{w1},d_{w2}),$d_{w1} \in [-255,255]$,$d_{w2} \in [-255,255]$。

步骤4 构建半平面 C_1 残差值的二维直方图 $H(d_{w1},$

d_{w2})。

步骤 5　由 $c = d_{w1} - d_{w2}$ 将二维直方图 $H(d_{w1}, d_{w2})$ 划分为多个不同的一维直方图 $H_c(d_{w1}, d_{w2})$,并选择可嵌入信道 EC。

步骤 6　对每一个可嵌入信道 EC,从 $H_c(d_{w1}, d_{w2})$ 中找到具有直方图分布值最大的两个峰值点,确定两个峰值点的位置($P_{w1}, P_{w1} - c$) 和($P_{w2}, P_{w2} - c$),并且满足 $P_{w1} < P_{w2}$。

步骤 7　对每一个可嵌入信道 EC,按如下步骤进行平移:

1) 如果 $d_{w2} = d_{w1} - c$ 且 $d_{w1} < P_{w1}$,那么满足 $d_{w1} \in [-255, P_{w1} - 1]$,$d_{w2} \in [-255, P_{w1} - c - 1]$ 的一维直方图 $H_c(d_{w1}, d_{w2})$ 向左平移一个单位。也就是说,灰度值 $X_{i,j}$ 的两个预测差值 d_{w1} 和 d_{w2} 分别对应减 1,即 $d'_{w1} = d_{w1} - 1$,$d'_{w2} = d_{w2} - 1$。

2) 如果 $d_{w2} = d_{w1} - c$ 且 $d_{w1} > P_{w2}$,那么满足 $d_{w1} \in [P_{w2} + 1, 255]$,$d_{w2} \in [P_{w2} - c + 1, 255]$ 的一维直方图 $H_c(d_{w1}, d_{w2})$ 向右平移一个单位。也就是说,灰度值 $X_{i,j}$ 的两个预测差值 d_{w1} 和 d_{w2} 分别对应加 1,即 $d'_{w1} = d_{w1} + 1$,$d'_{w2} = d_{w2} + 1$。

步骤 8　将步骤 2 由种子 S_w 得到的认证信息 n_w 依次嵌入到每一个 4 × 4 大小的图像分块中,即一个比特位的认证信息嵌入到一个 4 × 4 大小的子块中。对于每一个可嵌入信道 EC,具体嵌入过程如下:

1) 如果 4 × 4 大小的图像子块中的灰度值 $X_{i,j}$ 的预测差值满足 $d_{w1} = P_{w1}$,$d_{w2} = P_{w1} - c$,那么满足条件的所有残差值的变化如下:$d'_{w1} = d_{w1} - n_w$,$d'_{w2} = d_{w2} - n_w$。

2) 如果 4 × 4 大小的图像子块中的灰度值 $X_{i,j}$ 的预测差值满足 $d_{w1} = P_{w2}$,$d_{w2} = P_{w2} - c$,那么满足条件的所有残差值的变化如下:$d'_{w1} = d_{w1} + n_w$;$d'_{w2} = d_{w2} + n_w$。

步骤 9　使用式(4) 将预测差值转换为灰度值:

$$X'_{i,j} = d'_{w1} + \left\lfloor \frac{X_{i,j-1} + X_{i,j+1} + X_{i-1,j} + X_{i+1,j}}{4} \right\rfloor \tag{4}$$

步骤 10　对于每一个灰度值 $X_{i,j} \in C_2$,分别使用式(5) ~ (6) 计算该灰度值的预测差值 d_{b1} 和 d_{b2}:

$$d_{b1} = D_{i,j} = X'_{i,j} - \left\lfloor \frac{X'_{i,j-1} + X'_{i,j+1} + X'_{i-1,j} + X'_{i+1,j}}{4} \right\rfloor \tag{5}$$

$$d_{b2} = D_{i,j} = X'_{i,j} - \left\lfloor \frac{\sum_{s=-1}^{1} \sum_{t=-1}^{1} X'_{i+s,j+t}}{|\{X'_{i+s,j+t} \mid -1 \leqslant s \leqslant 1, -1 \leqslant t \leqslant 1\}|} \right\rfloor \tag{6}$$

其中:$\lfloor A \rfloor$ 表示小于等于 A 的最大整数,$|B|$ 表示与 B 相邻的灰度值的个数。

步骤 11　将步骤 2 由种子 S_b 得到的认证信息 n_b 依次嵌入到每一个 4 × 4 大小的图像分块中,嵌入过程如步骤 4 ~ 9。每一个可嵌入信道 EC 的两个峰值点分别为($P_{b1}, P_{b1} - c$) 和($P_{b2}, P_{b2} - c$)。

步骤 12　输出认证图像,半平面 C_1 和 C_2 的每一个可嵌入信道的峰值点,S_w,S_b。

以图 4 为例,假设原始图像为 8 × 8,那么原始图像可分为 4 个 4 × 4 大小的子块。首先,计算半平面 C_1 中的灰度值 $X_{i,j}$ 的预测差值。例如,位于(2,2) 的灰度值 $X_{2,2}$ 的预测差值 d_{w1} 为:

$$d_{w1} = D_{2,2} = X_{2,2} - \left\lfloor \frac{X_{1,2} + X_{2,1} + X_{2,3} + X_{3,2}}{4} \right\rfloor = 1$$

同样,预测差值 d_{w2} 为:

$$d_{w2} = X_{2,2} - \left\lfloor \frac{X_{1,1} + X_{1,2} + X_{1,3} + X_{2,1} + X_{2,3} + X_{3,1} + X_{3,2} + X_{3,3}}{8} \right\rfloor = 0$$

因此,$X_{2,2}$ 相应的预测差值对为(1,0)。图 5 给出了半平面 C_1 的所有灰度值的预测差值 d_{w1} 和 d_{w2}。表 1 则给出了不同的预测差值对(d_{w1}, d_{w2}) 出现的次数。根据表 1 各个不同的 (d_{w1}, d_{w2}) 出现的次数,可构建出二维直方图 $H(d_{w1}, d_{w2})$,如图 6 所示。根据 $c = d_{w1} - d_{w2}$,从图 6 可看出,残差值对(d_{w1}, d_{w2}) 主要分布在信道 $c = -1, 0, 1$ 中。选择信道 0 为可嵌入信道,信道 0 对应的一维直方图 $H_0(d_{w1}, d_{w2}) = \{\cdots, 1, 2, 8, 7, 6, 0, \cdots\}$,那么可嵌入信道 0 的两个峰值点分别为(0,0) 和(1,1)。信道 0 经移位操作后的二维直方图如图 7 所示。经平移之后,可嵌入信道 0 中的(-1,-1) 和(2,2) 个数变为 0。那么在等于(0,0) 或(1,1) 的预测差值上嵌入认证信息。因为原始图像被分为 4 个图像子块,所以假设认证信息为 $Y = 1101_{(2)}$,那么经平移嵌入之后的预测差值 d'_{w1} 和 d'_{w2} 如图 8 所示。

表 1　半平面 C_1 预测差值对(d_{w1}, d_{w2}) 出现的次数

(d_{w1}, d_{w2})	次数	(d_{w1}, d_{w2})	次数
(0,0)	8	(2,2)	6
(0,-1)	3	(3,2)	2
(1,0)	2	(3,3)	0
(1,1)	7	(-1,-1)	2
(1,2)	1	(-2,-2)	1

5	6	5	7	6	4	5	7
4	5	3	6	5	6	6	7
7	6	4	3	5	5	7	6
6	6	5	7	4	4	5	4
7	7	8	6	6	5	6	5
7	6	6	8	5	4	4	5
8	8	7	6	5	4	3	3
5	4	5	4	3	3	4	3

图 4　原始图像

0		0		1		0	
	1		2		1		1
2		0		1		2	
	0		3		0		-1
1		2		1		2	
	-1		3		0		1
2		1		1		0	
	-2		0		0		0

(a) 半平面C_1的预测差值d_{w1}

0		0		1		-1	
	0		2		1		1
2		0		0		2	
	0		2		-1		-1
1		2		1		2	
	-1		2		0		1
2		2		1		0	
	-2		-1		0		0

(b) 半平面C_1的预测差值d_{w2}

图 5　预测差值

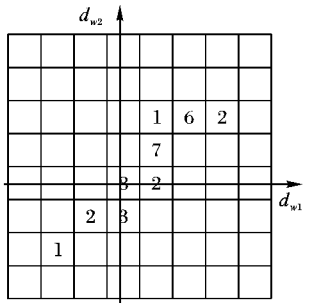


图6 由表1得到的二维直方图

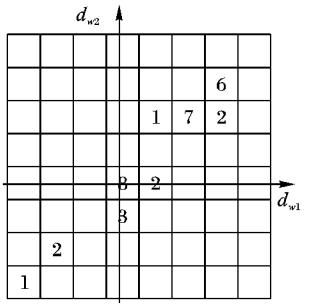


图7 信道0移位后的二维直方图

-1	-1	2	0				
	1	3	2	2			
3	-1	1	3				
	-1	3	0	-2			
1	3	2	3				
	-2	3	-1	2			
3	1	2	-1				
	-3	0	-1	-1			

(a) 经平移嵌入后的预测差值d'_{w1}

-1	-1	2	-1				
	0	3	2	2			
3	-1	0	3				
	-1	2	-1	-2			
1	3	2	3				
	-2	2	-1	2			
3	2	2	-1				
	-3	-1	-1	-1			

(b) 经平移嵌入后的预测差值d'_{w2}

图8 经平移嵌入后的预测差值

2.2 篡改检测过程

将认证信息嵌入到原始图像后，可以检测及定位出认证图像被篡改区域。在篡改检测算法中，需要已知参数 c_b，原始图像的残差图像二维直方图的可嵌入信道 c 的峰值点坐标 $(P_{w1},P_{w1}-c)$，$(P_{w2},P_{w2}-c)$，$(P_{b1},P_{b1}-c)$，$(P_{b2},P_{b2}-c)$ 和随机数种子 S_w、S_b。假设接收到的图像大小为 $M\times M$，每个灰度值的大小为 $Y_{i,j}\in[0,255](1\leqslant i\leqslant M,1\leqslant j\leqslant M)$。接收到的图像将由粗略到精细分两个层次进行篡改检测。第一层篡改检测算法如下：

步骤1 首先将接收图像的灰度值划分为棋盘格结构，同样将白色像素块和黑色像素块分别为“半平面 C_1”和“半平面 C_2”；并且将接收图像按 4×4 大小进行不重叠分块，分块总数为 $(M\times M)/16$。

步骤2 根据随机数种子 S_w、S_b 以及式(3)得到 $(M\times M)/16$ 个认证信息 n_w、n_b。

步骤3 分别利用式(1)～(2)得到半平面 C_2 的预测差值 d_{b1} 和 d_{b2}，并构建二维直方图 $H'(d_{b1},d_{b2})$。

步骤4 利用认证信息 n_b 依次检测图像子块，具体检测过程如下：

1) 如果 $n_b=1$，对应图像子块中的灰度值 $Y_{i,j}$ 的残差值对 (d_{b1},d_{b2}) 等于 $(P_{b1},P_{b1}-c)$ 或 $(P_{b2},P_{b2}-c)$，那么该图像子块被篡改；否则，图像子块未被篡改。

2) 如果 $n_b=0$，对应图像子块中的灰度值 $Y_{i,j}$ 的残差值对 (d_{b1},d_{b2}) 等于 $(P_{b1}-1,P_{b1}-c-1)$ 或 $(P_{b1}+1,P_{b1}-c+1)$，那么该图像子块被篡改；否则，图像子块未被篡改。

在这里，用灰色的块表示未被篡改的像素值，用白色的块表示已被篡改的像素值。当检测出图像子块中的任意一个灰度值被篡改时，该 4×4 大小的图像子块全部变为白色。

接下来根据直方图移位的逆运算，恢复半平面 C_2 的全部灰度值。

步骤5 对二维直方图 $H'(d_{b1},d_{b2})$ 进行平移，对于每一个可嵌入信道 EC：

1) 如果 $d_{b2}=d_{b1}-c$ 且 $d_{b1}<P_{b1}-1$，那么满足 $d_{b1}\in[-255,P_{b1}-2]$，$d_{b2}\in[-255,P_{b1}-c-2]$ 的一维直方图 $H'_c(d_{b1},d_{b2})$ 向右平移一个单位，那么恢复出的 $Y'_{i,j}$ 为 $Y'_{i,j}=Y_{i,j}+1$。

2) 如果 $d_{b2}=d_{b1}-c$ 且 $d_{b1}>P_{b2}+1$，那么满足 $d_{b1}\in[P_{b1}+2,255]$，$d_{b2}\in[P_{b2}-c+2,255]$ 的一维直方图 $H'_c(d_{b1},d_{b2})$ 向左平移一个单位，那么恢复出的 $Y'_{i,j}$ 为，$Y'_{i,j}=Y_{i,j}-1$。

步骤6 对于每一个 4×4 图像子块，如果其对应的认证信息为 $n_b=0$，那么该图像子块中的灰度值 $Y_{i,j}$ 均保持不变；如果其对应的认证信息为 $n_b=1$，那么：

1) 如果图像子块的灰度值 $Y_{i,j}$ 的预测差值对为 $(P_{b1}-1,P_{b1}-c-1)$，那么 $Y'_{i,j}=Y_{i,j}+1$。

2) 如果图像子块的灰度值 $Y_{i,j}$ 的预测差值对为 $(P_{b1}+1,P_{b1}-c+1)$，那么 $Y'_{i,j}=Y_{i,j}-1$。

步骤7 对于每一个灰度值 $Y_{i,j}\in C_1$，分别使用式(7)～(8)计算该灰度值的预测差值 d_{w1} 和 d_{w2}，并且构建半平面 C_1 的二维直方图。

$$d_{w1}=D_{i,j}=Y'_{i,j}-\left\lfloor\frac{Y'_{i,j-1}+Y'_{i,j+1}+Y'_{i-1,j}+Y'_{i+1,j}}{4}\right\rfloor \tag{7}$$

$$d_{w2}=D_{i,j}=Y'_{i,j}-\left\lfloor\frac{\sum_{s=-1}^{1}\sum_{t=-1}^{1}Y'_{i+s,j+t}}{|\{Y'_{i+s,j+t}\mid -1\leqslant s\leqslant 1,-1\leqslant t\leqslant 1\}|}\right\rfloor \tag{8}$$

步骤8 利用认证信息 n_w 依次检测图像子块，具体检测过程如下：

1) 如果 $n_w=1$，对应图像子块中的灰度值 $Y_{i,j}$ 的残差值对 (d_{w1},d_{w2}) 等于 $(P_{w1},P_{w1}-c)$ 或 $(P_{w2},P_{w2}-c)$，那么该图像子块被篡改；否则，图像子块未被篡改。

2) 如果 $n_w=0$，对应图像子块中的灰度值 $Y_{i,j}$ 的残差值对 (d_{w1},d_{w2}) 等于 $(P_{w1}-1,P_{w1}-c-1)$ 或 $(P_{w2}+1,P_{w2}-c+1)$，那么该图像子块被篡改；否则，图像子块未被篡改。

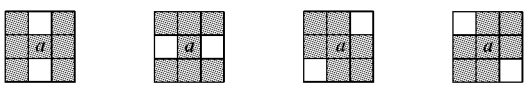
由于存在被篡改的认证图像的残差值与原始图像的残差值相同的可能性，导致一些被篡改的灰度值无法被检测出来，因此还要反复检测由以上步骤检测出来的篡改图像。文献[8]提出了多次检测的方案。假设图9中的灰度值 a 代表需要被进一步检测的灰度值，第二层篡改检测步骤如下：

步骤1 如果与灰度值 a 相邻的上、下两个灰度值均为白色的块(表示已被篡改)，那么灰度值 a 也要改为白色的块，如图9(a)所示。

步骤2 如果与灰度值 a 相邻的左、右两个灰度值均为白色的块，那么灰度值 a 也要改为白色的块，如图9(b)所示。

步骤3 如果与灰度值 a 相邻的右上、左下两个灰度值均为白色的块，那么灰度值 a 也要改为白色的块，如图9(c)所示。

步骤4 如果与灰度值 a 相邻的左上、右下两个灰度值均为白色的块，那么灰度值 a 也要改为白色的块，如图9(d)所示。



(a) 第一种情况 (b) 第二种情况 (c) 第三种情况 (d) 第四种情况

图9 第二层篡改检测四种情况

在每一轮检测中,记录需要修改的灰度值 a 的个数,如果 a 的个数大于等于1,那么继续第二层篡改检测的4个步骤;如果 a 的个数为0,那么终止检测[8]。

2.3　恢复图像

如果经上述检测过程检测的认证图像没有被篡改,那么可以利用直方图移位的逆运算恢复出原始图像,半平面 C_2 和 C_1 恢复过程如同2.2节介绍的步骤1 ~ 6,步骤4除外。

2.4　上溢和下溢的解决方案

经认证信息嵌入操作之后,半平面 C_1 和 C_2 中的每一个灰度值的大小可能会加1或减1。如果原始图像的灰度值为0或255,那么在认证图像中,它们可能会改变为 -1 或256。因此为了防止出现上溢和下溢的问题,文献[15]提出了预处理操作。如果原始图像的灰度值等于0或255,那么将它们改为1或254,因此,需要用一个标记位来区别原始图像的灰度值1和254。如果灰度值1或254是由0或255转换的,那么标记位设为0;否则,标记位设为1。因此在恢复图像过程中,可根据标记位将1或254恢复为原来的值[15]9。

3　实验结果分析

本文算法在 Matlab 平台上进行了实验,选取大小为256×256的不同灰度图像作为实验图像。本文方法和文献[13]方法的认证图像见图10。在仿真实验过程中,图像分块大小为4×4。

3.1　图像质量分析

基于直方图移位的信息嵌入算法保证了每一个灰度值的变化量为±1,因此认证图像具有较好的视觉效果。通常用峰值信噪比(Peak Signal-to-Noise Ratio, PSNR)来衡量认证图像的图像质量,其值越高,表示图像视觉效果越好。*PSNR* 的计算公式如(9)所示:

$$PSNR = 10 \times \lg \frac{255^2}{MSE} \tag{9}$$

其中:*MSE*(Mean Square Error)表示原始图像与认证图像灰度值的均方误差。对于大小为256 × 256的灰度图像,*MSE* 定义如下:

$$MSE = \frac{1}{256 \times 256} \sum_{i=1}^{256} \sum_{j=1}^{256} (x_{i,j} - x'_{i,j})^2 \tag{10}$$

其中:$x_{i,j}$ 和 $x'_{i,j}$ 分别表示原始图像和认证图像的灰度值。

表2给出了 Cameraman 和 Peppers 两幅实验图像的关于本文算法、文献[9]、文献[11]和文献[13]四种方法嵌入认证信息的图像 *PSNR* 和 *MSE* 值的比较,从表2可看出,本文算法和文献[11]随着参数 c_h 和 k 的增加,*PSNR* 的值也随着减小。但是本文算法 *PSNR* 的值普遍优于其他三种方案。

表2　实验图像的 *PSNR* 和 *MSE* 值比较

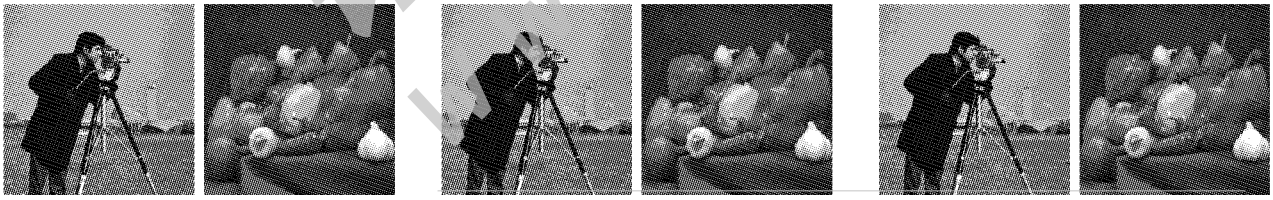
方法	参数	Cameraman		Peppers	
		MSE	*PSNR*/dB	*MSE*	*PSNR*/dB
本文方法	$c_h=2$	0.37	52.44	0.38	52.32
	$c_h=4$	0.64	50.13	0.58	50.52
文献[13]方法	$k=1$	0.47	51.43	0.45	51.62
	$k=2$	0.85	48.83	0.84	48.9
文献[9]方法		5.46	51.62	5.50	40.73
文献[11]方法		5.47	40.75	5.57	40.67

3.2　检测结果分析

3.2.1　噪声攻击

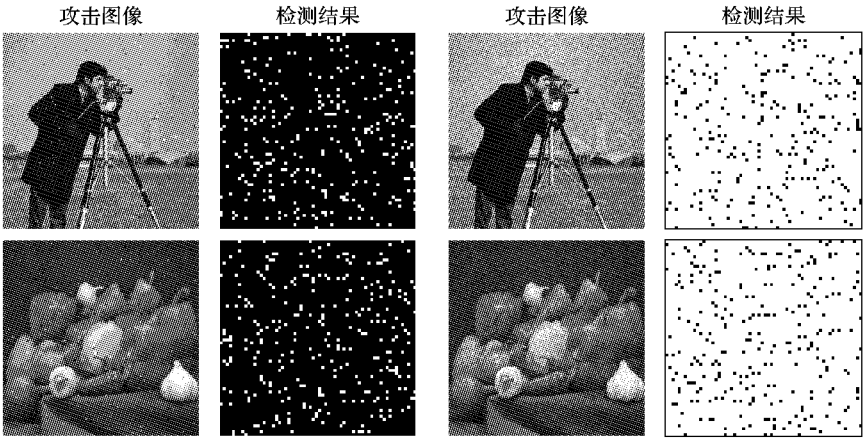
本实验对图10(b)认证图像进行了椒盐噪声和高斯噪声攻击,利用本文方法对攻击图像进行检测。实验结果显示,本文方法对于噪声攻击是鲁棒的。

图11为椒盐噪声攻击和高斯噪声攻击的 Cameraman 和



(a) 原始图像　(b) 本文方法的认证图像　(b) 文献[13]方法的认证图像

图10　原始图像和认证图像



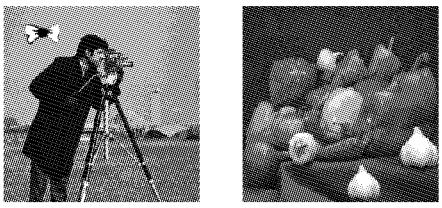
(a) 椒盐噪声攻击　(b) 高斯噪声攻击

图11　椒盐噪声攻击

Peppers 图像检测结果。

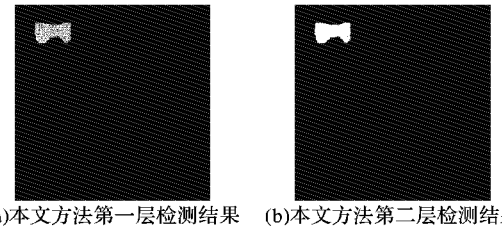
3.2.2 恶意篡改

图 12 是对认证图像进行不同程度的篡改图片。图 13 ~ 14 给出了分层篡改检测的检测结果,其中白色区域为标记的篡改区域,黑色区域为标记的完好区域。从图 13 ~ 14 中可以看,本文方法检测结果比文献[13]方法更加精确。

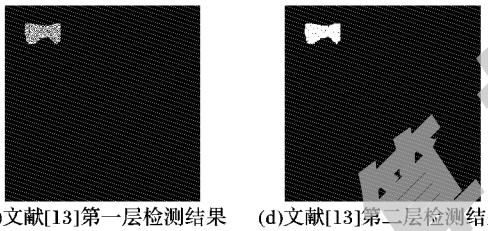


(a) Cameraman (b) Peppers

图 12 篡改图像

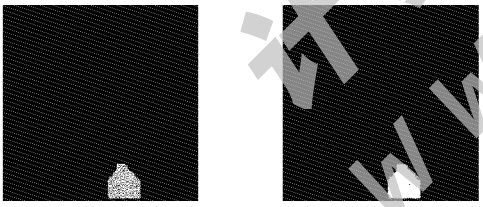


(a)本文方法第一层检测结果 (b)本文方法第二层检测结果

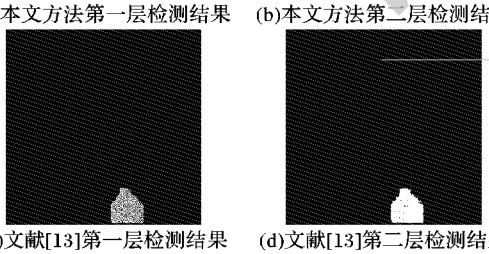


(c)文献[13]第一层检测结果 (d)文献[13]第二层检测结果

图 13 Cameraman 篡改检测结果



(a)本文方法第一层检测结果 (b)本文方法第二层检测结果



(c)文献[13]第一层检测结果 (d)文献[13]第二层检测结果

图 14 Peppers 篡改检测结果

4 结语

本文在分析了基于交叉预测差值直方图移位的信息隐藏的基础上,提出了一种基于二维直方图移位的图像篡改检测算法,利用直方图移位的信息隐藏的算法将认证信息嵌入原始图像,从而达到检测篡改图像的目的。本文算法不仅可用于棋盘格结构,也可用于其他预测结构。通过实验结果表明:基于二维直方图移位的图像认证算法能有效提高图像的 PSNR 值,图像的灰度值改变量维持在 ±1,因此认证图像具有较好的视觉效果。同时本文算法能有效提高图像篡改检测率,从而很好地实现图像内容完整性认证功能。

参考文献:

[1] LIN C. A robust image authentication method distinguishing JPEG compression from malicious manipulation[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2001, 11(2): 153--168.

[2] YANG S, XU C, ZHANG S. Combinational image watermarking in the spatial and frequency domains[J]. Pattern Recognition, 2003, 36(4): 969 - 975.

[3] KIM Y W, OH I S. Watermarking text document images using edge direction histograms[J]. Pattern Recognition Letters, 2004, 25(11): 1243 - 1251.

[4] CHAN C, CHANG C. An efficient image authentication method based on Hamming code[J]. Pattern Recognition, 2007, 40(2): 681 - 690.

[5] LU H, SHEN R, CHUNG F L. Fragile watermarking scheme for image authentication[J]. Electronics Letters, 2003, 39(12): 898 - 900.

[6] LEE T, LIN S. Dual watermark for image tamper detection and recovery[J]. Pattern Recognition, 2008, 41(11): 3497 - 3506.

[7] YUAN H, ZHANG X. Multiscale fragile watermarking based on the Gaussian mixture model[J]. IEEE Transactions on Image Processing, 2006, 15(10): 3189 - 3200.

[8] CHUANG J, HU Y. An adaptive image authentication scheme for vector quantization compressed image[J]. Journal of Visual Communication and Image Representation, 2011, 22(5): 440 - 449.

[9] CHAN C. An image authentication method by applying Hamming code on rearranged bits[J]. Pattern Recognition Letters, 2011, 40(2): 1679 - 1690.

[10] GEORGE V, IONNIS P. Chaotic mixing of digital images and applications to watermarking[C]// Proceedings of the 1996 European Conference on Multimedia Applications, Services and Techniques. Louvain-La-Neuve: [s. n.], 1996: 687 - 695.

[11] TONG X, LIU Y, ZHANG M, *et al.* A novel chaos-based fragile watermarking for image tampering detection and self-recovery[J]. Signal Processing: Image communication, 2013, 28(3): 301 - 308.

[12] WANG L, YE Q, XIAO Y, *et al.* An image encryption scheme based on cross chaotic map[C]// CISP 2008: Proceedings of the 2008 Congress on Image and Signal Processing. Piscataway: IEEE Press, 2008: 22 - 26.

[13] LO C C, HU Y C. A novel reversible image authentication scheme for digital images[J]. Signal Processing, 2014, 98(5): 174 - 185.

[14] YANG C, TSAI M H. Improving histogram-based reversible data hiding by interleaving predictions[J]. IET Image Processing, 2010, 4(4): 223 - 234.

[15] HSU F, WU M, YANG C, *et al.* Image reversibility in data embedding on the basis of blocking-predictions[J]. Peer-to-Peer Networking and Applications, 2014, 7(4): 723 - 736.

[16] WANG S, LI C, KUO W. Reversible data hiding based on two-dimensional prediction errors[J]. IET Image Processing, 2013, 7(9): 805 - 816.