DOI：10. 13471/j. cnki. acta. snus. ZR20240175

基于IPVO的高效图像可逆认证方法*

张汉华[1]，黄方军[1,2]

1. 中山大学计算机学院，广东 广州 510006
2. 中山大学网络空间安全学院，广东 深圳 518107

摘　要：提出了一种基于小波域预测误差直方图平移的图像可逆认证方法。首先，对待认证图像进行一次哈尔小波变换；其次，将变换得到的低频子带和高频子带分别分块，并根据块内的系数值和块的位置生成认证码；然后，使用改进的像素值排序（IPVO）方法将认证码嵌入到分块中，通过哈尔小波逆变换得到包含认证信息的图像；在认证阶段，通过对比分块提取认证码和生成认证码来实现篡改检测功能，并可无损地恢复原始图像。实验结果表明，该方法提供了更准确的检测结果，并确保了一定水平的图像质量。

关键词：图像；可逆认证；脆弱水印；篡改检测

中图分类号：TP391　　**文献标志码：**A　　**文章编号：**2097－0137（2024）05－0106－09

Efficient image reversible authentication method based on IPVO

ZHANG Hanhua[1]，*HUANG Fangjun*[1,2]

1. School of Computer Science and Engineering，Sun Yat-sen University，Guangzhou 510006，China
2. School of Cyber Science and Technology，Sun Yat-sen University，Shenzhen 518107，China

Abstract：A reversible image authentication method based on wavelet-domain prediction error histogram translation is proposed. First，the image to be authenticated performs a Haar wavelet transform. Second，the low-frequency and high-frequency subbands obtained from the transform are separately partitioned into blocks，and an authentication code is generated based on the coefficient values and locations of these blocks. Then，the authentication code is embedded into the blocks using the improved pixel value ordering（IPVO）method，and the image containing the authentication information is reconstructed using the Haar wavelet inverse transform. In the authentication stage，the tampering detection function is realized by extracting the authentication code and generating the authentication code. If the image is not tampered with，the original image can be recovered losslessly. Experimental results show that the method provides more accurate detection results and ensures a certain level of image quality.

Key words：image；reversible authentication；fragile watermarking；tamper detection

随着计算机技术的发展，对图像和视频进行篡改变得越来越容易。为了实现对图像的保护，密码保护、脆弱水印是一种较为常见的认证方法。但脆弱水印采用有损嵌入方式，会导致原始图像

* **收稿日期：**2024－05－25　　**录用日期：**2024－06－19　　**网络首发日期：**2024－07－12
基金项目：国家自然科学基金（U2336208，62072481）
作者简介：张汉华（1995年生），男；**研究方向：**可逆信息隐藏和图像认证；
E-mail：zhanghh73@mail2.sysu.edu.cn
通信作者：黄方军（1973年生），男；**研究方向：**人工智能安全和多媒体安全；
E-mail：huangfj@mail.sysu.edu.cn

的某些信息丢失。与脆弱水印不同，可逆信息隐藏技术的独特之处在于，在嵌入了信息后，原始载体可以被完全还原，且嵌入的信息可以被准确提取。图像可逆认证结合了可逆信息隐藏的数字水印技术，在数字版权保护、医学影像和司法取证等领域都具有重要意义。

对于空域中未经压缩的图像，目前主要采用三种可逆信息隐藏策略：无损压缩（Barton，1997）、差值扩展（Tian，2003）和直方图平移（Ni et al.，2006）。为了进一步提高嵌入能力，减少嵌入后的图像失真，研究人员提出了一系列新的可逆信息隐藏方法。这些方法包括一维预测误差直方图法（Tsai et al.，2009；Jia et al.，2019）、多维预测误差直方图法（Ou et al.，2019；Zhang et al.，2020）、像素值排序法（Wu et al.，2020；Fan et al.，2021）、多直方图法（Li et al.，2015；Qin et al.，2019）、非对称直方图法（Kim et al.，2019；何玉芬等，2019）以及结合卷积神经网络构建预测误差直方图的方法（Hu et al.，2021，2022）。近年来，学者们将上述方法运用到了空域图像认证领域。Lee et al.（2006）根据 Holliman et al.（2000）的方法生成认证信息，然后利用差值扩展的方法将其嵌入图像中。Lo et al.（2014）提出了一种图像分块且可定位篡改的可逆认证方法，首先将图像分为N个不重叠分块，针对每个分块生成预测误差直方图，然后对其进行平移扩展操作，从而将N比特的认证信息嵌入N个分块中。Nguyen et al.（2016）同样对图像进行分块，对每个分块进行小波变换，通过修改小波系数嵌入认证信息。为了进一步探究图像像素间的关联性，Yin et al.（2016）提出先对图像像素进行希尔伯特扫描，然后将扫描得到的像素序列分为N个分块，并利用基于像素值排序的方法将认证信息嵌入到分块中，取得了较好的认证效果。Hong et al.（2017）通过引入最低有效位替换的方式，解决了对于嵌入容量为0的分块无法有效认证的问题。Yao et al.（2020）提出了一种自适应分块方法，其目的是将图像分割为尺寸更小的分块，从而实现认证精度的提高。王泓等（2022）为了提高 Hong et al.（2017）方法的安全性，将分块中的子块进行 Arnold 置乱后再生成并且嵌入认证码。

现有的可逆认证方法在正确检测率方面仍有较大的提升空间。此外，在认证信息嵌入过程中，这些方法往往会影响图像的视觉质量，无法满足高质量图像认证的需求。本文将认证码嵌入到载体图像的小波域中。另外，哈尔小波变换具有良好的重构特性，能够在嵌入信息后准确地重构原始图像。因此，本文采用哈尔小波对载体图像进行变换和逆变换，其可逆特性非常适合可逆认证方法。研究成果不仅实现了图像的可逆恢复，而且大多数分块具有独立认证的能力。

1　IPVO方法介绍

1.1　方法

IPVO方法是对PVO方法的改进，其主要步骤如下：将图像划分为大小相同且不重叠的分块，对分块中像素值$\{x_1, x_2, \cdots, x_{n-1}, x_n\}$进行升序排序得到$\{x_{\sigma_1}, x_{\sigma_2}, \cdots, x_{\sigma_{n-1}}, x_{\sigma_n}\}$，其中下标$\sigma_i$表示$x_{\sigma_i}$在$\{x_1, x_2, \cdots, x_{n-1}, x_n\}$中的位置，当$x_i = x_j$且$i < j$时，有$\sigma_i < \sigma_j$.

为了在最大像素值x_{σ_n}中嵌入1 bit信息，计算预测误差值$d_{\max} = x_u - x_v$，其中

$$u = \min(\sigma_n, \sigma_{n-1}),\ v = \max(\sigma_n, \sigma_{n-1}).$$

根据$d_{\max}$值决定能否在像素x_{σ_n}中嵌入1 bit信息：

$$x'_{\sigma_n} = \begin{cases} x_{\sigma_n} + b, & d_{\max} = 1 \text{ 或 } 0; \\ x_{\sigma_n} + 1, & d_{\max} > 1 \text{ 或 } d_{\max} < 0. \end{cases} \tag{1}$$

同理，计算预测误差值$d_{\min} = x_s - x_t$，其中$s = \min(\sigma_1, \sigma_2)$，$t = \max(\sigma_1, \sigma_2)$.根据$d_{\min}$值决定能否在像素$x_{\sigma_1}$中嵌入1 bit信息：

$$x'_{\sigma_1} = \begin{cases} x_{\sigma_1} - b, & d_{\min} = 1 \text{ 或 } 0; \\ x_{\sigma_n} - 1, & d_{\min} > 1 \text{ 或 } d_{\min} < 0. \end{cases} \tag{2}$$

式中x'_{σ_n}为修改后的最大像素值；x'_{σ_1}为修改后的最小像素值；b为待嵌入的信息（$b = 0$或1）。

由公式（1）和（2）可见，当预测误差值$d = \{0, 1\}$时，可以将信息b嵌入到最大/最小像素值$\{x_{\sigma_1}, x_{\sigma_n}\}$中；当$d < 0$或$d > 1$时，对$x_{\sigma_n}$加1或$x_{\sigma_1}$减1，使得小于0的$d$向左边平移、大于1的$d$向右边平移一个单位。根据以上嵌入规则，在嵌入信息后，分块的升序序列不会改变，嵌入信息后的x'_{σ_n}和x'_{σ_1}仍是分块中的最大和最小像素值。

在提取分块中的嵌入信息时，将分块中的像素值进行升序排序，用上述方法计算升序序列中的预测误差$d'_{\max}$和$d'_{\min}$，再从中提取出嵌入的信息，最后可逆还原分块。公式（3）和（4）用于从$d'_{\max}$和$d'_{\min}$中提取信息，b'为提取出来的比特。

$$b'=\begin{cases}0, & d'_{\max}=1 \text{ 或 } 0;\\ 1, & d'_{\max}=-1 \text{ 或 } 2;\end{cases} \tag{3}$$

$$b'=\begin{cases}0, & d'_{\min}=1 \text{ 或 } 0;\\ 1, & d'_{\min}=-1 \text{ 或 } 2.\end{cases} \tag{4}$$

根据公式(5)和(6)还原分块中的最大像素值x_{σ_n}和最小像素值x_{σ_1}:

$$x_{\sigma_n}=\begin{cases}x'_{\sigma_n}, & d'_{\max}=1 \text{ 或 } 0;\\ x'_{\sigma_n}-1, & d'_{\max}>1 \text{ 或 } d'_{\max}<0;\end{cases} \tag{5}$$

$$x_{\sigma_1}=\begin{cases}x'_{\sigma_1}, & d'_{\min}=1 \text{ 或 } 0;\\ x'_{\sigma_1}+1, & d'_{\min}>1 \text{ 或 } d'_{\min}<0.\end{cases} \tag{6}$$

1.2 实例

用一个简单的例子来简要说明IPVO嵌入方法。假设某2 × 2分块像素值为$\{x_1, x_2, x_3, x_4\}=\{51, 60, 59, 55\}$，对其升序排序后得到

$$\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}=\{1, 4, 3, 2\},$$

$$\{x_{\sigma_1}, x_{\sigma_2}, x_{\sigma_3}, x_{\sigma_4}\}=\{51, 55, 59, 60\}.$$

1.2.1 嵌入流程 实例中，$u=2$、$v=3$，对应的预测误差值$d_{\max}=x_u-x_v=60-59=1$，则可以嵌入1比特信息。

假设要嵌入的比特$b=1_2$，由式(1)将$b=1_2$嵌入到像素$x'_{\sigma_4}=x_{\sigma_4}+1=61$中；同样地，$s=1$、$t=4$，对应的$d_{\min}=x_s-x_t=51-55=-4$，不满足嵌入条件；据式(2)将像素$x_{\sigma_1}$移动1个单位，即$x'_{\sigma_1}=x_{\sigma_1}-1=50$。完成以上嵌入步骤后$\{x'_{\sigma_1}, x'_{\sigma_2}, x'_{\sigma_3}, x'_{\sigma_4}\}=\{50, 55, 59, 61\}$，完成嵌入后该分块的像素值为$\{x'_1, x'_2, x'_3, x'_4\}=\{50, 61, 59, 55\}$.

1.2.2 提取流程 对分块$\{x'_1, x'_2, x'_3, x'_4\}=\{50, 61, 59, 55\}$进行稳定地升序排序得$\{x'_{\sigma_1}, x'_{\sigma_2}, x'_{\sigma_3}, x'_{\sigma_4}\}=\{50, 55, 59, 61\}$. 预测误差值$d'_{\max}=x'_u-x'_v=61-59=2$，则可从$x'_{\sigma_4}$中提取出比特$b=1_2$，并根据公式(5)将$x'_{\sigma_4}$还原为$x_{\sigma_4}=x'_{\sigma_4}-1=60$；同样地，计算预测误差值$d'_{\min}=x'_s-x'_t=50-55=-5$，根据公式(6)还原$x'_{\sigma_1}=x_{\sigma_1}+1=50+1=51$.

2 图像可逆认证

所提出方法的嵌入流程如图1所示。嵌入方法首先对大小为512 × 512的原始图像X进行一次哈尔小波变换，得到大小为512 × 256的低频子带X^l以及高频子带X^h. 然后，将变换后得到的低频子带X^l和高频子带X^h分为若干个大小为4 × 4且互不重叠的分块。根据分块内的系数值和分块位置信息生成认证码，再将认证码嵌入到分块内。在不发生溢出的情况下，嵌入认证码不会产生附加信息。最后，通过哈尔小波逆变换将认证后的低频子带Y^l与高频子带Y^h变换为认证图像Y.

2.1 哈尔小波变换

哈尔小波变换能够对图像进行多尺度分析，将图像分解为不同尺度的子带，分别表示不同频率的成分。低频成分反映图像的整体结构，而高频成分反映图像的细节和边缘信息。在低频子带中嵌入信息可以减少对图像视觉质量的影响，而在高频子带中嵌入信息则可以利用人眼对高频细节不敏感的特点，提高嵌入信息的隐蔽性。此外，整数哈尔小波变换具有良好的重构特性，将认证后的低频和高频子带通过哈尔小波逆变换重构，可以使认证信息均匀分布到图像中，从而提升认证效果。

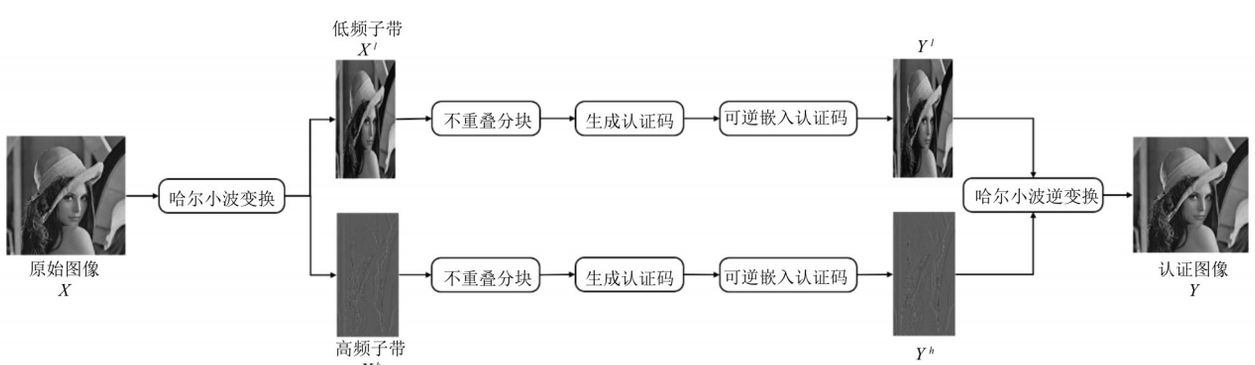


图1 图像可逆认证方法流程图

Fig. 1 Flowchart of the image reversible authentication method

哈尔小波变换实现方法为：记x_1和x_2为原始图像X中的两个相邻像素，这两个像素对应的低频小波系数x^l和高频小波系数x^h为

$$x^l = \left\lfloor (x_1 + x_2)/2 \right\rfloor, \tag{7}$$

$$x^h = x_1 - x_2 . \tag{8}$$

该变换是可逆变换，通过对x^l和x^h进行哈尔小波逆变换，可以还原出x_1和x_2：

$$x_1 = x^l + \left\lfloor (x^h + 1)/2 \right\rfloor, \tag{9}$$

$$x_2 = x^l - \left\lfloor x^h/2 \right\rfloor . \tag{10}$$

2.2　图像不重叠分块

图像拥有者对图像的低频子带X^l和高频子带X^h分别进行不重叠分块，每个分块B_i为4 × 4大小。再对每个分块B_i按图2的方式进一步划分为2 × 2大小的嵌入单元，即$B_i = \{B_i^k\}_{k=1}^4$. 用$\{B_{i,\sigma_j}^k\}_{j=1}^4$表示排序后的分块$B_i$中第$k$个嵌入单元的系数值，则有$B_{i,\sigma_1}^k \leqslant B_{i,\sigma_2}^k \leqslant B_{i,\sigma_3}^k \leqslant B_{i,\sigma_4}^k$.

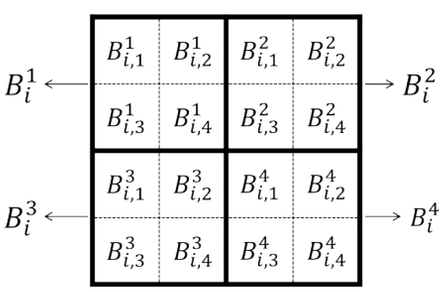


图2　图像分块

Fig. 2　Partition of the image

使用Peng et al.(2014)的IPVO技术将认证码嵌入到每个分块的4个嵌入单元中。根据B_i的嵌入容量将分块划分为可嵌入块或不可嵌入块，即：

1）利用IPVO方法计算分块B_i中每个2 × 2嵌入单元的嵌入容量$\alpha_i^j\left(j = 1, 2, 3, 4\right)$，便可得到分块$B_i$的嵌入容量$\alpha_i = \sum_{j=1}^{4} \alpha_i^j$，易知$0 \leqslant \alpha_i \leqslant 8$；

2）若分块B_i的嵌入容量$\alpha_i = 0$，将其分类为不可嵌入块$\left(B_i \in U\right)$；若$\alpha_i \geqslant 1$，则分类为可嵌入块$\left(B_i \in E\right)$.

2.3　不可嵌入块的认证码嵌入

在分块B_i的嵌入容量$\alpha_i = 0$时，通过替换最低有效位(LSB)的方法将一位认证码嵌入到密钥k_e指定的嵌入单元中。为保证图像在未被篡改的情况下可逆还原，需要将被替换的LSB存储到一个动态数组SB_{LSB}中。

首先，使用IPVO方法将4个排序后的嵌入单元中的最大和最小系数值分别移动一个单位，移动后的分块B_i记为$B_i' = \{B_i'^k\}_{k=1}^4$. 采用LSB替换的方法有可能会导致不可嵌入块变为可嵌入块，为了避免这种情况发生，根据密钥k_e选取一个嵌入单元$B_i'^*$，再将$B_i'^*$中的最小系数B'^*_{i,σ_1}和最大系数B'^*_{i,σ_4}分别移动2个单位，即$B''^*_{i,\sigma_1} = B'^*_{i,\sigma_1} - 2$，$B''^*_{i,\sigma_4} = B'^*_{i,\sigma_4} + 2$，以保证采用LSB替换方式嵌入一位认证码后嵌入单元$B_i'^*$的预测误差值$d'_{\max} > 2$以及$d'_{\min} > 2$.

经过以上预处理后的分块$B_i'' = \{B''^*_i, B''^{z*}_i\}_{z=1}^3$，其中嵌入单元$B''^*_i$为被密钥$k_e$选中的单元，其余3个$\{B''^{z*}_i\}_{z=1}^3$则是未被选中的单元。为了生成1位认证码，使用MD5哈希函数对B_i''中所有系数值的高7位以及B_i''的位置信息生成128位哈希值，并对结果进行异或直到得到1位认证码ac_i^1.

然后，提取被密钥k_e选中的嵌入单元B''^*_i的左上角系数值($B''^*_{i,1}$)的LSB并将其保存到动态数组SB_{LSB}中，接着将$B''^*_{i,1}$的LSB替换为认证码ac_i^1. 将嵌入完成后的块记为$\hat{B}_i$. 动态数组SB_{LSB}的长度与不可嵌入块的个数相同，并会在下节中被嵌入可嵌入块内。

2.4　可嵌入块的认证码嵌入

在分块B_i的嵌入容量$\alpha_i \geqslant 1$时，该块为可嵌入块. 记B_i的四个嵌入单元升序排序后的系数值为$\{B_{i,\sigma_1}^k, B_{i,\sigma_2}^k, B_{i,\sigma_3}^k, B_{i,\sigma_4}^k\}_{k=1}^4$，在嵌入认证码时，$B_{i,\sigma_2}^k$和$B_{i,\sigma_3}^k$中的系数值保持不变，利用$B_i$中4个嵌入单元的$B_{i,\sigma_2}^k$和$B_{i,\sigma_3}^k$系数以及分块$B_i$的位置信息来生成128位的哈希值，再对生成的哈希值进行反复异或得到α_i位数的认证码$ac_i^{\alpha_i}$，认证码生成后便可用IPVO方法嵌入到B_i中。

为保证图像在未被篡改的情况下可逆还原，当分块B_i的嵌入容量$\alpha_i \geqslant 3$且动态数组SB_{LSB}中存在附加信息时，从SB_{LSB}中取出一位比特，替换认证码$ac_i^{\alpha_i}$的最低有效位并嵌入到分块B_i中。

在完成低频子带X^l和高频子带X^h中所有不可嵌入块和可嵌入块的认证信息嵌入后，将会得到认证后的低频子带Y^l和高频子带Y^h. 图像拥有者对低频子带Y^l和高频子带Y^h进行一次哈尔小波逆变换便可得到认证图像Y.

2.5 图像可逆恢复与篡改定位

在确保图片未被篡改的情况下，图片接收方可以对图片进行可逆还原。通过IPVO算法计算得到每个分块$\hat{B}_i$的嵌入容量α_i以及该子带中可嵌入块的数量N_E和不可嵌入块的数量N_U. 然后，可嵌入块根据IPVO的提取方法进行可逆还原，并在前N_U个嵌入容量$\alpha_i \geqslant 3$的可嵌入块中提取出动态数组SB_{LSB}. 不可嵌入块从SB_{LSB}中提取一位比特替换密钥k_e指定嵌入单元的第一个系数的最低有效位后，对不可嵌入块进行可逆还原。

图片接收方在无法确认图片是否被篡改的情况下，通过以下流程对图片进行认证。首先，接收方对认证图像Y进行一次哈尔小波变换，接着对两个子带分别进行分块处理，得到$2N$个不重叠的4×4分块$\left\{\hat{B}_i^{\mathrm{low}}\right\}_{i=1}^{N}$和$\left\{\hat{B}_i^{\mathrm{high}}\right\}_{i=1}^{N}$。其中，$\hat{B}_i^{\mathrm{low}}$和$\hat{B}_i^{\mathrm{high}}$分别代表低频子带$Y^l$和高频子带$Y^h$中的第$i$个分块。计算低频子带$Y^l$中分块$\hat{B}_i^{\mathrm{low}}$和高频子带$Y^h$中分块$\hat{B}_i^{\mathrm{high}}$的嵌入容量，根据块的容量选定认证方式：

1）可嵌入块认证。如果分块$\hat{B}_i$的嵌入容量$\alpha_i \geqslant 1$，用IPVO算法从$\hat{B}_i$中提取出认证码$ac_i^{\alpha_i}$. 接着对$\left\{\hat{B}_{i,\sigma_2}^k,\ \hat{B}_{i,\sigma_3}^k\right\}_{k=1}^{4}$系数值以及分块$\hat{B}_i$的位置信息进行哈希生成认证码$ac'^{\alpha_i}_i$. 对比提取认证码以及生成认证码是否相同，若$ac_i^{\alpha_i} = ac'^{\alpha_i}_i$，则将分块$\hat{B}_i$标记为未篡改块，并利用IPVO将分块$\hat{B}_i$可逆恢复；若$ac_i^{\alpha_i} \neq ac'^{\alpha_i}_i$，则将分块$\hat{B}_i$归为篡改块。

2）不可嵌入块认证。如果分块$\hat{B}_i$的嵌入容量$\alpha_i = 0$，则$\hat{B}_i$为不可嵌入块，根据$\hat{B}_i$中所有系数值的7个最高有效位以及$\hat{B}_i$的位置信息进行哈希生成1位认证码ac'^1_i. 接收方根据密钥选取出嵌入单元$\hat{B}^*{}_i$，并从$\hat{B}^*{}_i$的左上角系数$\hat{B}^*{}_{i,1}$中提取出一位认证码ac_i^1（即$\hat{B}^*{}_{i,1}$的LSB），并对比ac_i^1是否与ac'^1_i相等。

3）若$ac_i^1 = ac'^1_i$，则该块未被篡改，从动态数组SB'_{LSB}中提取出一位比特对$\hat{B}^*{}_{i,1}$的LSB位进行还原，并将嵌入单元$\hat{B}^*{}_i$的排序后的最小和最大系数值分别进行加2和减2。最后，使用IPVO方法对分块$\hat{B}_i$进行还原。若$ac_i^1 \neq ac'^1_i$，则将分块$\hat{B}_i$标记为篡改块。

3 实验结果

实验部分采用了图3中9幅The USC-SIPI Image Database（Weber，1997）的512 × 512大小的标准灰度图像以及BOSSbase 1.01（Bas et al.，2011）中100幅512 × 512大小的自然风光图像进行实验，分块大小均为4 × 4。为衡量图像在嵌入认证信息后的视觉质量，采用峰值信噪比（PSNR）和正确检测率$\mathrm{CR} = C_{\mathrm{block}}/T_{\mathrm{block}} \times 100\%$对比方法的认证性能。其中，$C_{\mathrm{block}}$表示被正确检测到的篡改块数量，$T_{\mathrm{block}}$表示篡改块的数量。

3.1 认证图像的嵌入容量和图像质量

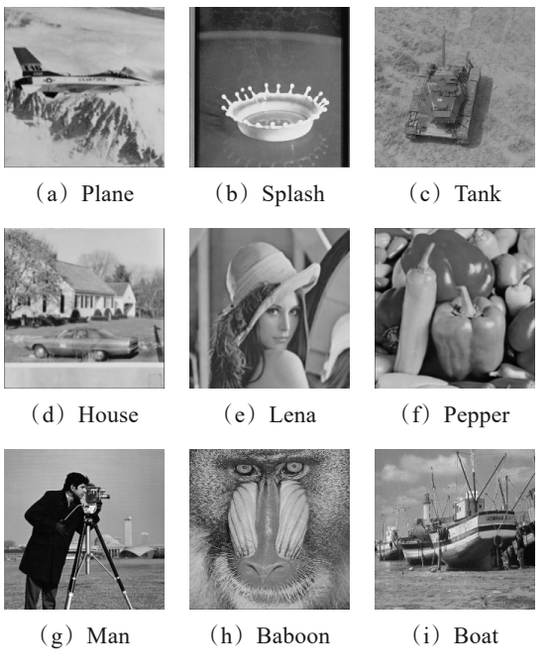
表1和表2为嵌入容量和PSNR的对比结果。表中，方法一、方法二、方法三、方法四依次分为Hong et al.（2017）、Yao et al.（2020）、王泓等

表1 嵌入容量对比

Table 1 Comparison of embedded capacity 10^4 bit

	方法一	方法二	方法三	方法四	本文方法
Plane	5.2	5.2	4.7	8.7	4.9
Splash	5.3	5.3	4.6	8.7	5.1
Tank	2.8	2.8	2.5	3.9	2.8
House	4.6	4.6	4.2	7.6	4.5
Lena	3.8	3.8	3.2	6	3.7
Pepper	3.1	3.1	2.8	3.8	3.0
Man	7.2	7	5.9	14.1	6.8
Baboon	—	1.3	—	2.0	1.3
Boat	2.6	2.8	2.3	3.2	2.8
BOSSBase 100	3.96	4.02	3.52	13.7	4.01
平均	3.94	4.01	3.51	13.1	3.99

注：—表示该数据没有被检测到。



（a）Plane　（b）Splash　（c）Tank

（d）House　（e）Lena　（f）Pepper

（g）Man　（h）Baboon　（i）Boat

图3　实验图像

Fig. 3　Experimental images

（2022）和钟亦友等（2023）的结果（下同）。相比之下，方法四具有最高的嵌入容量，这是因为其采用了双层嵌入策略，且大部分分块内的像素用于嵌入认证信息，但这也导致了显著的PSNR下降。本文方法为了保证良好的视觉质量，采用了IPVO的嵌入方式，最多只修改分块中的一半系数值。因此，本文方法在图像的视觉质量上表现更好，同时具有更高的正确检测率。方法一和方法三在图3(h)Baboon上无法有效进行认证。这是因为图3(h)的纹理比较复杂，使用这些方法时发现可嵌入认证信息的分块数量少于不可嵌入的分块数量，会导致认证信息的嵌入失败。

3.2　认证性能对比

本节实验中，对109幅实验图像进行认证，再进行四种篡改攻击，篡改检测单元均为4 × 4大小。其中，四种篡改攻击分别为剪贴攻击、常数攻击、拼贴攻击和随机篡改，攻击方式和篡改检测标记如图4所示。

表2　PSNR对比

Table 2　Comparison of PSNR

	方法一	方法二	方法三	方法四	本文方法
Plane	51. 04	48. 84	50. 65	42. 40	49. 24
Splash	51. 65	49. 55	51. 31	46. 08	49. 80
Tank	50. 17	50. 43	49. 86	42. 32	48. 42
House	50. 37	47. 85	49. 96	41. 24	48. 61
Lena	50. 60	47. 95	50. 01	42. 64	48. 95
Pepper	50. 34	50. 62	50. 02	41. 39	48. 80
Man	50. 21	49. 89	49. 42	44. 35	49. 63
Baboon	—	48. 21	—	34. 62	46. 85
Boat	48. 74	49. 92	48. 05	42. 75	48. 46
BOSSBase 100	49. 1	49. 45	49. 12	40. 42	50. 06
平均	49. 19	49. 43	48. 71	40. 54	49. 94

注：—表示该数据没有被检测到。

表3为正确检测率对比，本文方法的正确检测率高于其他四种方法。主要原因是前两种方法中存在较多分块只能嵌入1 bit认证码；方法三对分块内像素进行了置乱，导致像素相关性降低，牺牲了一定的认证性能；方法四和本文提出的方法都使用了块的两层认证方法，其中每个块可以嵌入至少2位认证码。这种做法有效降低了提取的认证码与生成的认证码相等的可能性，因此在认证性能方面优于其他方法。

3.3　认证时间对比

在对BOSSbase数据集中的100幅图像进行认证信息的嵌入和提取时，记录了方法的处理时间。所有实验均在MATLAB环境下完成，实验所用计算机配备了Intel Core i7-4790 3.60 GHz的CPU和16 GB的运行内存。在开始处理100幅图像的循环之前，使用tic函数开始计时，并在处理完所有图

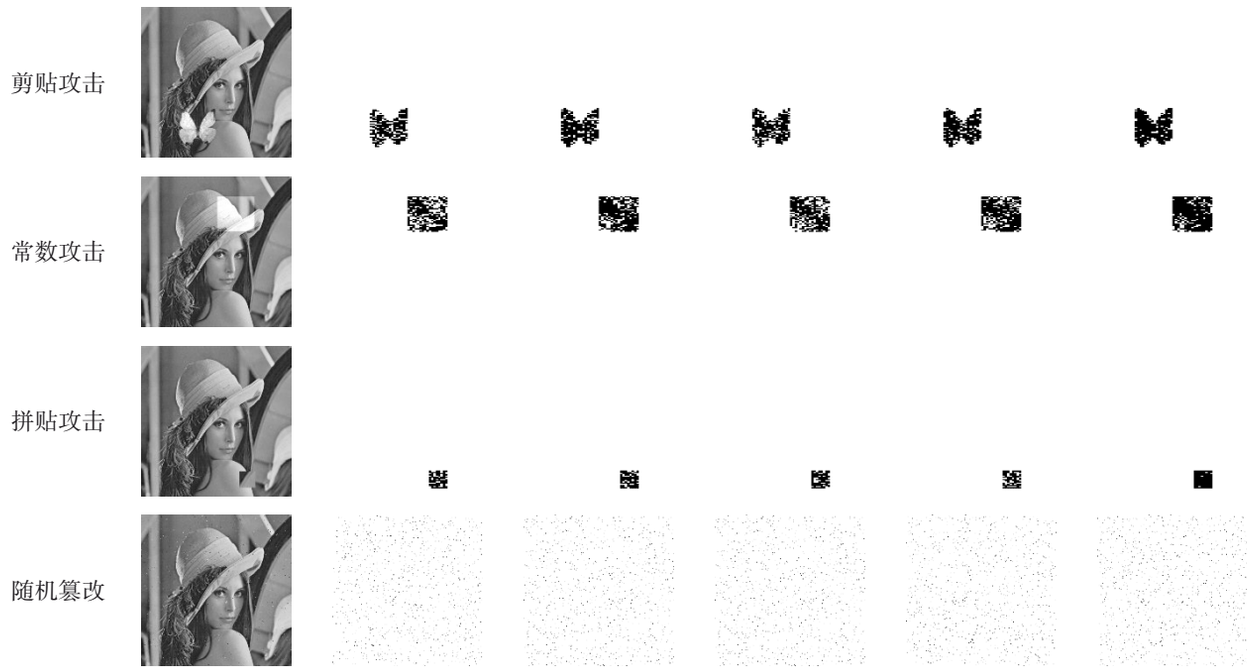


图4 篡改检测标记

Fig. 4 Tamper detection markers

表3 正确检测率对比

Table 3 Comparison of correct detection rates %

	方法一	方法二	方法三	方法四	本文方法
剪贴	71. 70	76. 43	66. 87	89. 12	88. 72
常数	68. 91	74. 12	64. 50	78. 45	83. 43
拼贴	66. 78	73. 50	70. 37	79. 15	83. 26
随机	63. 82	51. 47	58. 85	82. 10	78. 23
平均	67. 80	68. 88	65. 14	82. 20	83. 41

像后使用 toc 函数结束计时。表 4 为认证时间的对比结果。表中后两种方法的处理时间明显较长，这主要是因为方法三在进行分块认证之前需要对分块内像素进行置乱操作，而方法四为了实现“差分块”和“平移块”的嵌入，需要更复杂和耗时的过程。

表4 认证时间对比

Table 4 Comparison of processing time s

	方法一	方法二	方法三	方法四	本文方法
认证信息嵌入时间	312. 41	1 240. 73	1 864. 86	3 153. 93	300. 81
认证信息提取时间	309. 84	1 626. 90	1 856. 89	2 902. 12	328. 75
每张图片平均处理时间	3. 11	14. 34	18. 60	30. 28	3. 15

3. 4 消融实验

本文方法在对载体图像进行认证时，对载体图像的低频子带和高频子带都进行了认证信息的嵌入，而本节实验中仅对载体图像的低频子带进行认证，不修改高频子带。从表 5 可以看出，当且仅在载体图像的低频子带中嵌入认证信息时，仅修改低频子带的本文方法的 PSNR 略高于其他方法。

在正确检测率的对比过程中，使用了与图 4 相同的四种篡改手段。如表 6 所示，本文方法在正确

检测率上优于四种对比方法中的前三种，略低于最后一种方法；特别是在随机攻击中，仅修改低频子带的方法的检测率显著下降。这主要是因为在仅修改低频子带时，部分分块只能容纳1比特的认证信息，导致在进行随机篡改后，有50%的概率使得该分块的篡改后认证信息与篡改前的认证信息相同。为了进一步提升正确检测率，可以考虑采用本文方法，即同时在低频子带和高频子带中嵌入认证信息。这种做法能够有效解决仅修改低频子带时检测率下降的问题，因为高频子带的额外信息嵌入可以提供更多的认证信息，增强对篡改的敏感性和准确性。

表5　PSNR对比

Table 5　Comparison of PSNR

	方法一	方法二	方法三	方法四	仅认证低频子带
Plane	51.04	48.84	50.65	42.40	50.99
Splash	51.65	49.55	51.31	46.08	51.73
Tank	50.17	50.43	49.86	42.32	50.08
House	50.37	47.85	49.96	41.24	50.21
Lena	50.60	47.95	50.01	42.64	50.76
Pepper	50.34	50.62	50.02	41.39	50.75
Man	50.21	49.89	49.42	44.35	51.19
Baboon	—	48.21	—	34.62	48.31
Boat	48.74	49.92	48.05	42.75	50.35
BOSSBase 100	49.10	49.45	49.12	40.42	51.92
平均	49.19	49.43	48.71	40.54	51.79

注：—表示该数据没有被检测到。

表6　正确检测率对比

Table 6　Comparison of correct detection rates　　%

	方法一	方法二	方法三	方法四	仅认证低频子带
剪贴	71.70	76.43	66.87	89.12	82.41
常数	68.91	74.12	64.50	78.45	78.72
拼贴	66.78	73.50	70.37	79.15	76.42
随机	63.82	51.47	58.85	82.10	66.32
平均	67.80	68.88	65.14	82.20	75.96

4　结　论

本文提出了一种基于IPVO的高效图像可逆认证方法。通过对图像进行一次哈尔小波变换，然后将IPVO方法应用于小波系数的修改，同时对待认证图像的低频子带和高频子带进行嵌入，实现了双层认证的效果。此方法能够对几乎所有分块进行独立认证。实验结果表明，与现有基于分块且可逆的图像认证方法相比，本文方法在保持图像质量的同时，具备较好的篡改检测和定位能力。

参考文献：

何玉芬，殷赵霞，汤进，等，2019. 基于非对称直方图平移的可逆信息隐藏算法[J]. 网络与信息安全学报，5(5)：80-89.

王泓，黄方军，2022. 基于可逆信息隐藏技术的认证方案的攻击与改进[J]. 信息安全学报，7(1)：56-65.

钟亦友，黄方军，2023. 基于分块的高效图像可逆认证方法[J]. 软件学报，34(12)：5848-5861.

BARTON J M，1997. Method and apparatus for embedding authentication information within digital data：US5646997 [P/OL]. https://www.freepatentsonline.com/

5646997.html.

BAS P，FILLER T，PEVNY T，2011.Break our steganographic system：The ins and outs of organizing BOSS［M］. Lecture Notes in Computer Science. Berlin Heidelberg：Springer.

FAN G，PAN Z，GAO E，et al，2021. Reversible data hiding method based on combining IPVO with bias-added Rhombus predictor by multi-predictor mechanism［J］. Signal Process，180：107888.

HOLLIMAN M，MEMON N，2000. Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes［J］. IEEE Trans Image Process，9（3）：432-441.

HONG W，CHEN M，CHEN T，2017. An efficient reversible image authentication method using improved PVO and LSB substitution techniques［J］. Signal Process Image Commun，58：111-122.

HU R，XIANG S，2021. CNN prediction based reversible data hiding［J］. IEEE Signal Process Lett，28：464-468.

HU R，XIANG S，2022. Reversible data hiding by using CNN prediction and adaptive embedding［J］. IEEE Trans Pattern Anal Mach Intell，44（12）：10196-10208.

JIA Y，YIN Z，ZHANG X，et al，2019. Reversible data hiding based on reducing invalid shifting of pixels in histogram shifting［J］. Signal Process，163：238-246.

KIM S，QU X，SACHNEV V，et al，2019. Skewed histogram shifting for reversible data hiding using a pair of extreme predictions［J］. IEEE Trans Circuits Syst Video Technol，29（11）：3236-3246.

LEE S K，SUH Y H，HO Y S，2006. Reversible image authentication based on watermarking［C］//International Conference on Multimedia and Expo. Toronto，ON，Canada：IEEE：1321-1324.

LI X，ZHANG W，GUI X，et al，2015. Efficient reversible data hiding based on multiple histograms modification［J］. IEEE Trans Inf Forensics Secur，10（9）：2016-2027.

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

NGUYEN T S，CHANG C C，YANG X Q，2016. A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain［J］. Int J Electron Commun，70（8）：1055-1061.

NI Z，SHI Y Q，ANSARI N，et al，2006. Reversible data hiding［J］. IEEE Trans Circuits Syst Video Technol，16（3）：354-362.

OU B，LI X，ZHANG W，et al，2019. Improving pairwise PEE via hybrid-dimensional histogram generation and adaptive mapping selection［J］. IEEE Trans Circuits Syst Video Technol，29（7）：2176-2190.

PENG F，LI X，YANG B，2014. Improved PVO-based reversible data hiding［J］. Digit Signal Process，25：255-265.

QIN J，HUANG F，2019. Reversible data hiding based on multiple two-dimensional histograms modification［J］. IEEE Signal Process Lett，26（6）：843-847.

TIAN J，2003. Reversible data embedding using a difference expansion［J］. IEEE Trans Circuits Syst Video Technol，13（8）：890-896.

TSAI P，HU Y C，YEH H L，2009. Reversible image hiding scheme using predictive coding and histogram shifting［J］. Signal Process，89（6）：1129-1143.

WEBER A G，1997. The USC-SIPI image database version 5［P/OL］.https://sipi.usc.edu/reports/.

WU H，LI X，ZHAO Y，et al，2020. Improved PPVO-based high-fidelity reversible data hiding［J］. Signal Process，167：107264.

YAO H，WEI H，QIN C，et al，2020. A real-time reversible image authentication method using uniform embedding strategy［J］. J Real Time Image Process，17（1）：41-54.

YIN Z，NIU X，ZHOU Z，et al，2016. Improved reversible image authentication scheme［J］. Cogn Comput，8（5）：890-899.

ZHANG T，LI X，QI W，et al，2020. Location-based PVO and adaptive pairwise modification for efficient reversible data hiding［J］. IEEE Trans Inf Forensics Secur，15：2306-2319.

（责任编辑　王海蓉）