

引用格式:吕冬梅,李国东. 基于密文域扩展和 DNA 双向编码的可逆水印算法[J]. 微电子学与计算机,2020,37(2):43-50.
[LV D M,LI G D. Reversible watermarking algorithm based on ciphertext domain extension and DNA bidirectional coding[J].
Microelectronics & Computer,2020,37(2):43-50.]

基于密文域扩展和 DNA 双向编码的可逆水印算法

吕冬梅,李国东

(新疆财经大学 统计与数据科学学院,新疆 乌鲁木齐 830012)

摘 要: 在综合考虑可逆水印算法的鲁棒性和嵌入容量的基础上,提出一种基于密文域扩展的加密域可逆水印算法,该算法不仅保证了高鲁棒性,还使嵌入容量高达 8.0625dB. 首先,基于 IWT 和 DNA 双向编码完成对二维载体图像和二维水印图像的加密,然后,基于密文域扩展将加密后水印嵌入加密后载体图像,最终,二维载体图像扩展为含水印的三维图像,算法完成. 采用 SSIM 评价指标对图像的恢复质量进行分析,SSIM 值为 1 说明文中算法实现了完全可逆,求得文中算法的嵌入容量为 8.0625dB,远大于其他文献,鲁棒性分析显示文中算法具有较好的鲁棒性. 该算法在保证原始载体内容安全的前提下实现了密文域中水印信息的完全可逆性及原始图像的无损恢复.

关键词: 可逆水印; IWT; DNA 双向编码; 密文域扩展; 鲁棒性

中图分类号: TP309

文献标识码: A

文章编号: 1000—7180(2020)02—0043—08

Reversible watermarking algorithm based on ciphertext domain extension and DNA bidirectional coding

LÜ Dong-mei, Li Guo-dong

(School of Statistics and Data Science, Xinjiang University of Finance and Economics,
Urumqi 830012, China)

Abstract: Based on the comprehensive consideration of the robustness and embedding capacity of the reversible watermarking algorithm, A cryptographic domain reversible watermarking algorithm based on ciphertext domain extension is proposed. This algorithm not only ensures high robustness, but also makes the embedding capacity as high as 8.0625dB. Firstly, the two-dimensional carrier image and the two-dimensional watermark image are encrypted based on IWT and DNA bidirectional encoding. Then, the encrypted watermark is embedded into the encrypted carrier image based on the ciphertext domain extension, and finally, the two-dimensional carrier image is converted into a watermarked image. Three-dimensional image, the algorithm is completed. The SSIM evaluation index is used to analyze the restoration quality of the image. The SSIM value is 1 and the algorithm is completely reversible. The embedding capacity of the algorithm is 8.0625dB, which is much larger than other literatures. The robustness analysis shows that the algorithm is better. The algorithm achieves the complete reversibility of the watermark information in the ciphertext domain and the lossless recovery of the original image under the premise of ensuring the security of the original carrier content.

Key words: reversible watermarking; IWT; DNA bidirectional coding; ciphertext domain extension; robustness

1 引言

近几年,可逆水印技术已经非常成熟.目前存在的可逆水印技术主要包含无损压缩^[1-2]、差值扩展^[3-4]、像素预测^[5]、直方图位移^[6-7]等.信息安全问题体现在机密性,可用性,完整性,认证性 4 个方面^[8],为保证这 4 个性能,大量学者将加密技术和水印技术有机结合.大多数水印算法是基于明文域的,即首先对明文图像嵌入水印,再将含水印图像加密^[9-12].

在综合考虑可逆水印算法的鲁棒性和嵌入容量的基础上,文中提出一种基于密文域扩展和 DNA 双向编码的加密域可逆水印算法.首先,依据基于混沌系统和 DNA 双向编码的加密技术,对二维水印图像进行加密.其次,依据基于 IWT 和 DNA 双向编码的混沌加密算法对二维载体载体图像进行加密,最后,将加密后水印嵌入加密后载体图像,嵌入算法为基于密文域扩展的可逆水印算法,该算法具有较强的鲁棒性,和较大的嵌入容量两特点.

2 基础知识

2.1 整数小波分解

一幅图像经过一层小波分解,其小波系数分为 4 部分,其意义分别如下:

- LL₁——图像的近似部分;
 - LH₁——水平方向图像细节;
 - HL₁——垂直方向图像细节;
 - HH₁——对角方向图像细节;
- 一般地,对图像进行二层小波分解是对近似部分 LL₁再次进行小波分解,得到二层分解结果 LL₂、LH₂、HL₂、HH₂.

加密过程的结果会引起图像信号在重构后发生图像降质,若进行多层小波分解,将引起更严重的降质.使用整数小波的优点是其小波系数都是整数,从而可以直接进行异或等运算,即使进行多层小波分解,经逆变换后仍没有失真.

2.2 DNA 双向编码及 DNA 代数操作

2.2.1 DNA 序列正向编码

将数值矩阵编码为 DNA 矩阵称为 DNA 序列正向编码.在传统 DNA 编码理论中,所有信息由含四中碱基的 DNA 序列表示.一般来说,灰度图像像素值取值为 0-255 区间内整数,可将每个像素值表示为 8 位二进制数.在二进制序列中,0 和 1 是互补的,可以推至序列 00 和 11 互补,01 与 10 互补,正

好对应 DNA 序列中的两两互补的碱基对.使用 00、01、10、11 来对 DNA 序列进行编码时,所有的编码方案共有 4! 种,其中只有 8 种编码方案符合 Watson-Crick 互补规则,如表 1 所示.

表 1 DNA 序列正向编码方案								
碱基	0	1	2	3	4	5	6	7
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
C	01	10	00	11	00	11	01	10
G	10	01	11	00	11	00	10	01

例如,一像素点的灰度值为 121,表示为 8 位二进制序列为 01111001,依据表 1 中编码规则 0 对二进制序列编码,结果为 CTGC,记为一个 DNA 组,一个像素点经过 DNA 序列正向编码后变成一个 DNA 组.

2.2.3 DNA 序列逆向编码

将 DNA 矩阵编码为数值矩阵称为 DNA 序列逆向编码.在尺寸为 N * N 的 DNA 矩阵中,每个元素为一个 DNA 组,每个 DNA 组由四个碱基构成,在一个规则里,编码方案有 4^4=256 种,如表 2 所示.则编码规则有 256 种,文中基于混沌序列对其顺序进行重排.例如,若将表 2 视作其中一种编码规则,一个尺寸为 2 * 2 的 DNA 矩阵为 $\begin{bmatrix} ATAA & ACAA \\ ACCA & GGGG \end{bmatrix}$,根据该 DNA 逆向编码规则可表示为数值矩阵 $\begin{bmatrix} 1 & 4 \\ 5 & 255 \end{bmatrix}$.

表 2 DNA 序列逆向编码方案							
0	1	2	3	4	5	...	255
A	A	A	A	A	A	...	G
A	T	T	T	C	C	...	G
A	A	T	T	A	C	...	G
A	A	A	T	A	A	...	G

DNA 双向编码为 DNA 编码注入了新活力.将 DNA 编码用入加密过程,其算法流程一般如图 1 所示,例如文献[13]、[14].文中在加密算法中使用 DNA 双向编码,流程如图 2 所示,减少了运算量.



图 1 基于 DNA 编码的一般加密流程

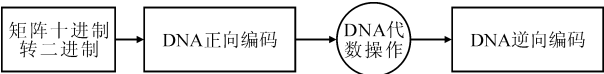


图 2 基于 DNA 双向编码的加密流程

2.2.3 DNA 序列的加与减代数操作

DNA 加操作如表 3 所示,表现为双螺旋结构,符合 Watson-Crick 互补规则;DNA 减操作如表 4 所示,与加操作相反,但不符合双螺旋结构,只把减操作作为对应的解密规则。

表 3 DNA 加操作				
+	A	T	C	G
A	A	T	G	G
T	T	G	A	C
C	C	A	G	T
G	G	C	T	A

表 4 DNA 减操作				
—	A	T	C	G
A	A	C	T	G
T	T	A	G	C
C	C	G	A	T
G	G	T	C	A

2.3 混沌系统

新四维超混沌如式(1)所示:

$$\begin{cases} \dot{x}_1 = -a_1x_1 + b_1x_2 \\ \dot{x}_2 = -a_1x_1 - x_1x_3 - x_2 - x_4 \\ \dot{x}_3 = x_1x_2 - c_1(x_1 + x_3) \\ \dot{x}_4 = k_1x_1 \end{cases} \quad (1)$$

式中,参数 $a1 = 20, b1 = 35, c1 = 5, k1 = 4$ 时,式(1)处于超混沌状态..

超混沌 chen 系统如式(2) 所示:

$$\begin{cases} \dot{y}_1 = a_2(y_2 - y_1) \\ \dot{y}_2 = -y_1y_3 + b_2y_1 + c_2y_2 - y_4 \\ \dot{y}_3 = y_1y_2 - d_2y_3 \\ \dot{y}_4 = y_1 + k_2 \end{cases} \quad (2)$$

式中, $a2 = 36, b2 = -16, c2 = 28, d2 = 3, k2 = [-0.7, 0.7]$ 时,式(2)处于超混沌状态.

2.4 加密域中数值溢出现象的处理

加密域中的负数和小数的表示一般是采用数据搬移和乘以扩展因子来实现的.文中采用基于整数小波域的加密算法,数值溢出主要表现为负整数和大于 255 的正整数两类.文中采用 12+1 模式来标记各数,前 12 位为数值位,最后 1 位为符号位.若该

数大于 0,则末位记为‘0’,若小于 0,则记为‘1’.例如,小波逆变换后系数为-1011,根据 12+1 模式表示为‘00111111100111’.

3 加密域水印系统

对载体图像 H 嵌入双重水印 W 和 I.首先,依据基于混沌系统和 DNA 双向编码的加密算法,对二维水印图像 I 进行加密.其次,对以明文形式嵌入二值水印 W 后的载体图像 H 进行加密,加密算法为基于 IWT 和 DNA 双向编码的混沌加密算法.最后,将加密后水印 I 嵌入加密后载体图像,嵌入算法为基于密文域扩展的可逆水印算法,该算法具有较强的鲁棒性,和较大的嵌入容量两特点.

3.1 水印图像加密

为了保证水印图像的安全性,采用基于混沌系统和 DNA 双向编码的加密算法完成对水印图像的加密.

步骤 1 生成混沌序列

(1) 将初始条件 $X0 = [0.1\ 0.2\ 0.3\ 0.4]$ 代入式(1),迭代 $1000 + N \times N$ 次,得序列 X_1, X_2, X_3, X_4 .将初始条件和迭代次数 1000 记为密钥 K_1, K_2, K_3, K_4, K_5 .

(2) 将初始条件 $Y0 = [1.1\ 2.2\ 1.3\ 2.4], k2 = 0.157$ 代入式(2),迭代 $2000 + N \times N$ 次,得序列 Y_1, Y_2, Y_3, Y_4 .将初始条件、参数 k_2 和迭代次数 2000 记为密钥 $K_6, K_7, K_8, K_9, K_{10}, K_{11}$.

步骤 2 像素置乱.

(1) 设水印图像为尺寸 $N \times N$ 的矩阵 I ,将矩阵 I 中像素位置坐标 (x, y) 根据式(3)更新为 (x', y') ,位置更新后水印记为 I_1 .

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab + 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \quad (3)$$

式中, a, b 分别作为密钥保存为 K_{12}, K_{13} .

(2) 将 I_1 转化为一维向量 I_2 ,转化规则如图 3 所示,按 ①②③④⑤… 的规则排列.

$$I_2 = [I_1(1, :), I_1(2; N, 1), I_1(2, 2; N), I_1(3; N, 2) \cdots I_1(N, N)] \quad (4)$$

(3) 取序列 X_1 后 $N \times N$ 项存入矩阵 key_1, key_{11} 为 key_1 降序排列后的索引序列,依据 key_{11} 对 I_2 进行置乱,置乱后矩阵为 I_3 .

$$I_3(i) = I_2(key_{11}(i)), i = 1, 2, 3, \cdots, N \times N; \quad (5)$$

步骤 3 像素扩散

(1) 取序列 X_2 后 $N \times N$ 项存入矩阵 key_2 ,由式

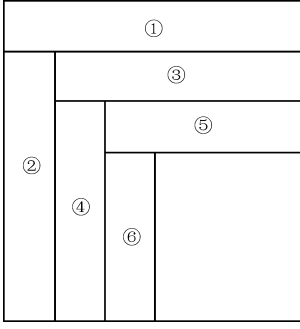


图3 矩阵重组示意图

(6) 将矩阵 key_2 量化为矩阵 key_{21} .

$$key_{21} = \text{reshape}(\text{mod}((key_2 - \text{floor}(key_2)) * 10^{14}, 256), N, N) \quad (6)$$

式中, reshape 为按列读取重组矩阵为 N 行 N 列矩阵, mod 为取模运算. 同全文.

(2) 由式(7)将 I_3 矩阵重组为 I_4 矩阵.

$$I_4 = \text{reshape}(I_3, N, N) \quad (7)$$

(3) 根据正向编码规则 7, 对矩阵 key_{21} 和矩阵 I_4 进行 DNA 正向编码, 并进行 DNA 加操作, 得 DNA 矩阵 I_5 ,

从序列 X_2 3500 处往后取 256 项, 求其索引序列并对编码方案进行重排, 得一组编码规则, 根据该规则对矩阵 I_5 进行 DNA 逆向编码, 并记结果为矩阵 I_6 , 该矩阵尺寸为 $N \times N$, 其中元素为取值在 $[0, 255]$ 区间的数值.

将正向编码规则 7 和数值 3500 记为密钥 K_{14}, K_{15} .

(4) 取序列 X_3 后 $N \times N$ 项存入矩阵 key_3 , 由式(8)将 key_3 矩阵量化为 key_{31} 矩阵.

$$key_{31} = \text{reshape}\left(\frac{\text{mod}((key_3 - \text{floor}(key_3)) * 10^{14}, 256), N, N}{10^{14}}, N, N\right) \quad (8)$$

(5) 将矩阵 I_6 与矩阵 key_{31} 做异或操作, 如式(9)所示, 记结果为 I_7 .

$$I_7(i) = I_6(i) \oplus key_{31}(i), \quad i = 1, 2, 3, \dots, N \times N; \quad (9)$$

3.2 载体图像加密

步骤 1 设载体图像为尺寸 $N \times N$ 的矩阵 H , 对矩阵进行 2 级整数小波变换, 变换结果见 H_1 , 其中 LL_1, LH_1, HL_1, HH_1 为一级小波系数, LL_2, LH_2, HL_2, HH_2 为二级小波系数.

$$H_1 = \begin{bmatrix} LL_1 & LH_1 \\ HL_1 & HH_1 \end{bmatrix};$$

$$\text{式中: } LL_1 = \begin{bmatrix} LL_2 & LH_2 \\ HL_2 & HH_2 \end{bmatrix};$$

步骤 2 为了提高水印的不可见性, 选择 HH_2 区域为水印图像 W 的嵌入区域, 嵌入方法为 LSB 算法^[15](最低有效位直接替代法), 并保留 HH_2 区域最低位放入矩阵 HH_2_L , 其尺寸为 $\frac{N}{4} \times \frac{N}{4}$.

步骤 3 对更新后小波系数进行 1 层小波逆变换, 得到矩阵 H_2 .

$$H_2 = \begin{bmatrix} LL1_new & LH1 \\ HL1 & HH1 \end{bmatrix}$$

步骤 4 取序列 X_4 后 $N \times N$ 项存入矩阵 key_4 , 根据式(4)将 key_4 矩阵量化为 key_{41} 矩阵.

步骤 5 根据正向编码规则 3, 对 H_2, key_{41} 进行 DNA 正向编码, 并进行 DNA 加操作, 得 DNA 矩阵 H_3 .

从 X_4 序列 4 500 处往后取 256 项, 求其索引序列并对编码方案进行重排, 得一组编码规则, 根据该规则对矩阵 H_3 进行 DNA 逆向编码, 记结果为矩阵 H_4 .

记正向编码规则 3 和数值 4 500 为密钥 K_{16}, K_{17} .

步骤 6 对矩阵 H_4 进行 1 层小波逆变换, 得到矩阵 H_5 .

步骤 7 将 H_5 转化为一维矩阵 H_6 , 转化规则为式(10).

$$H_6 = [H_5(:, 1), H_5(1, 2:N), H_5(2:N, 2), H_5(2, 3:N) \dots H_5(N, N)] \quad (10)$$

步骤 8 取序列 Y_1 后 $N \times N$ 项存入矩阵 key_5 , key_{51} 为 key_5 升序排列后的索引序列, 如(11)、(12)所示, 依据 key_{51} 对 H_6 进行置乱, 将置乱后矩阵重组为尺寸为 $N \times N$ 的矩阵 H_8 .

$$H_7(i) = H_6(key_{51}(i)), i = 1, 2, 3, \dots, N \times N; \quad (11)$$

$$H_8 = \text{reshape}(H_7, N, N) \quad (12)$$

3.3 水印嵌入

文中提出一种基于密文域扩展的嵌入策略, 不仅可以在完全不损坏载体图像的情况下嵌入水印, 还保证了很大的嵌入空间.

步骤 1 在整数小波域上对图像进行加密, 小波逆变换后的 H_8 矩阵存在元素数值溢出现象, 根据 2.4 节对 H_8 矩阵依据 12+1 模式标记各数, 记结果为 H_9 .

步骤 2 将 I_7 矩阵中各元素表示为 8 位二进

制,记结果为 I_8 .

步骤3 如表5所示,选取方式3将 H_9 、 I_8 结合,得到长度为 $N \times 21N$ 的矩阵 H_{10} ,矩阵里元素为‘0’和‘1’.记方式3为 K_{18} .

表5 矩阵拼接结合方式

编号	结合方式
1	$H_{10} = [H_9; I_8]$
2	$H_{10} = [I_8(:,1); H_9(:,1); I_8(:,2); H_9(:,2); \dots; H_9(:,21N)]$
3	$H_{10} = [I_8(:,1:2); H_9(:,1:2); I_8(:,3:4); \dots; H_9(:,21N)]$
4	$H_{10} = [I_8(:,1:3); H_9(:,1:3); I_8(:,4:6); \dots; H_9(:,21N)]$
.....	
$N+1$	$H_{10} = [I_8; H_9]$

步骤4 根据式(1)将 H_{10} 更新为 H_{11} .

步骤5 取序列 Y_2 后 $N \times N$ 项存入矩阵 key_6 ,生成二值矩阵 key_{61} .

生成规则如图4所示:取矩阵 key_6 里每个元素小数点后的第3、5、7位,若 $i \geq 5$,则 $i = 1$,否则 $i = 0$;其中, key_6 为 $N \times N$, key_{61} 为 $3N \times N$.

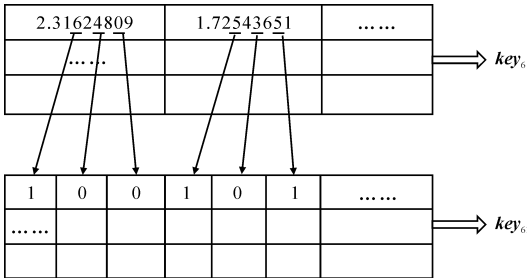


图4 取位示意图

步骤6 将矩阵 HH_2L 放入矩阵 key_{61} ,得矩阵 key_{62} ,并将位置保存为密钥 K_{19} , K_{19} 表示矩阵 HH_2L 的首位元素处于矩阵 key_{61} 中的横纵坐标.

步骤7 将 key_{62} 和 H_{11} 相结合,构成24位加密矩阵 H_{12} ,其尺寸为 $N \times 24N$,元素取值为0或1.

$$H_{12} = [key_{62}; H_{11}] \quad (13)$$

步骤8 取 Y_3 序列后 $N \times N$ 项存入矩阵 key_7 ,取序列 Y_4 后 $N \times 2N$ 项存入矩阵 key_8 ,构成尺寸为 $N \times 3N$ 的密钥矩阵 key_9 ,将其量化得 key_{10} ,将其中元素由十进制转化为二进制,得一尺寸为 $N \times 24N$ 的矩阵 key_{11} ,矩阵里各元素取值为0或1.

步骤9 将 key_{11} 与 H_{12} 进行异或操作,结果存入矩阵 H_{13} ,依据从左到右顺序分成3个 $N \times 8N$ 矩阵,并分别命名为矩阵 R_f, B_f, G_f ,依据从左到右,从上到下顺序将每8个二值元素转成一个十进制数,

得到三个尺寸为 $N \times N$,元素取值范围为 $[0,255]$ 区间上整数的矩阵,并将三个矩阵合并最终构成一张彩色图像 H_{14} .

3.4 水印提取

水印提取过程为3.3节的逆过程,流程如图5所示.

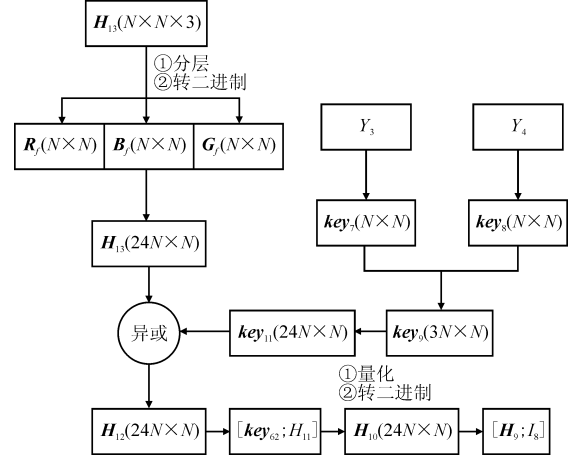


图5 水印提取流程图

依据密钥 K_{17} 提取水印 W .将 I_8 转化为十进制矩阵,即得加密后水印图像,依据水印图像加密算法的逆过程可得到正确水印.

3.5 载体图像解密

解密为3.2节的逆过程.

4 实验与分析

4.1 算法安全性分析

文中的水印算法依赖于混沌系统的内随机性,初值敏感性.文中采用两个超混沌动力学系统作为密钥流发生器.超混沌系统的动力学行为在更多的方向上进行拉伸折叠,其动态行为比混沌系统更复杂,在混沌加密方面,超混沌系统通常比混沌系统具有更好的效果和更为广泛的前景.文中具有19个密钥,混沌初始值密钥有8个,足以保障算法的安全性.

4.2 可逆回复质量分析

对算法进行仿真,测试载体对象为灰度图像 lena、Boat、Jet,水印图像为 I、W-A、W-B.三幅测试载体图像和水印图像 I 尺寸均为 256×256 ,水印图像 W-A、W-B 尺寸均为 16×16 .通过对比图6-9中明文图像和恢复图像可知,文中算法在保证载体图像完全无损的情况下嵌入和提取水印图像,恢复后载体图像与明文图像完全相同,并且提取的水印图像和明文水印图像完全相同,实现了无损载体图像的完全可逆水印技术.

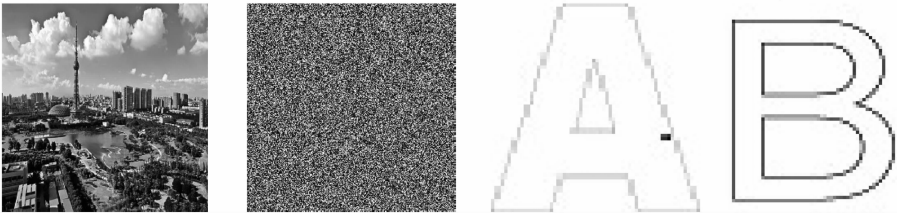


图 6 水印图像



图 7 lena 图像加密域可逆水印效果



图 8 Boat 图像加密域可逆水印效果



图 9 Jet 图像加密域可逆水印效果

文中采用结构相似性(SSIM)来衡量提取水印和原始明文水印之间,明文载体图像和恢复载体图像之间的质量.

SSIM 是用来衡量两幅图像相似度的新指标,从亮度,对比度和结构 3 个方面衡量图像的相似性.为了简化 SSIM 的计算,本文设置 $\alpha = \beta = \gamma = 1, C3 = C2/2$,简化后的 SSIM 为

$$SSIM(x,y)=\frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)}$$

(14)

表 6 3 种算法关于恢复质量比较结果

衡量指标	图像	算法		
		文献 16	文献 17	文中
SSIM 明文图 像和恢 复图像	Lena	0.997 5	0.994 5	1
	Boat	0.996 8	0.997 3	1
	Pepper	0.997 5	0.996 4	1
	Jet	0.998 2	0.996 7	1
SSIM 明文水 印和提 取水印	Lena	0.986 3	0.995 1	1
	Boat	0.998 6	0.994 8	1
	Pepper	0.998 1	0.996 9	1
	Jet	0.997 4	0.997 5	1

如果两幅图像越接近,SSIM 的值越接近 1;若两幅图像完全相同,则 SSIM 的值为 1.

表 6 为文中算法和文献[16]、[17]中可逆水印算法关于恢复质量的比较结果. 本文算法和文献 16、17 都实现了密文域水印技术. 由表 6 可知,相比文献[16]、[17],文中算法具有更好的性能,文中算法的 SSIM = 1,因此本文算法实现了水印的完全可逆技术.

4.3 嵌入容量分析

水印嵌入容量是指单位像素嵌入的比特数,即

$$C = \frac{E}{M \times N} \tag{15}$$

式中,C 是容量;M、N 是被测图像的宽度和高度;E 是嵌入像素值比特总量. 文中嵌入了双重水印 I 和 W,其中 I 的尺寸为 $N \times N$,W 同它的嵌入区域 HH_2_L 尺寸相同,为 $\frac{N}{4} \times \frac{N}{4}$. 其中 I 为灰度图像,W 为二值图像. 由表 7 所示,本文的嵌入容量为 8.0625. 远大于文献[16]、[17]中算法的嵌入容量.

表 7 最大容量比较

方法	最大容量
文中	8.0625
文献 16	0.25
文献 17	0.92

4.4 鲁棒性分析

为了验证文中算法的鲁棒性,对含水印密文图像实施了不同的常见攻击,如随机噪声、中值滤波、图像平滑、卷积模糊等,通过计算原始水印和提取出的攻击后图像的水印的相似度. 由表 8 可知,文中算法在遭遇不同种类的攻击后,仍能较好的恢复出水印图像.

表 8 不同攻击下提取的水印图像-原始水印图像相似度比较结果

	Lena	Boat	Jet
随机噪声	0.894 7	0.891 6	0.914 4
中值滤波	0.856 1	0.879 5	0.891 5
图像平滑	0.902 5	0.901 3	0.882 6
卷积模糊	0.876 9	0.910 2	0.872 9

5 结束语

为综合考虑加密域水印算法的鲁棒性和水印嵌入容量,文中提出了一种基于密文域扩展和 DNA 双向编码的加密域可逆水印技术. 该算法在保证载体图像无损的情况下在加密域中嵌入灰度水印图

像,使嵌入容量高达 8.0625 dB,而且文中算法能够抵抗一些常见攻击,如随机噪声、中值滤波等. 然而,文中算法将水印图像和载体图像相结合,使二维载体图像变成三维图像,是在牺牲 PSNR 值的情况下提升嵌入容量,这也是下一步工作的重点.

参考文献:

[1] FRIDRICH J,GOLJAN M,DU R. Lossless data embedding - new paradigm in digital watermarking[J]. EURASIP Journal on Applied Signal Processing,2002 (2):185-196.

[2] ELIK M U,SHARMA G,TEKALP A M, et al. Lossless generalized-LSB data embedding[J]. IEEE Transactions on Image Process, 2005, 14 (2): 253-266.

[3] TIAN J. Reversible Data Embedding Using a Difference Expansion[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13 (8): 890-896.

[4] DRAGOI I-C, COLTUC D. Local-prediction-based difference expansion reversible watermarking [J]. IEEE Trans on Image Processing, 2014, 23 (4): 1779-1790.

[5] LUO L, CHEN Z, CHEN M, et al. Reversible image watermarking using interpolation technique. IEEE Transactions on Information Forensics and Security , 2010,5(1) : 187-193.

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

[7] 王俊祥,倪江群,潘金伟. 一种基于直方图平移的高性能可逆水印算法[J]. 自动化学报,2012,38(1) : 88 - 96.

[8] 石慧,冯斌,王相海,等. 用于盗版追踪的格雷码加密域可逆水印研究[J]. 中国图象图形学报,2018,23(11): 1635-1651.

[9] 李琦,颜斌,陈娜,等. 基于单向预测误差扩展的三维医学图像可逆水印算法[J]. 计算机应用,2019,39(2): 483-487.

[10] 陈青,李伟,卜莹. 基于整数小波变换与矩阵分解的兴趣区域可逆水印算法研究[J]. 包装工程,2019,40 (5):219-224.

[11] 项世军,罗欣荣,石书协. 一种同态加密域图像可逆水印算法[J]. 计算机学报,2016,39 (3) : 571-581.

[12] 罗昊,谢晓尧,彭长根. 基于直方图平移的加密域可逆水印算法[J]. 郑州大学学报(理学版),2018,50(2): 29-34.

[13] 包林霞. 基于 DNA 编码与非涅尔域变换的光学图像

加密[J]. 光学技术,2018,44(6):757-762.

[14] 冉维, 韦鹏程, 段昂. 融合多混沌映射和 DNA 编码的图像加密算法[J]. 计算机工程与设计, 2018, 39(7): 2020-2026.

[15] 宫海梅. 基于不同图层的 LSB 自适应数字水印隐藏算法研究[J]. 电子测试, 2016(21):58-5.

[16] AL-QERSHI O M, KHOO B E. Two-dimensional difference expansion (2D-DE) scheme with a characteristics-based threshold [J] . Signal Processing, 2013, 93(1):154-162.

[17] LEI B, TAN E-L, CHEN S, et al. Reversible water-

marking scheme for medical image based on differential evolution [J]. Expert Systems with Applications, 2014, 41 (7) : 3178-3188.

作者简介:

吕冬梅 女, (1995-), 硕士研究生. 研究方向为数据挖掘与图像处理. E-mail:1481696500@qq. com.

李国东 男, (1972-), 博士, 教授. 研究方向为数据与图像处理.