计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2021,30(12):226−234 [doi: 10.15888/j.cnki.csa.008225]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于 ZUC 可分离加密图像可逆水印算法①

连　帅, 丁海洋, 张珍珍, 李祯祯, 李子臣

(北京印刷学院 信息工程学院, 北京 102600)
通讯作者: 李子臣, E-mail: lizichen@bigc.edu.cn

摘　要: 本文基于祖冲之 (ZUC) 算法, 设计实现了一种可分离加密图像可逆水印算法, 算法中内容所有者先进行图像标记并生成位置图, 然后使用 ZUC 加密算法加密载体图像; 水印嵌入者得到加密图像后根据位置图将水印信息嵌在选中像素的第 7 位或第 8 位; 接收者根据加密密钥和嵌入密钥可以得到直接解密图像、水印信息和恢复图像. 算法使用 ZUC 算法对图像进行加解密, 很好地保证算法的安全性; 在嵌入水印信息之前对图像进行标记, 将水印信息嵌在选中的位置上; 接收者在利用相邻像素相关性基础上通过一种自适应差值算法实现水印提取和图像恢复, 保证恢复的载体图像和直接解密图像的质量. 实验表明所提出的算法具有较高的安全性并且达到可分离的效果, 同时恢复的载体图像和直接解密图像都具有较高质量.

关键词: 图像加密; 祖冲之 (ZUC) 算法; 可分离; 可逆水印; 图像标记

引用格式: 连帅,丁海洋,张珍珍,李祯祯,李子臣.基于 ZUC 可分离加密图像可逆水印算法.计算机系统应用,2021,30(12):226–234. http://www.c-s-a.org.cn/1003-3254/8225.html

Reversible Watermarking Algorithm for Separable Encrypted Image Based on ZUC

LIAN Shuai, DING Hai-Yang, ZHANG Zhen-Zhen, LI Zhen-Zhen, LI Zi-Chen

(College of Information Engineering, Beijing Institute of Graphic Communication, Beijing 102600, China)

Abstract: Based on the ZU Chongzhi (ZUC) algorithm, this study designs and implements a reversible watermarking algorithm for separable encrypted images. In the algorithm, the content owner first marks the image to produce a position map and then runs the ZUC encryption algorithm to encrypt the original image. After the watermark embedder obtains the encrypted image, the watermark information is embedded into the second most significant bit or the most significant bit position of the selected pixels according to the position map. Through the encryption key and the embedding key, the receiver can get the directly decrypted image, watermark information, and the recovered image. The ZUC algorithm is adopted to encrypt and decrypt the image to ensure the security of the algorithm. The image was marked before the watermark information is embedded in the selected positions. The receiver employs an adaptive difference algorithm based on the correlation between adjacent pixels to extract watermarks and restore the image, ensuring the quality of the recovered original image and the directly decrypted image. Experiments show that the proposed algorithm has high security and achieves a separable effect. At the same time, the recovered original image and the directly decrypted image also have high quality.

Key words: image encryption; ZU Chongzhi (ZUC) algorithm; separable; reversible watermark; image mark

① 基金项目:　国家自然科学基金 (61370188);　北京市教委科技计划一般项目 (KM202010015009);　北京市教委科研计划重点项目 (KZ201510015015, KZ201710015010)

Foundation item: National Natural Science Foundation of China (61370188); General Program of Science and Technology Program of Beijing Municipality Education Commission (KM202010015009); Key Project of Science and Technology Plan of Beijing Municipal Education Commission (KZ201510015015, KZ201710015010)

收稿时间: 2021-03-08; 修改时间: 2021-03-31; 采用时间: 2021-04-13

随着信息技术的飞速发展以及互联网技术在生活中的普及, 传统媒体的内容形式逐渐向数字转变, 数字技术使得图像、音频、视频和文本等一些多媒体数据储存和传播变得非常的方便[1], 版权侵犯、内容篡改等违法行为变得更加容易, 数字作品的版权、完整性和有效性得不到保障, 使得严重损害了作品所有者的利益, 因此解决版权保护和信息安全问题变得尤为重要[2].

数字水印[3,4] 是信息安全领域的研究热门问题, 可逆水印隐藏不仅能从载密图像中提取出秘密信息, 还能将载体图像无损还原. 现有的加密图像可逆水印隐藏方法分为以下几类: (1) 加密前对图像不做处理, 通过修改加密后数据以嵌入水印信息[5–8]; (2) 加密后通过压缩密文数据腾出空间以嵌入水印信息[9–11]; (3) 加密前对载体图像先进行预处理, 预留出空间进行水印信息嵌入[12–14]; (4) 加密数据阶段使用公钥机制, 水印嵌入阶段利用加密技术的同态性[15]. 除此之外, 在水印提取和图像恢复阶段, 根据水印提取和图像恢复是否可以独立操作, 算法分为可分离加密域可逆水印算法和不可分离加密域可逆水印算法, 其中不可分离的算法可以利用图像像素的平滑度来实现可逆性[16], 但是这种方法的提取水印和恢复图像的质量与分块的大小有关; 可分离算法[16–18] 可以解决当嵌入率比较高时无法准确提出水印的问题. 文献 [18] 利用压缩技术保证了信息的完全提取, 同时还提高了嵌入率, 文献 [17,18] 中的算法嵌入率和恢复图像质量都有了提高. 文献 [19] 提出将直方图平移随机化, 增强了算法的安全性, 并通过多层级嵌入增加嵌入容量. 文献 [20] 中的算法通过直方图平移的方法嵌入秘密信息, 具体方法是将图像进行分块, 然后将块内像素分组, 最后建立差值直方图. 文献 [21] 利用不同的加密方法对原始图像加密, 利用同态加法、差值扩展方法分别在高、低位平面嵌入水印信息.

文献 [17] 中提出的可分离加密域可逆数据隐藏算法将水印信息隐藏到高位上并且结合预测算法实现了可逆性, 由于水印信息嵌到高位导致直接解密图像质量不高, 针对这个问题, 本文在嵌入水印信息之前对图像进行标记, 通过图像标记将水印信息有选择的嵌在第 7 或 8 位, 在相邻像素相关性基础上通过一种自适应差值算法实现水印提取和图像恢复, 既能保证无失真地恢复图像又能提高解密的图像质量.

1 相关知识

1.1 祖冲之算法

祖冲之算法 (ZUC) 是一种流密码算法. 其加密过程为, 将 ZUC 算法产生的密钥和输入的明文按位进行异或运算; 解密过程为, 使用加密密钥和密文按位进行异或运算, 过程如图 1 所示.

ZUC 算法结构设计[22] 如图 2 所示, 分别包括 LFSR 线性反馈移位寄存器、BR 比特重组以及非线性函数 F. LSFR 的每一个寄存器都是 31 bit, BR 实现 LFSR 数据单元到非线性函数 F 和密钥输出 Z 的数据转换.

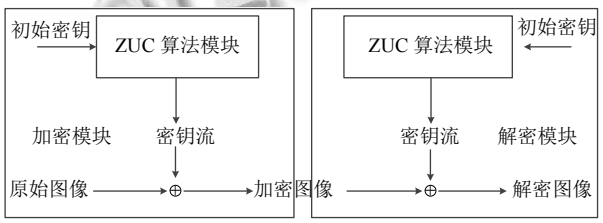


图 1 ZUC 加解密过程

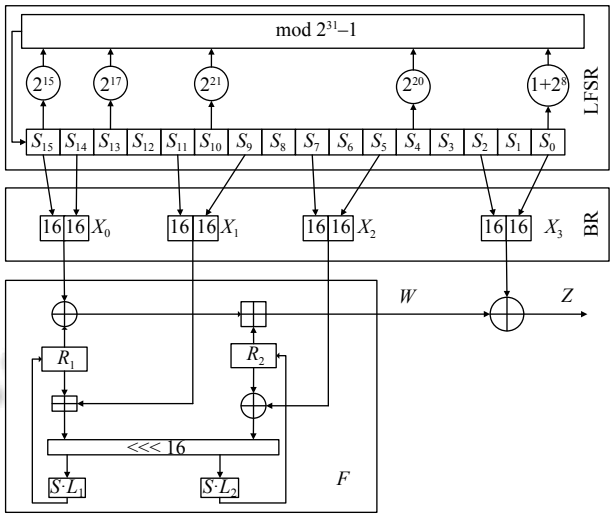


图 2 ZUC 算法结构图

1.2 加密域可逆水印技术

加密域可逆水印不仅加密域嵌入的水印信息可以完整提取, 而且水印经提取后原始载体也可以无损地恢复. 文献 [16] 利用自然图像的空间相关性实现了可逆性; 文献 [17] 提出的算法在恢复阶段使用图像预测的方法实现了算法的可逆性. 该技术一般用于多媒体作品的完整性认证, 广泛适用于一些保密强、安全密级高以及精度要求高的领域, 如医学领域、军事领域、电子发票、法律文书图片等.

2 基于 ZUC 算法可分离加密图像可逆水印算法设计

算法流程图如图 3 所示. 首先内容所有者先对载体图像进行图像标记并生成位置图, 然后利用 ZUC 算法对原始载体图像加密得到加密图像, 其次水印嵌入者得到加密图像后根据位置图将水印信息嵌入到加密图像中, 得到含水印信息的加密图像. 最后, 接收者利用嵌入密钥提取出水印信息. 接收者使用加密密钥得到直接解密的图像. 接收者使用嵌入密钥和加密密钥进行出水印信息提取以及恢复原始图像.

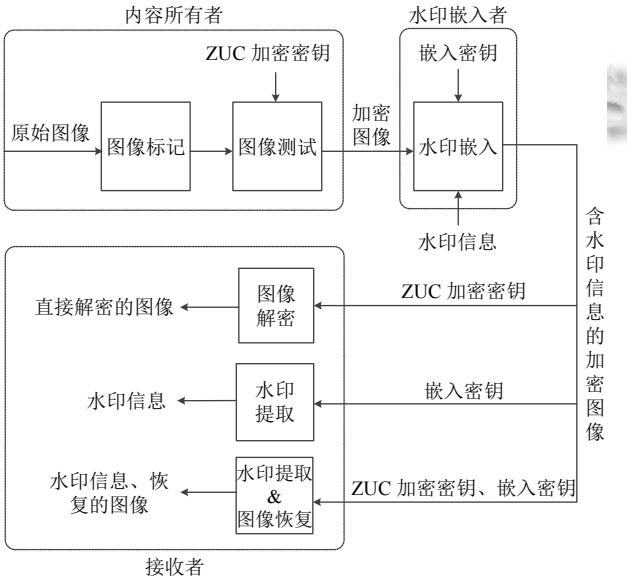


图 3 本文算法框架图

2.1 图像标记

在嵌入水印信息之前对图像进行标记, 通过标记判断嵌入的位置, 能保证恢复图像和直接解密图像具有较高的质量. 图像标记示意图如图 4 所示, 加密前的选中像素用 $b(d)$ 表示, 解密后含有水印信息的像素用 $D(d)$ 表示, 其中 $d=1, 2, \cdots, L$, L 为水印信息的长度. 水印信息嵌入第 7 位且正确恢复 $b(d)$ 有两种情况: 第一种情况是 $b(d)$ 的第 7 位为 0, 在恢复阶段, 将 $D(d)$ 的第 7 位置 1 得到 $D_0(d)$, 置 0 得到 $D_1(d)$. 这时 $D_1(d)$ 为该像素的真实值, 即 $D_1(d)=b(d)$. 因此, 在判决阶段使 $D_{out}(d)=D_1(d)$ 就能正确恢复该像素. 由式 (15) 可知, 当预测值 $D_{est}(d)$ 与 $D_1(d)$ 更接近时才能使 $D_{out}(d)=D_1(d)$. 因为 $D_0(d)-D_1(d)=2$, 由此可以得出在第一种情况下满足条件 $D_{est}(d)<b(d)+1$, 可以正确恢复原始像素. 第二种情况是 $b(d)$ 的第 7 位为 1, 同理可得正确恢复的条件为 $D_{est}(d)\geq b(d)-1$.

内容所有者对每个像素测试并将测试结果标记在位置图上. 若该像素的第 7 位是 0 且满足 $D_{est}(d)<b(d)+1$, 或第 7 位是 1 且满足 $D_{est}(d)\geq b(d)-1$, 则记为 0; 否则记为 1. 水印嵌入者在得到加密图像和位置图后使用嵌入密钥进行水印嵌入, 如果选中像素在位置图上的标记为 0, 则水印信息嵌在第 7 位. 如果选中像素在位置图上的标记为 1 则嵌在第 8 位.

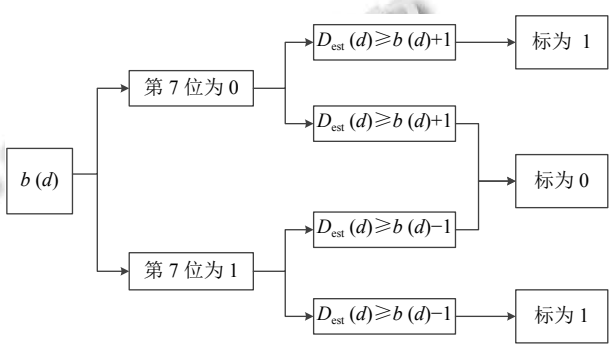


图 4 图像标记示意图

2.2 图像加密

首先内容所有者使用 ZUC 算法对图像进行加密. 对于一个大小为 $M\times N$ 的灰度图像, 灰度值 $I_{i,j}$ 的取值范围为 [0, 255], (i,j) 表示像素的位置 $(1\leq i\leq M, 1\leq j\leq N)$, $I_{i,j}$ 可表示为 8 位二进制 $b_{i,j,1}, b_{i,j,2}, \cdots, b_{i,j,8}$ 则:

$$b_{i,j,k}=\left\lfloor \frac{I_{i,j,k}}{2^{k-1}} \right\rfloor \bmod 2,\ k=1,2,\cdots,8 \tag{1}$$

其中, $\lfloor\cdot\rfloor$ 表示向下取整, 内容所有者利用 ZUC 算法产生密钥流 $r_{i,j,k}$, 与图像像素各比特位 $b_{i,j,k}$ 进行异或运算.

$$e_{i,j,k}=b_{i,j,k}\oplus r_{i,j,k},\ k=1,2,\cdots,8 \tag{2}$$

所得到的 $e_{i,j,k}$ 即加密后的结果.

由式 (3) 得到加密图像:

$$E_{i,j}=\sum_{k=1}^{8} e_{i,j,k}\times 2^{k-1},\ k=1,2,\cdots,8 \tag{3}$$

2.3 水印信息嵌入

内容所有者将加密图像和位置图传送给水印嵌入者, 假设 L 为水印信息是长度 $S(1), S(2), \cdots, S(L)$. 首先, 水印嵌入者将加密图像的像素分为用来存放嵌入信息和存放没有嵌入信息两个集合, 其中用来存放嵌入信息集合用 Q_{emb} 表示, 存放没有嵌入信息的集合用 Q_{ban} 表示. 在初始阶段令 Q_{emb} 初始值为空集, Q_{ban} 初始值为加密图像的上下左右 4 个像素即 $Q_{ban}=\{(i,j)|i=1\vee$

$j=1\vee i=M\vee j=N\}$. 然后, 水印嵌入者使用嵌入密钥随机选取与水印信息长度相同的 L 个像素, 保证选取的像素不属于 Q_{ban}, 将选取的像素放入用来存放嵌入信息集合 Q_{emb} 中, 并将该选中像素相邻的上下左右 4 个像素放入 Q_{ban} 中, 如图 5 所示, t_1, t_2, t_3, t_4 表示 4 个相邻像素. 这样对于每个用来嵌入的像素, 与它相邻的 4 个像素均不能用来嵌入水印信息, 所以这 4 个像素的值在嵌入前后保持不变. 最后, 水印嵌入者结合位置图利用式 (4) 将选中像素 $B(d)$ 的第 T 位数值 b 替换成秘密信息 $S(d)$, 从而完成水印的嵌入.

标记的位置图决定了水印嵌入的位置, 如果该像素在位置图上的标记为 0, 说明水印嵌在第 7 位该像素可以完全恢复, 为了得到更高质量的直接解密的图像, 将水印信息嵌在第 7 位. 若该像素在位置图上的标记为 1, 说明嵌在第 8 位该像素可以完全恢复, 为了得到更高质量的恢复载体图像, 将水印信息嵌在第 8 位.

$$b=\left\lfloor \frac{B(d)}{2^{(8-T)}} \right\rfloor \bmod 2,\ d=1,2,\cdots,L \tag{4}$$

$$B'(d)=B(d)-b\times 2^{(8-T)}+S(d)\times 2^{(8-T)},\ d=1,2,\cdots,L \tag{5}$$

式中, b 表示选中像素第 T 位的值, $B'(d)$是含有水印信息的加密像素.

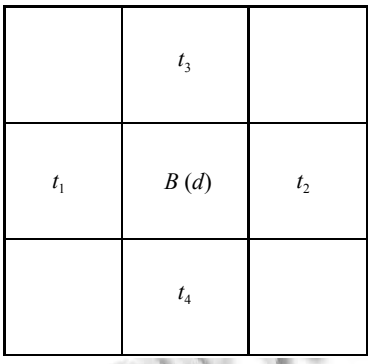


图 5 $B(d)$ 及其相邻像素的位置关系

2.4 水印信息提取及图像恢复

接收者利用加密密钥解密得到含水印信息的解密图像. 接收者利用 ZUC 算法产生密钥流 $r_{i,j,k}$, 并与$e'_{i,j,k}$逐位进行异或运算.

$$b'_{i,j,k}=e'_{i,j,k}\oplus r_{i,j,k},\ k=1,2,\cdots,8 \tag{6}$$

所得到的$b'_{i,j,k}$为直接解密的结果, $e'_{i,j,k}$为含有水印信息的加密数据.

接收者使用嵌入密钥提取水印信息, 首先根据嵌入密钥得到含有水印信息的 L 个像素$B'(1),B'(2),\cdots,B'(L)$; 再根据式 (7) 和位置图提取出水印信息 $S(d)$, 式中 T 的值由该像素在位置图上的标记决定, 若标记为 0, 则 T=7; 若标记为 1 则 T=8.

$$S(d)=\left\lfloor \frac{B'(d)}{2^{(8-T)}} \right\rfloor \bmod 2,\ d=1,2,\cdots,L \tag{7}$$

接收者同时使用加密密钥和嵌入密钥, 既可以提取水印, 也可以恢复原始载体图像. 首先, 利用加密密钥对图像进行解密得到直接解密图像, 然后根据嵌入密钥得到含有水印信息的解密像素$D(1),D(2),\cdots,D(L)$, 最后通过自适应差值算法得到嵌入像素的预测值. 取出每个含有水印信息的像素 $D(d)$ 的 4 个相邻像素 t_1, t_2, t_3, t_4, 将 t_1, t_2, t_3, t_4 代入式 (8) 计算出斜率 g, 然后对照表 1 得到相应的类型 t, 再对照表 2 得到对应的预测系数$\alpha_1,\alpha_2,\alpha_3,\alpha_4$, 最后将预测系数代入式 (9) 计算出预测值 $D_{\text{est}}(d)$.

$$g=|t_1-t_2|-|t_3-t_4| \tag{8}$$

$$D_{\text{est}}=\alpha_1 t_1+\alpha_2 t_3+\alpha_3 t_2+\alpha_4 t_4 \tag{9}$$

表 1 斜率分类

斜率 g	类型 t
$g\geq 40$	1
$40>g\geq 20$	2
$20>g\geq 8$	3
$8>g\geq 0$	4
$0>g\geq -8$	5
$-8>g\geq -20$	6
$-20>g\geq -40$	7
$g<-40$	8

表 2 预测系数和斜率类型对应关系

类型t	α_1	α_2	α_3	α_4
1	0.350	0.150	0.350	0.150
2	0.220	0.280	0.220	0.280
3	0.300	0.200	0.300	0.200
4	0.124	0.317	0.232	0.326
5	0.190	0.310	0.190	0.310
6	0.230	0.270	0.230	0.270
7	0.172	0.305	0.218	0.303
8	0.220	0.280	0.220	0.280

计算出预测误差后利用式 (10)–式 (12) 将该像素的第 T 位置 1 得到 $D_0(d)$, 置 0 得到 $D_1(d)$, 如果该像素在位置图标记为 0, 则 T=7; 如果该像素在位置图标记为 1, 则 T=8.

$$b'=\left\lfloor \frac{D(d)}{2^{(8-T)}} \right\rfloor \bmod 2,\ d=1,2,\cdots,L \tag{10}$$

$$D_0(d)=D(d)-b'\times 2^{(8-T)}+1\times 2^{(8-T)},\ d=1,2,\cdots,L \quad (11)$$

$$D_1(d)=D(d)-b'\times 2^{(8-T)},\ d=1,2,\cdots,L \quad (12)$$

其中, b'为 $D(d)$ 第 T 位的值.

然后由式 (13), 式 (14) 计算出预测误差 $R_0(d)$, $R_1(d)$.

$$R_0(d)=|D_0(d)-D_{\text{est}}(d)| \quad (13)$$

$$R_1(d)=|D_1(d)-D_{\text{est}}(d)| \quad (14)$$

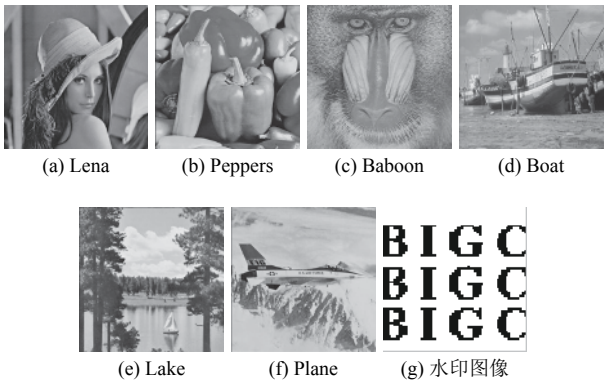
最后比较预测误差 $R_0(d)$, $R_1(d)$ 的大小, 误差较小的像素值作为恢复的像素值.

$$D_{\text{out}}(d)=\begin{cases} D_0(d), & R_0(d)\le R_1(d) \\ D_1(d), & R_0(d)>R_1(d) \end{cases} \quad (15)$$

式中, $D_{\text{out}}(d)$ 即为恢复的像素值.

3 实验结果分析

实验选取载体图像为 6 个大小为 512×512 像素的灰度图像, 以大小为 64×64 像素的图像作为水印图像进行实验. 如图 6 所示, 它们包括 Lena, Peppers, Baboon, Boat, Lake, Plane 以及水印图像“BIGC”.



(a) Lena (b) Peppers (c) Baboon (d) Boat

(e) Lake (f) Plane (g) 水印图像

图 6 实验中的 6 个测试图像 Lena, Peppers, Baboon, Boat, Lake, Plane 以及水印图像“BIGC”

3.1 算法完整性测试

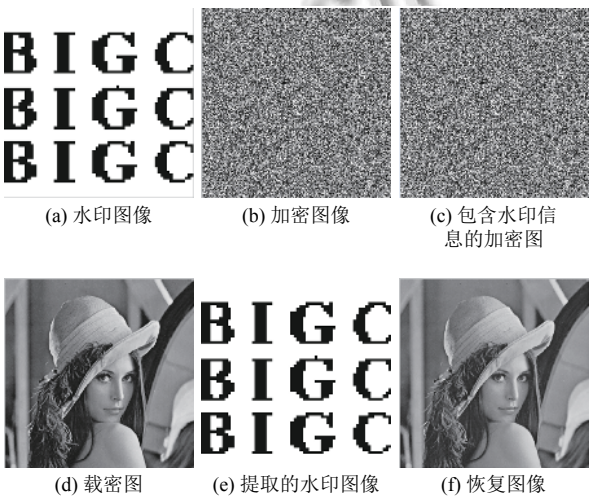
以图 6(a) 作为原始载体图像, 图 6(g) 作为待嵌入的大小为 64×64 像素的水印为例, 共嵌入 4096 位水印信息, 嵌入率为 0.156 25; 图 7(b) 为使用 ZUC 算法加密后得到的加密图像; 包含水印信息的加密图如图 7(c) 所示. 接收者接收到含有水印信息的加密图后先利用加密密钥解密图像得到含有水印信息的解密图如图 7(d) 所示; 再利用嵌入密钥从解密后的图像中成功地提取出嵌入的水印, 完整地恢复出原始图像. 提取水印和恢复图像如图 7(e), 图 7(f) 所示.

3.2 算法安全性分析

通过计算图像熵来分析加密图像安全性. 图像中平均信息量用信息熵表示. 信息熵计算如下:

$$H(X)=-\sum_{i=0}^{255}p(X_i)\log_2 p(X_i) \quad (16)$$

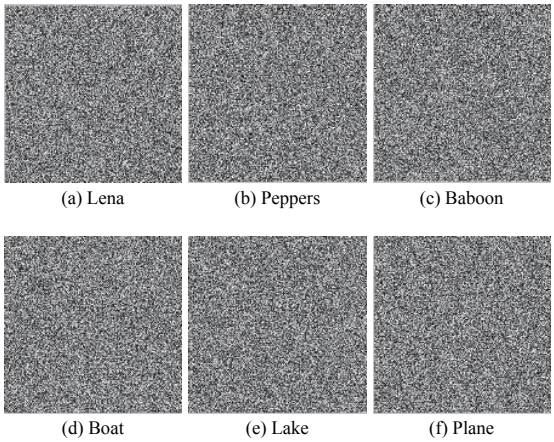
其中, $p(X_i)$°表示图像中灰度值为 X_i 的像素所占的比例, $H(X)$ 的最大理论值为 8, 通常, 熵越高, 图像越安全. 图 8 为 6 个测试图像的加密图, 表 3 显示了原始图像和加密图像的熵值; 由表 3 可知, 加密图像的所有熵值都非常接近最大理论值 8, 而原始图像的熵值却远离最大理论值, 这说明使用 ZUC 加密可以保证算法的安全性.



(a) 水印图像 (b) 加密图像 (c) 包含水印信息的加密图

(d) 载密图 (e) 提取的水印图像 (f) 恢复图像

图 7 以 Lena 图作为原始载体图像的测试效果图



(a) Lena (b) Peppers (c) Baboon

(d) Boat (e) Lake (f) Plane

图 8 实验中的 6 个测试图像的加密图

表 3 不同测试图像的原始图像和加密图像的熵

图像	原始图像信息熵$H(X)$	加密图像信息熵$H(X)$
Lena	7.5771	7.9902
Peppers	7.5797	7.9893
Baboon	7.3715	7.9897
Boat	7.1572	7.9885
Lake	7.4585	7.9898
Plane	6.7332	7.9893

通过实验得到 6 组图像的原始图像和加密图像的直方图如图 9 所示. 图 9(a)、图 9(c)、图 9(e)、图 9(g)、图 9(i)、图 9(k) 为原始图像的直方图. 图 9(b)、图 9(d)、图 9(f)、图 9(h)、图 9(j)、图 9(l) 是加密后的直方图, 通过对比可以明显看出较为平滑, 像素的比例较为均匀, 说明加密后的图像安全性更高.

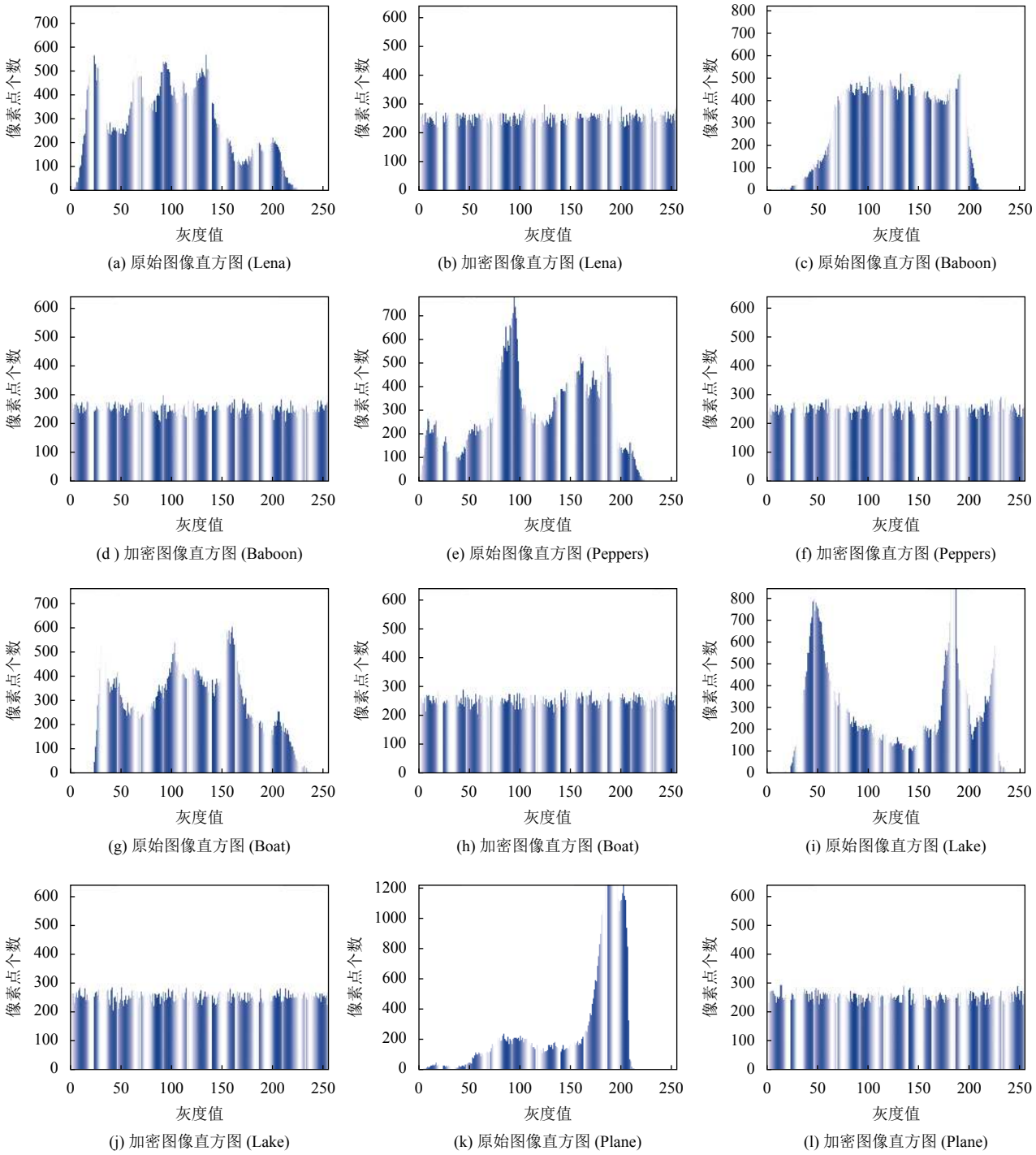


图 9 测试图像 Lena, Peppers, Baboon, Boat, Lake, Plane 加密前后直方图对比

3.3 算法嵌入能力测试

图 10 展示了对于图像 Lena, Lake, Baboon, Man 嵌入量与解密图像峰值信噪比的关系. 可以看出随着嵌入率的增加, 含水印的解密图像仍拥有较高的 PSNR 值.

本文算法与文献 [16–18] 的算法嵌入量与 PSNR 对比情况如图 11 所示.

从图 11 可以看出, 本文算法直接解密图像的 PSNR 大于文献 [17,18], 因此本文提出的方案具有更好的整体性能.

表 4–表 7 列出了不同嵌入率本文算法与文献 [17,18] 算法 PSNR 值的对比. 通过表格对比可以看出本文算法的直接解密和恢复图像的 PSNR 值最高, 说明该算法优于文献 [17,18].

4 结论

本文提出了一种可分离加密图像可逆水印算法, 与其他算法不同的是该算法在用 ZUC 算法加解密图像, 具有较高的安全性; 算法在嵌入水印信息前进行图像测试并标记, 保证了嵌入水印信息的像素在接收方能够完全恢复, 同时提高了恢复图像和直接解密图像的质量; 水印嵌入者用水印信息替换选中像素的第 T (T=7 或 8) 位完成水印信息的嵌入; 接收者根据嵌入密钥和加密密钥可以提取水印和恢复出原始载体图像. 通过实验对比分析了原始图像和加密图像的熵以及原始图像和加密图像的直方图, 证明了使用 ZUC 算法加密图像具有较高的安全性. 通过实验计算直接解密图像和恢复图像的 PSNR 值和 NC 值, 证明了本文算法的性能优于文献 [18] 的算法.

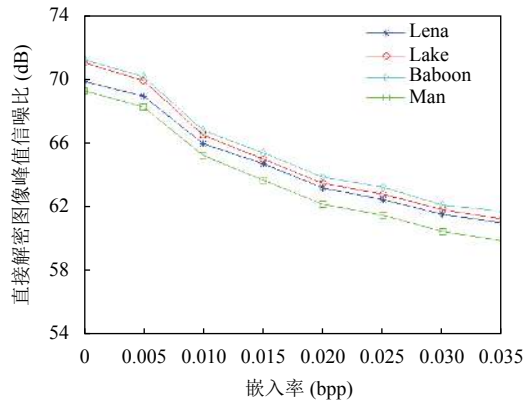


图 10 图像 Lena, Lake, Baboon, Man 嵌入率与直接解密图像峰值信噪比关系对比

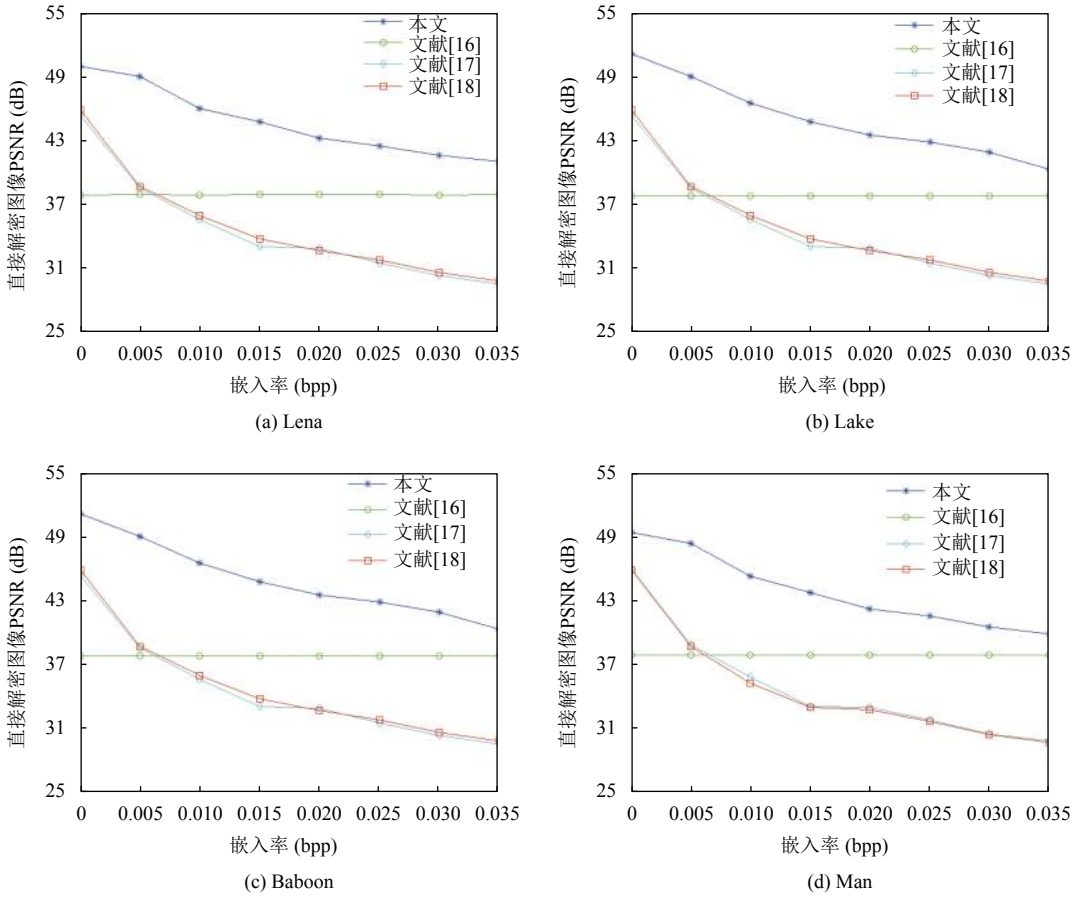


图 11 不同算法嵌入量与直接解密图像 PSNR 对比

表 4 本文算法和文献 [17]、文献 [18] 嵌入率和 PSNR 比较 (Lena)

嵌入位数	嵌入率 (bpp)	算法	直接解密图 PSNR (dB)	恢复图像 NC值
4096	0.0156	本文	44.40	1
		文献[17]	33.18	1
		文献[18]	33.19	1
16384	0.0625	本文	38.52	1
		文献[17]	27.04	1
		文献[18]	27.05	1
40960	0.1563	本文	32.53	1
		文献[17]	23.05	1
		文献[18]	23.06	1

表 5 本文算法和文献 [17]、文献 [18] 嵌入率和 PSNR 比较 (Baboon)

嵌入位数	嵌入率 (bpp)	算法	直接解密图 PSNR (dB)	恢复图像 NC值
4096	0.0156	本文	45.28	1
		文献[17]	32.71	1
		文献[18]	59.11	1
16384	0.0625	本文	38.52	1
		文献[17]	26.73	1
		文献[18]	27.05	1
40960	0.1563	本文	33.01	1
		文献[17]	22.76	1
		文献[18]	23.07	1

表 6 本文算法和文献 [17]、文献 [18] 嵌入率和 PSNR 比较 (Lake)

嵌入位数	嵌入率 (bpp)	算法	直接解密图像PSNR (dB)	恢复图像 NC值
4096	0.0156	本文	44.74	1
		文献[17]	33.10	1
		文献[18]	33.12	1
16384	0.0625	本文	38.93	1
		文献[17]	27.11	1
		文献[18]	27.11	1
40960	0.1563	本文	32.75	1
		文献[17]	23.06	1
		文献[18]	23.07	1

本文算法具有较高的安全性和性能, 但是由于嵌入水印时将图像分成了嵌入水印集合和非嵌入水印集合, 这使得水印的嵌入量有了一定的影响, 接下来的研究工作将从如何提高算法的嵌入量入手.

表 7 本文算法和文献 [17]、文献 [18] 嵌入率和 PSNR 比较 (Man)

嵌入位数	嵌入率 (bpp)	算法	直接解密图像PSNR (dB)	恢复图像 NC值
4096	0.0156	本文	43.42	1
		文献[17]	33.08	1
		文献[18]	33.10	1
16384	0.0625	本文	37.47	1
		文献[17]	27.08	1
		文献[18]	27.11	1
40960	0.1563	本文	31.70	1
		文献[17]	23.02	1
		文献[18]	23.04	1

参考文献

1 Gibson J, Rondeau R, Eveleigh D, *et al*. Benefits and challenges of three cloud computing service models. Proceedings of the 4th International Conference on Computational Aspects of Social Networks. Sao Carlos: IEEE, 2012. 198–205.

2 金聪. 数字水印理论与技术. 北京: 清华大学出版社, 2008.

3 Zhang XP, Wang SZ. Efficient steganographic embedding by exploiting modification direction. IEEE Communications Letters, 2006, 10(11): 781–783. [doi: 10.1109/LCOMM.2006.060863]

4 Zhang XQ, Sun ZR, Tang ZJ, *et al*. High capacity data hiding based on interpolated image. Multimedia Tools and Applications, 2017, 76(7): 9195–9218. [doi: 10.1007/s11042-016-3521-0]

5 Zhang XQ, Yu CQ, Wang XY, *et al*. A reversible data hiding scheme for JPEG images. ICIC Express Letters, 2013, 7(9): 2575–2580.

6 Hong W, Chen TS, Wu HY. An improved reversible data hiding in encrypted images using side match. IEEE Signal Processing Letters, 2012, 19(4): 199–202. [doi: 10.1109/LSP.2012.2187334]

7 Hong W, Chen TS, Wu HY, *et al*. An enhanced smoothness evaluation for reversible data hiding in encrypted images. Proceedings of SPIE 8334, 4th International Conference on Digital Image Processing (ICDIP 2012). Kuala Lumpur: SPIE, 2012. 833434.

8 Yu J, Zhu GP, Li XL, *et al*. An improved algorithm for reversible data hiding in encrypted image. In: Shi YQ, Kim HJ, Pérez-González F, eds. The International Workshop on Digital Forensics and Watermarking 2012. Heidelberg: Springer, 2013. 384–394.

9 Liao X, Shu CW. Reversible data hiding in encrypted images

based on absolute mean difference of multiple neighboring pixels. Journal of Visual Communication and Image Representation, 2015, 28: 21–27. [doi: 10.1016/j.jvcir.2014.12.007]

10 Zhang XP. Separable reversible data hiding in encrypted image. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 826–832. [doi: 10.1109/TIFS.2011.2176120]

11 Zhang XP, Qin C, Sun GL. Reversible data hiding in encrypted images using pseudorandom sequence modulation. In: Shi YQ, Kim HJ, Pérez-González F, eds. The International Workshop on Digital Forensics and Watermarking 2012. Heidelberg: Springer, 2013. 358–367.

12 Zhang XP, Qian ZX, Feng GR, *et al*. Efficient reversible data hiding in encrypted images. Journal of Visual Communication and Image Representation, 2014, 25(2): 322–328. [doi: 10.1016/j.jvcir.2013.11.001]

13 Ma KD, Zhang WM, Zhao XF, *et al*. Reversible data hiding in encrypted images by reserving room before encryption. IEEE Transactions on Information Forensics and Security, 2013, 8(3): 553–562. [doi: 10.1109/TIFS.2013.2248725]

14 Jagdale MV, Hingway SP, Suresh SS. Reversible encryption and data hiding. International Journal of Advance Research in Computer Science and Management Studies, 2014, 2(1): 293–299.

15 Zhang WM, Ma KD, Yu NH. Reversibility improved data hiding in encrypted images. Signal Processing, 2014, 94: 118–127. [doi: 10.1016/j.sigpro.2013.06.023]

16 Zhang XP. Reversible data hiding in encrypted image. IEEE Signal Processing Letters, 2011, 18(4): 255–258. [doi: 10.1109/LSP.2011.2114651]

17 Wu XT, Sun W. High-capacity reversible data hiding in encrypted images by prediction error. Signal Processing, 2014, 104: 387–400. [doi: 10.1016/j.sigpro.2014.04.032]

18 田野, 项世军. 可分离加密域可逆数据隐藏方案. 应用科学学报, 2015, 33(6): 585–594. [doi: 10.3969/j.issn.0255-8297.2015.06.002]

19 Ge HL, Chen Y, Qian ZX, *et al*. A high capacity multi-level approach for reversible data hiding in encrypted images. IEEE Transactions on Circuits and Systems for Video Technology, 2019, 29(8): 2285–2295. [doi: 10.1109/TCSVT.2018.2863029]

20 李志佳, 夏玮. 基于差值直方图平移的密文域可逆信息隐藏算法. 计算机工程, 2019, 45(11): 152–158.

21 周能, 张敏情, 林文兵. 基于秘密共享的可分离密文域可逆信息隐藏算法. 计算机工程, 2020, 46(10): 112–119.

22 任高峰, 乔树山, 黑勇. 祖冲之算法在数字图像加密中的应用与实现. 科学技术与工程, 2013, 13(3): 766–770. [doi: 10.3969/j.issn.1671-1815.2013.03.047]