# 直方图移位安全可逆图像水印算法的研究*

赵文鹏，李子臣，游福成，李祯祯
（北京印刷学院 信息工程学院，北京 102600）

**摘 要：** 针对一些在数字版权保护和多媒体信息安全领域中，需要对嵌入的水印信息进行加密来确保水印信息的机密性，提出直方图移位安全可逆的图像水印算法。对载体图像的最大像素值和最小像素值分别进行减一加一的操作，并且对该像素值进行标记，图像预处理的方法，解决了嵌入水印信息时像素值修改产生的溢出问题。利用祖冲之序列密码算法(ZUC 算法)对水印信息进行加密。在水印嵌入阶段，计算每个半平面像素的四邻域、八邻域的预测差值，来构建二维直方图，嵌入加密的水印。实验结果表明，算法能够无损地恢复原始载体图像，加密水印信息能够正确解密，含加密水印图像的峰值信噪比均达到 50 dB 以上；该方案具有良好的加解密效果，水印图像具有很好的质量和水印隐蔽性，算法具有可逆性，并且解决了像素溢出的问题。

**关键词：** 加密水印；预测差值；直方图移位；像素溢出
**中图分类号：** TP309.7　　**文献标识码：** A　　**DOI：** 10.19358/j.issn.2096-5133.2020.09.007
**引用格式：** 赵文鹏，李子臣，游福成，等. 直方图移位安全可逆图像水印算法的研究[J].信息技术与网络安全，2020，39(9)：34-38.

## Research on histogram shift safe reversible image watermarking algorithm

Zhao Wenpeng，Li Zichen，You Fucheng，Li Zhenzhen
(School of Information Engineering，Beijing Institute of Graphic Communication，Beijing 102600，China)

**Abstract：** In the field of digital copyright protection and multimedia information security，the embedded watermark information needs to be encrypted to ensure the confidentiality of the watermark information，so a safe and reversible image watermarking algorithm for histogram shift is proposed. The maximum and minimum pixel values of the carrier image are subtracted one and added one respectively，and the pixel value is marked. The carrier image is preprocessed to solve the problem of overflow caused by pixel value modification when embedding watermark information. The watermark information is encrypted using ZUC sequence cipher. In the stage of watermark embedding，the predicted difference of four fields and eight fields of each half-plane pixel is calculated to construct a two-dimensional histogram，and then the encrypted watermark is embedded. Experimental results show that the algorithm can restore the original carrier image lossless，the encrypted watermark information can be decrypted correctly，and the peak signal-to-noise ration value of the encrypted watermark image reaches more than 50 dB. The experimental results further illustrate that the scheme has good encryption and decryption effects，the watermark image has good quality and watermark concealment，the algorithm is reversible，and solves the problem of pixel overflow.

**Key words：** encrypted watermark；prediction difference；histogram shifting；pixel overflow

## 0 引言

随着网络和多媒体的快速发展及普及，数字内容规模呈指数级增长，使得数字内容的安全性越发重要[1]。数字水印技术(Digital Watermarking)应运而生。数字水印技术是信息隐藏的一个重要分支。

传统的水印是以显性嵌入在作品中的形式存在的，会极大地影响原作品的展示、传播、学习和欣赏。显性水印指的是嵌入水印之后，人类肉眼可以

* 基金项目：国家自然科学基金(61370188)；北京市教委科技计划重点项目(KZ201510015015，KZ201710015010)；北京市教委科技一般项目(KM202010015009)

看见嵌入的水印信息。

现在越来越多的水印是隐性水印，隐性的水印嵌入技术是指载体图像嵌入水印之后，人类肉眼无法看见嵌入的水印信息。版权方面[2]，现在的数字水印技术是将水印信息，如用户信息、版权信息等嵌入到数字载体中，由此来确定版权拥有者、跟踪侵权行为、所有权认证、认证数字内容来源的真实性等。一旦攻击者获知了水印算法，利用提取水印算法很容易获取水印信息，出现信息泄露或伪造水印的现象，因此，使用水印加密技术，即使水印被攻击也只能得到无用的数据。在其他领域，如军事方面，数字水印用于秘密通信，让军事机密消息的传递不暴露在传统的信息通道中，同时也需要保护水印信息。

在已有研究中，文献[3]提出了基于直方图移位的方法，具有良好的 PSNR 值，但嵌入容量和水印图像的鲁棒性需要进一步提高。文献[4]中提出了对直方图进行修改并对提取方式进行了改进，增强水印的鲁棒性，但算法并没有提高水印嵌入容量。文献[5]中提出了一种基于直方图修改的图像水印算法，能抵抗一般的传统攻击，增强了算法的鲁棒性，但算法并没有提高水印嵌入容量。文献[6]提出了基于二维直方图平移的方法，解决图像在嵌入容量较大的情况下，水印隐蔽性和认证图像质量不高的问题，利用篡改检测方法定位出图像被篡改的区域，图像完整性的认证进一步增强，但是没有考虑像素溢出和水印信息安全的问题。

在上述研究的基础上，针对如何保护水印信息的机密性，解决嵌入水印信息时像素溢出的问题，实现无损地恢复原始图像，本文提出了直方图移位安全可逆图像水印算法。首先，对载体图像进行图像预处理，防止出现像素上溢和下溢的问题。把图像划分为棋盘结构，计算每个半平面像素的四邻域、八邻域的预测差值，构建二维直方图，使用 ZUC 算法对水印信息进行加密，保证水印信息的机密性。利用直方图移位安全可逆图像水印算法，嵌入和提取加密水印，并恢复原始载体图像。实验结果表明，被加密的水印信息抗攻击能力强，图像预处理解决了像素溢出的问题，并且水印图像具有很好的峰值信噪比，该算法能够无损地恢复原始图像，实现算法的可逆。

本文算法流程图如图 1 所示。

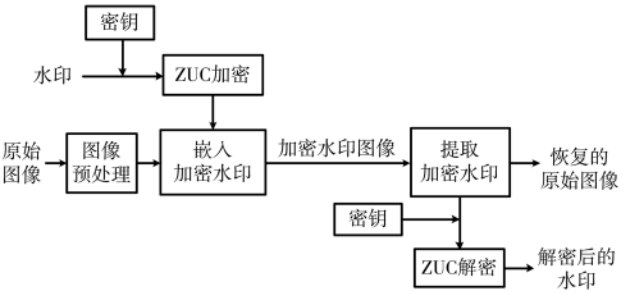


图 1 算法流程图

## 1 直方图移位安全可逆图像水印算法

### 1.1 图像预处理

假设原始图像的每个像素 $x_{i,j}$ 的取值范围为 [0,255]。$x(i,j)$ 表示位于 $(i,j)$ 的载体图像像素值。

在每个半平面的嵌入过程中，像素值可能增加 1 或减少 1。为了防止溢出的问题(即像素值变为 256 或 -1)，采用预处理的方法，在对每个半平面嵌入水印之前，预先将等于 255 或 0 的像素值分别改为 254 和 1，而具有其他值的像素保持不变。换句话说，254 或 255 的像素具有相同的结果值 254，而像素值 0 或 1 的像素具有相同的结果 1。对进行修改的像素使用标志位来标识像素。提取水印的过程中，在执行每个半平面的提取之后，根据标志位将值为 1 或 254 的像素改变为其原始值。

### 1.2 计算四邻域、八邻域预测差值

把灰度图像分为两个半平面：黑色半平面和白色半平面，类似于棋盘，如图 2 所示。

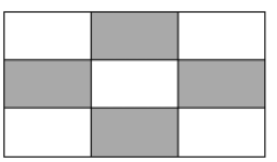

图 2 黑白棋盘结构

第一种预测差值方法：对于载体图像的每个像素用该点的像素值与其周围的上、下、左、右 4 个相邻像素的均值向下取整后做差，得到该像素点的第一个预测差值。如式(1)所示：

$$d_1=x'(i,j)=x(i,j)-\lfloor(x(i,j-1)+x(i,j+1)+x(i-1,j)+x(i+1,j))/4\rfloor \quad (1)$$

当像素点位于顶点或者边界存在特殊情况时，周围不存在 4 个像素点，则按实际相邻像素点数进行计算。

如图 3 所示，像素位于顶点，则第一个预测差值计算公式为：

$$x'(i,j)=x(i,j)-\lfloor x(i,j+1)+x(i+1,j))/2\rfloor \quad (2)$$

如图 4 所示，像素位于边界，则第一个预测差值计算公式为：

$$x'(i,j)=x(i,j)-\lfloor x(i,j+1)+x(i-1,j)+x(i+1,j))/3\rfloor \quad (3)$$

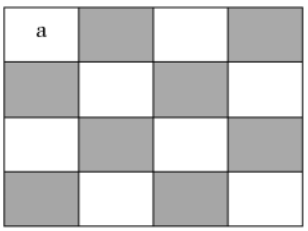


图 3 像素位于顶点的情况

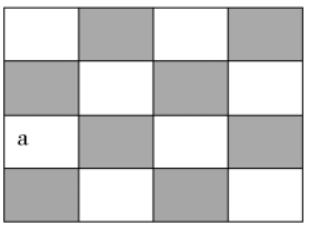


图 4 像素位于边界的情况

第二种预测差值方法：对于原始图像的每个像素用该点的像素值与其周围的 8 个相邻像素的均值向下取整后做差，得到该像素点的第二个预测差值。当像素点位于顶点或者边界存在特殊情况，周围不存在 8 个像素点时，采用有几个点算几个点的方法，与第一种预测差值的方法类似。

$$d_2=x'(i,j)=x(i,j)-\left\lfloor \begin{matrix}(x(i-1,j-1)+x(i-1,j)\\+x(i-1,j+1)+x(i,j-1)\\+x(i,j+1)+x(i+1,j-1)\\+x(i+1,j)+x(i+1,j+1))/8\end{matrix} \right\rfloor \quad (4)$$

### 1.3 水印加密

传统的保护水印方法，仅仅是对水印信息采用一些简单的置乱处理，没有对水印信息进行有效的保护。序列密码具有加解密处理速度快、实现简单、便于硬件实施等特点，因此本文采用序列密码中的 ZUC 密码算法进行加密。本文的水印信息为图片的形式。

ZUC 算法称为祖冲之算法[7-8]，属于序列密码。ZUC 算法是 3GPP 机密性算法 EEA3 和完整性算法 EIA3 的核心，加密是将 ZUC 产生的密码流和输入的明文按位异或；解密过程是将密文与加密过程相同的密码流按位异或，实现解密。

对于一个未经压缩的灰度图像，一个图像像素 $x_{i,j}$ 的取值范围为 $[0,255]$，$(i,j)$ 表示像素在块中的位置，$x_{i,j}$ 可用 8 bit 来表示，设各像素的比特位为 $b_{i,j,1},b_{i,j,2},\cdots,b_{i,j,k}$，则：

$$b_{i,j,k}=\left\lfloor \frac{x_{i,j}}{2^k} \right\rfloor \bmod 2,k=0,1,\cdots,7 \quad (5)$$

$$x_{i,j}=\sum_{k=0}^{7} b_{i,j,k}\cdot 2^k \quad (6)$$

其中 $\lfloor\cdot\rfloor$ 表示向下取整。内容所有者利用 ZUC 算法产生一个伪随机比特流 $r_{i,j,k}$，与图像像素各比特位 $b_{i,j,k}$ 逐位进行异或运算。

$$B_{i,j,k}=b_{i,j,k}\oplus r_{i,j,k} \quad (7)$$

所得到的 $B_{i,j,k}$ 即图像像素 $x_{i,j}$ 加密的结果。

水印信息为灰度图像，图像采用 ZUC 进行加密，实验结果如图 5、图 6 所示。


图 5 水印信息

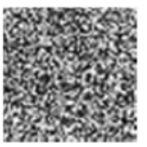

图 6 加密后的水印信息

### 1.4 水印嵌入与提取过程

与其他数据隐藏方案一样，该算法支持多层嵌入。对于每一层，嵌入过程包括两轮：第一轮，通过执行步骤(1)~(5)将消息嵌入到黑半平面；第二轮，通过再次执行步骤(1)~(5)，将消息嵌入到白色半平面。具体步骤如下：

(1)将原始载体图像分为两个半平面，类似黑白棋盘格结构。首先对黑色半平面中的每个像素计算它的四邻域差值和八邻域差值，分别用 $d_1$，$d_2$ 表示。

(2)利用差值对 $(d_1,d_2)$ 出现的频次构建黑色半平面中的二维直方图 $H(d_1,d_2)$。

(3)由 $c=d_1-d_2$ 将二维直方图 $H(d_1,d_2)$ 划分为多个不同的一维直方图 $H_c=(d_1,d_2)$，并选择可嵌入信道(Embeddable Channel，EC)。

$c$ 的绝对值越小代表信道的位置越接近直线 $d_1=d_2$，而 $c$ 的绝对值越大代表信道的位置距离直线 $d_1=d_2$ 就越远。信道所在的位置越接近直线 $d_1=d_2$，就有越好的嵌入效果。参数 $c_b$ 用来选择 EC，例如 $c_b=2$，那么信道 $-2$、$-1$、0、1、2 均为可嵌入信道。

(4)对于每个 EC，找出相应直方图的“左峰”和“右峰”。通道 c 的左峰和右峰是通道中具有最大直方图值的两个位置 $(p_l,p_l-c)$ 和 $(p_r,p_r-c)$，$p_l<p_r$。如果通道中的某些位置具有相同的直方图值，则选择最左边的位置作为左峰，最右边的位置作为右峰。

对 EC 进行平移，将 $d_2=d_1-c$ 且 $d_1>p_r$ 的直方图 $H_c=(d_1,d_2)$ 右上移动 1 个单位。将 $d_2=d_1-c$ 且 $d_1<p_l$ 的直方图 $H_c=(d_1,d_2)$ 左下移动 1 个单位。具体平移过程如下所示：

$$x'(i,j)=\begin{cases}x(i,j)-1, & d_1<p_1\\ x(i,j)+1, & d_1>p_r\\ x(i,j), & \text{其他}\end{cases} \tag{8}$$

(5)在峰值点嵌入加密水印消息，水印信息为二进制序列，$b$ 表示一位水印信息，它的值为 0 或 1，为了避免引起混淆，含水印图像的像素用 $y(i,j)$ 表示。具体嵌入过程如下：

$$y(i,j)=\begin{cases}x'(i,j)-b, & d_1=p_1\\ x'(i,j)+b, & d_1=p_r\\ x'(i,j), & \text{其他}\end{cases} \tag{9}$$

(6)最终得到嵌入加密水印的黑色半平面，再次重复步骤(1)~(5)对白色半平面嵌入水印，最终得到含加密水印的图像。

嵌入过程中的参数 CB、标志位、峰值信息和加密水印的密钥，可以通过隐蔽通道进行传输，在提取阶段使用。

提取过程是水印嵌入的逆过程。具体步骤如下所述：

步骤(1)~(3)与嵌入过程的步骤(1)~(3)相同。

(4)扫描黑色半平面。如果扫描的像素值 $y(i,j)$ 属于 EC，$(p_1,p_1-c)$ 和 $(p_r,p_r-c)$ 是左峰和右峰，则执行以下处理，处理有五种情况：

$$①\ b=\begin{cases}1, d_1=p_1 \ \&\& \ p_1-1\leqslant d_1\leqslant p_1\\ 0, d_1=p_1-1 \ \&\& \ p_1-1\leqslant d_1\leqslant p_1\end{cases}$$

$$x_{i,j}=y_{i,j}+b \tag{10}$$

$$②\ b=\begin{cases}1, d_1=p_r+1 \ \&\& \ p_r\leqslant d_1\leqslant p_r+1\\ 0, d_1=p_r \ \&\& \ p_r\leqslant d_1\leqslant p_r+1\end{cases}$$

$$x_{i,j}=y_{i,j}-b \tag{11}$$

③if $d_1<p_1-1$

$$x_{i,j}=y_{i,j}+1 \tag{12}$$

④if $d_1>p_r+1$

$$x_{i,j}=y_{i,j}-1 \tag{13}$$

⑤其他情况像素值不改变。

(5)最终得到提取加密水印之后的黑色半平面，再对白色半平面重复同样的步骤，最终得到恢复的图像。

### 1.5 加密水印的解密

提取的加密水印通过 ZUC 密码算法，利用密钥实现对水印图像解密，计算收到的信息和 $r_{i,j,k}$ 的异或得到解密图像，如式(14)所示：

$$b_{i,j,k}=B_{i,j,k}\oplus r_{i,j,k} \tag{14}$$

实验结果如图 7、图 8 所示。

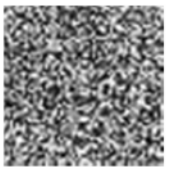

图 7 提取后的加密水印


图 8 解密后的水印

## 2 实验结果分析

本方案在 MATLABR2014a，Windows10 操作系统下验证性能，选取了 PEPPER、COUPLE、LENA 这三幅大小为 256×256 的经典灰度图像进行实验，水印信息选用 64×64 的数字图像，如图 5 所示。从不可见性、可逆性和水印信息的加密几方面验证算法的性能。

### 2.1 图像质量分析

峰值信噪比(Peak Signal to Noise Ration，PSNR)衡量图像的质量，PSNR 值越大，即图像质量越好，视觉效果越好。表 1 说明针对 256×256 大小的灰度图像，在嵌入信道为 $c_b=3$、$c_b=5$ 时，本文算法的 PSNR 值。计算 PSNR 的公式如下：

$$\text{PSNR}=10\times\log_{10}\frac{255^2}{\text{MSE}}\ \text{dB} \tag{15}$$

式中，MSE 代表原宿主图像和含水印图像之间的均方差。

表 1 256×256 大小的图像嵌入加密水印的 PSNR 值 (dB)

| 图像(256×256) | $c_b=3$ | $c_b=5$ |
|---|---|---|
| PEPPER | 50.679 0 | 50.145 6 |
| COUPLE | 51.200 1 | 50.375 4 |
| LENA | 52.795 4 | 51.145 6 |

通常 PSNR 的普遍基准在 30 dB，30 dB 以下的图像劣化较为明显，在50 dB 以上则表明效果良好，而表 1 中本文算法的 PSNR 值均达到 50 dB 以上，说明可视效果好。

实验分别对三幅原始图像嵌入水印，得到含水印图像，通过图 9 对比可以看出，水印嵌入之后，水印的不可见性和水印图像的质量都很好。

通过原始图像与提取水印信息后恢复的图像之间的归一化系数 NC 来说明算法的可逆性：

$$\text{NC}(w_1,w_2)=\frac{\sum_{i=1}^{l_1}\sum_{j=1}^{l_2}w_1(i,j)w_2(i,j)}{\sqrt{\sum_{i=1}^{l_1}\sum_{j=1}^{l_2}w_1(i,j)^2\times\sum_{i=1}^{l_1}\sum_{j=1}^{l_2}w_2(i,j)^2}} \tag{16}$$

(a)PEPPER 原始图像　(b)PEPPER 含加密水印的图像

(c)COUPLE 原始图像　(d)COUPLE 含加密水印的图像

(e)LENA 原始图像　(f)LENA 含加密水印的图像

图 9　原始图像和含加密水印的图像

式中，$w_1$、$w_2$ 分别表示原始图像和提取水印恢复后的图像，$l_1$、$l_2$ 表示原始图像的宽度和高度。

从表 2 看出，本次以三幅大小为 256×256 的灰度图像作为原始图像的实验，得到的 NC 值为 1，这说明恢复的图像并无损失，提取加密水印信息过程和图像恢复阶段是完全无失真的，从而说明水印算法的可逆性。

表 2　可逆性测试表

| 图像(256×256) | NC |
|---|---|
| PEPPER | 1 |
| COUPLE | 1 |
| LENA | 1 |

### 2.2 水印信息的加密

传统水印信息的加密方法，仅仅是对水印信息采用一些简单的置乱处理，没有对水印信息进行有效的保护。而 ZUC 算法具有实现简单、便于硬件实施、加解密处理速度快等特点。利用 ZUC 密码算法对水印信息进行加密，水印信息能够抵抗目前各种常见的攻击。

## 3 结论

在版权方面和多媒体信息安全方面，水印信息具有很重要的意义，需要对水印信息进行保护。本文的方案，采用国密 ZUC 对水印进行加密，加密的水印能够有效地抵抗各种常见的攻击，水印信息能得到有效的保护。对原始图像进行预处理的方法，解决了像素溢出的问题，提取水印信息后图像能够百分之百地恢复，从而实现算法的可逆性。本文算法保证了含水印图像具有良好的 PSNR 值。

## 参考文献


[1] 刘洋.基于公钥加密的图像数字水印算法研究[D].北京：中国地质大学，2019.

[2] 易哲为. SoC 安全水印系统研究[D].杭州：浙江大学，2019.

[3] NI Z，SHI Y Q，ANSARI N，et al.Reversible data hiding[J].IEEE Transactions on Circuits and Systems for Video Technology，2006，16(3)：354－362.

[4] DENG C，GAO X B，PENG H，et al.Histogram modification based robust image watermarking approach[J].International Journal of Multimedia Intelligence and Security，2010，1(2)：153－168.

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

[6] 李丁盛，田丽华，李晨.基于二维直方图平移的可逆图像水印算法[J].计算机工程与设计，2018，39(9)：175－180.

[7] ZUC 算法研制组.ZUC－256 流密码算法[J].密码学报，2018，5(2)：167－179.

[8] 王梓宇，毛明，张艳硕.ZUC－256 流密码的猜测决定攻击[J].计算机应用，2019，39(S1)：105－108.


(收稿日期：2020－07－02)


作者简介：

赵文鹏(1995－)，男，硕士研究生，主要研究方向：数字水印。

李子臣(1962－)，男，博士，教授，博士生导师，主要研究方向：数字签名、后量子密码、公钥密码。

# 版权声明