计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2021,30(11):266−272 [doi: 10.15888/j.cnki.csa.008206]

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

基于 Arnold 置换的交换加密水印算法①

赵培越, 张珍珍, 丁海洋, 李子臣

(北京印刷学院 信息工程学院, 北京 102600)
通讯作者: 赵培越, E-mail: zhaopy1996@163.com

摘　要: 针对载体图像内容安全与数字水印版权保护, 结合 Arnold 置换与直方图平移可逆水印算法, 提出基于 Arnold 置换的交换加密水印算法. 算法利用置换后图像直方图不变的特性, 将在密文中嵌入水印的操作映射到明文中, 实现了加密与水印操作先后顺序的交换. 在提取水印时, 可直接从含水印的密文中提取水印, 也可解密后再提取水印. 实验结果表明, 该算法加密操作与水印嵌入操作间的先后顺序不影响含水印密文的生成, 解密操作与水印提取操作的先后顺序不影响水印提取与图像恢复, 且直接解密得到的含水印明文图像质量较高, 水印的不可见性好, 算法有较高的效率.

关键词: 图像置换; 直方图平移; 数字水印; 交换加密水印算法

引用格式: 赵培越,张珍珍,丁海洋,李子臣.基于 Arnold 置换的交换加密水印算法.计算机系统应用,2021,30(11):266–272. http://www.c-s-a.org.cn/1003-3254/8206.html

Commutative Encryption and Watermarking Algorithm Based on Arnold Permutation

ZHAO Pei-Yue, ZHANG Zhen-Zhen, DING Hai-Yang, LI Zi-Chen

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

Abstract: To protect the security of carrier image content and digital watermark copyright, this study proposes a commutative encryption and watermarking algorithm integrating the Arnold permutation and histogram translation-based reversible watermarking algorithm. Taking advantage of the invariance of the image histogram after Arnold permutation, the algorithm maps the operation of watermark embedding in ciphertext to plaintext, which realizes the exchange of encryption and watermark embedding in operation sequence. The watermark can be extracted directly from the watermarked ciphertext, or be extracted after decryption. Experimental results show that the sequence of encryption and watermark embedding of this algorithm does not affect the generation of watermarked ciphertext, and the sequence of decryption and watermark extraction does not influence watermark extraction and image restoration. In addition, the direct decryption yields high-quality watermarked plaintext images, good invisibility of the watermark, and high efficiency of the algorithm.

Key words: image permutation; histogram translation; digital watermark; commutative encryption and watermarking

① 基金项目: 国家自然科学基金 (61370188); 北京市教委科研计划一般项目 (KM202010015009); 北京市教委科研计划 (KM202110015004); 北京印刷学院博士启动金项目 (27170120003/020); 北京印刷学院科研创新团队项目 (Eb202101)
Foundation item: National Natural Science Foundation of China (61370188); General Project of Scientific Research Plan of Beijing Municipal Education Commission (KM202010015009); Scientific Research Plan of Beijing Municipal Education Commission (KM202110015004); Start-up Fund for Ph.D. Student of Beijing Institute of Graphic Communication (27170120003/020); Scientific Research and Innovation Project of Beijing Institute of Graphic Communication (Eb202101)
收稿时间: 2021-02-09; 修改时间: 2021-03-17; 采用时间: 2021-04-02; csa 在线出版时间: 2021-10-22

1 引言

近年来, 互联网、云计算、大数据等技术朝着高效快速的方向发展, 数据隐私保护和信息安全[1] 日益受到重视, 其中图像加密和数字水印成为了研究的热点. 在一些特殊领域如医学、军事、卫星监测等需要对图像进行处理, 将密码技术与数字水印结合到一起, 提供了图像加密与水印共存的安全保护方案[2].

图像置换作为一种重要的图像加密和技术, 其目的是将目标图像进行一定程度上的修改, 使其包含的真实信息可以不被破坏地隐藏起来, 这样便具有不可见性, 保证了图像传输的安全性. 其基本思想是将数字图像作为矩阵进行有限次的初等置换来使图像的像素点变得混乱无序, 从而实现加密效果. 典型的有幻方置换、骑士巡游置换、Fibonacci 置换、基于 Hilbert 曲线置换[3] 等算法. 其中 Arnold 置换直观、简单、具有周期性, 使用非常方便, 该方法使像素的移动具有混沌特性, 加密后的图像安全性较高.

水印算法根据操作域的不同可分为 3 类: 空域算法、频域算法以及压缩域算法. 空域算法有基于 LSB 的水印算法、基于差值扩展的水印算法[4] 和基于无损压缩的水印算法[5] 等. 其中基于直方图平移的可逆水印算法[6] 是最具代表性的算法之一. 文献 [7] 对图像分块, 建立多个差值直方图来嵌入水印信息; 文献 [8] 通过混沌加密与直方图平移结合, 实现了无损提取水印信息, 但其水印嵌入容量十分有限; 文献 [9] 利用多组差值直方图平移获取更多差值, 通过图像分块和边缘差值嵌入, 虽然提高了嵌入率, 但是其含水印图像质量随之下降. 文献 [10] 提出了对载体图像进行分块置换加密, 并通过 DCT 变换来嵌入水印信息, 文献 [11] 对水印信息进行置换加密, 对载体图像进行分块后过 DCT 变换与直方图平移来嵌入水印.

交换加密水印算法是现阶段实现密码技术和水印技术相结合的一种主要方法. 文献 [12] 最先提出了交换加密水印技术 (Commutative Encryption and Watermarking , CEW), 将加解密、水印嵌入、提取融合到一起, 在发送前既可先加密后嵌水印, 也可先嵌水印后加密, 均能得到含水印的密文; 在发送后既可从密文中先提取水印, 再解密恢复图像, 也可先解密, 再提取水印恢复图像[13]. 而置换加密后不会对图像的某些统计特征造成影响[14], 所以可通过修改原始载体图像的统计特征来嵌入水印从而实现交换加密水印算法. 文献 [15] 将原始载体图像分组嵌入比特信息后, 通过修改数据最低比特, 使得全组数据之和的奇偶性与对应嵌入的水印信息相同, 并在同组数据范围内进行置换从而实现 CEW, 但仅对载体数据进行置乱, 安全性有待提高. 文献 [16] 通过空间位置置换及修改载体图像直方图嵌入水印信息实现 CEW.

基于对上述算法的研究, 利用 Arnold 置换前后直方图不变的特性, 提出了一种基于 Arnold 置换的交换加密水印算法. 原始载体图像先进行分块, 再进行块内和块间的置换加密, 通过直方图平移来实现水印嵌入. 加密操作与水印嵌入操作的顺序不影响含水印密文的生成, 且解密操作与水印提取操作的顺序不影响水印信息的提取与图像的恢复. 实验结果表明, 该算法可以无损恢复原始载体图像并提取水印, 且解密后的含水印明文图像质量高, 水印的不可见性好.

2 基本原理

本节主要介绍 Arnold 置换, 直方图平移可逆水印算法及交换加密水印算法.

2.1 Arnold 置换

Arnold 置换 (又称猫脸置换) 是一种基于古典密码体制的图像加密算法, 本质上是对长宽相等的图像中像素点的位置进行多次矩阵运算, 从而改变空间中像素点的位置, 破坏图像相邻像素点之间的相关性.

2.1.1 Arnold 置换原理

传统的 Arnold 置换[3] 的矩阵形式可以表达为: 设有平面点集$S=[0,1]\times[0,1]$, 对$(x,y)\in S$则有:

$$\begin{bmatrix} x' \\ y' \end{bmatrix}=\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}(\mathrm{mod}\ 1) \tag{1}$$

若 (x,y) 为二维图像坐标, 那么上述置换可以转化为:

$$\begin{bmatrix} x' \\ y' \end{bmatrix}=\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}(\mathrm{mod}\ N) \tag{2}$$

置换矩阵可设为$C=\begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix}$, 则:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix}=\begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix}\begin{bmatrix} x_n \\ y_n \end{bmatrix}(\mathrm{mod}\ N) \tag{3}$$

其中, n 代表第 n 次变换.

2.1.2 Arnold 置换的周期性

Arnold 置换具有周期性[17], 通过对一个 4×4 矩阵

进行 Arnold 置换来说明 Arnold 的周期性.

设原始矩阵为$A=\begin{bmatrix}1&2&3&4\\5&6&7&8\\9&10&11&12\\13&14&15&16\end{bmatrix}$, 分别对该矩阵进行 1,2,3 次 Arnold 置换. 得出 3 次置换后的矩阵分别为:

$$\begin{bmatrix}1&14&11&8\\12&5&2&15\\3&16&9&6\\10&7&4&13\end{bmatrix}\quad\begin{bmatrix}1&7&9&15\\6&12&14&4\\11&13&3&5\\16&2&8&10\end{bmatrix}$$

$$\begin{bmatrix}1&2&3&4\\5&6&7&8\\9&10&11&12\\13&14&15&16\end{bmatrix}$$

可以看到经过 3 次置换后, 矩阵 A 恢复成原始状态. Arnold 置换周期与图像阶数的关系见表 1.

2.1.3　Arnold 置换恢复算法

解密时需要用到 Arnold 置换恢复算法. 目前归纳的 Arnold 置换恢复算法[18] 有 3 种: 一是利用周期恢复; 二是通过逆矩阵恢复; 三是解方程组法. 本算法利用周期性来恢复.

设大小为 $N\times N$ 的图像进行 Arnold 置换, 置换了 n 次, Arnold 置换周期为 T, 以此求恢复图像. 已经置换 n 次, 利用置换周期, 只要再经过$T-(n \mod T)$次即可恢复原图.

2.2　基于直方图平移的可逆水印算法

文献 [19] 提出了基于直方图平移的信息隐藏基本方案, 直方图中横坐标是灰度值, 纵坐标是该灰度值对应的像素点的数量, 而每一个竖条称为一个 bin. 直方图中最高的那个点, 就称为峰点 P. 最低的那个点 (通常为 0), 叫做零点 Z (如无为 0 的点, 可以将灰度值为 254 的点的灰度值改为 255, 并进行标记, 以此空出 254 位置, 最后可根据标记恢复).

对灰度图像直方图进行分析, 通过将直方图峰值点与零点的像素平移来空出嵌入空间, 并在峰值点嵌入水印信息, 提取恢复时根据峰值点与相临的 bin 便可提取水印信息并恢复图像. 直方图平移嵌水印过程如图 1.

表 1　图像阶数 N 与置换周期 T 的关系

N	T	N	T
2	3	50	450
3	4	64	48
4	3	100	150
8	6	120	60
10	30	128	96
16	12	256	192
25	50	480	240
32	24	512	384

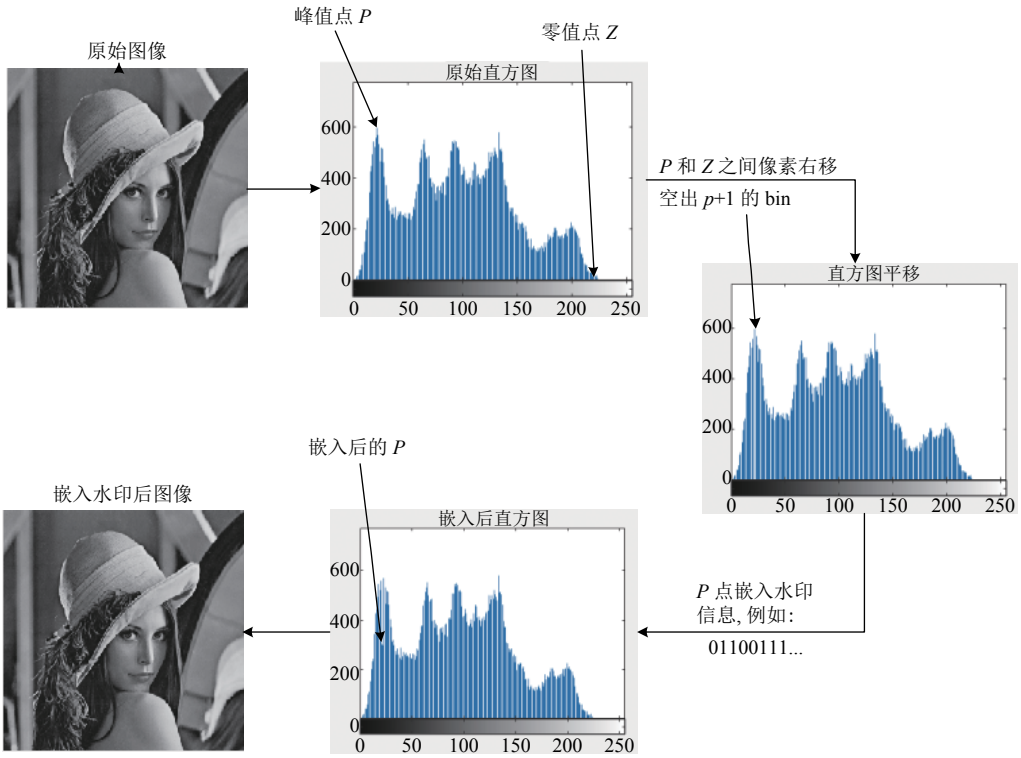


图 1　直方图平移嵌水印流程图

2.3 交换加密水印算法

在发送方, 加密与嵌入水印顺序可以交换; 在接收方, 可从含水印的密文图像中直接提取水印, 也可从解密后恢复图像的中提取水印, 从而达到交换加密水印的目的. 交换加密水印算法框架如图 2. 其中 I 为原始载体图像, w 为水印, k 为密钥, I_w为含水印图像, I'_w为含水印密文图像.

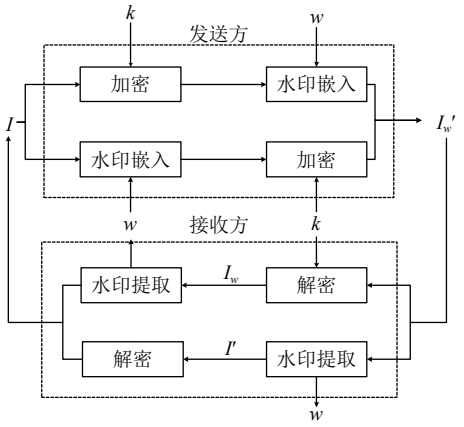


图 2 交换加密水印算法框架

3 基于 Arnold 置换的交换加密水印算法

本文提出的基于 Arnold 置换的交换加密水印算法如图 3.

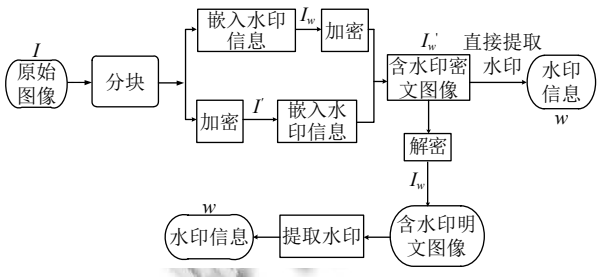


图 3 基于 Arnold 置换的交换加密水印算法

算法步骤可总结如下:

(1) 对原始图像进行分块;

(2) 在嵌入水印时, 在明文和密文中均可以嵌入, 最终得到含水印密文图像;

(3) 提取水印时, 可从含水印密文图像中直接提取, 也可解密后再提取.

3.1 含水印密文图像的生成

算法中涉及的参数有 a、b、n_1、n_2、T_1、T_2. 其中 a、b 为置换矩阵参数, $ab \neq 0$, $(n_1 \mod T_1) \neq 0$, $(n_2 \mod T_2) \neq 0$. n_1为水印图像置换次数与原始图像各小块的块间置换次数, n_2为原始图像各小块的块内置换次数. T_1为水印图像对应的置换周期, T_2为原始图像小块对应的置换周期.

3.1.1 先加密后嵌水印

其步骤可总结如下:

(1) 水印图像 m 置换n_1次, 得到水印 w;

(2) 把原始图像 I 分为 k 个的大小为 8×8 的明文分块, 记第 k 小块为 $I(k)$. 对 $I(k)$ 按照 2.1.1 小节分别进行块内置换n_2次、块间置换n_1次, 最终得到密文图像I';

(3) 按照从上到下、从左到右的方式遍历密文小块$I'(k)$的像素点;

(4) 将小块内$P+1$到$Z-1$的所有 bin 向右平移一位, 空出$P+1$的 bin. 可通过判断某个点的灰度值是否在 P–Z 之间, 然后对应灰度值加 1 即可;

(5) 每个密文小块嵌入 1 bit 信息, 嵌入到峰值点 P 中. 仅在第一个峰值点像素值 P 处嵌入信息. 嵌 0 就是加 0 运算, 嵌 1 就是加 1 运算, 这样像素值就会保持为 P 不变或者变为$P+1$.

嵌入公式如式 (4) 所示:

$$p' = \begin{cases} p+b, \text{ if } p = P \\ p+1, \text{ if } p \geq P \text{ and } p \leq Z-1 \\ p, \text{ otherwise} \end{cases} \tag{4}$$

其中, p 是原始像素值, b 是 1 bit 水印, p'是嵌入信息后的像素值;

(6) 将全部水印信息嵌入到密文图像I', 最终得到含水印的密文图像I'_w.

3.1.2 先嵌水印后加密

其步骤可总结如下:

(1) 水印图像 m 置换n_1次, 得到水印 w;

(2) 把原始图像 I 分为 k 个的大小为 8×8 的明文分块, 记第 k 个小块为 $I(k)$;

(3) 按照 3.1.1 小节中步骤 (3)–步骤 (5), 将水印 w 嵌入到原始图像 I 中, 每个小块嵌入 1 bit 信息, 最终得到含水印的图像I_w;

(4) 对I_w按照式 (3) 分别进行块内置换n_2次、块间置换n_1次, 最终得到含水印的密文图像I'_w.

3.2 水印提取与图像恢复

接收方接收到含水印的密文图像后进行相应处理, 可先提取水印信息、恢复图像; 也可解密以后再提取

水印信息、恢复图像. 在提取水印时, 因为每个小块只嵌入 1 bit 水印信息, 所以只需判断像素值为 P+1 的点的个数即可得知该小块嵌入的是 0 还是 1.

本文以先加密后嵌水印得到的含水印密文图像为例, 对提取水印恢复图像过程进行详细描述.

3.2.1 直接提取水印、恢复图像

其步骤可总结如下:

(1) 按照与嵌入时相同的方式遍历小块$I_w'(k)$的像素点.

(2) 判断小块$I_w'(k)$内像素值 P+1 的个数 num.

(3) 提取 1 bit 水印信息, 如式 (5) 所示:

$$w=\begin{cases}0, \text{ if } num=0\\ 1, \text{ otherwise}\end{cases} \tag{5}$$

(4) 其他小块重复步骤 (1)–步骤 (3), 完成全部水印信息的提取, 最终得到水印图像 w, 然后对 w 再置换 $T_1-(n_1 \mod T_1)$次得到水印图像 m.

(5) 提取水印后, 将$I'(k)$中像素值进行处理, 如式 (6) 所示:

$$p=\begin{cases}p', \text{ if } p'=P\\ p'-1, \text{ if } p'=P+1\\ p'-1, \text{ if } p'\geq P+2 \text{ and } p'\leq Z\\ p', \text{ otherwise}\end{cases} \tag{6}$$

(6) 其他小块重复步骤 (1)–步骤 (5), 最终获取完整的密文图像I'.

(7) 对$I'(k)$块间置换$T_1-(n_1 \mod T_1)$次, 块内置换$T_2-(n_2 \mod T_2)$次, 得到恢复图像.

3.2.2 先解密, 再提取水印恢复图像

其步骤可总结如下:

(1) 对含水印的密文图像I_w'分别进行块间置换$T_1-(n_1 \mod T_1)$次、块内置换$T_2-(n_2 \mod T_2)$次, 得到含水印的明文图像I_m.

(2) 对I_m各小块进行处理, 同 3.2.1 小节中步骤 (1)–步骤 (3). 最终得到水印 m.

(3) 按照式 (6) 对提取水印后的图像进行处理, 得到恢复图像.

4 算法仿真分析

本文算法在 Matlab R2020a, Windows 10 操作系统下进行仿真测试, 使用水印算法的客观评价标准, 选取大小为 512×512 的经典灰度图像进行测试, 从加密参数、不可见性、可逆性、效率说明算法的性能. 置换矩阵中参数选取为 a=1, b=1.

4.1 加密参数测试

嵌入率可以用来衡量算法的嵌入容量, 计算公式如式 (7) 所示:

$$\text{嵌入率}=\frac{\text{嵌入的bit数}}{\text{载体图像像素个数}} \tag{7}$$

选取三幅灰度图 Lena、Boat、Peppers, 在嵌入水印容量为 0.156 bpp 时, 对置换加密参数(n_1,n_2)进行测试. 选取 6 对不同参数对(n_1,n_2)时, 在密文域嵌水印, 解密后得到的含水印图像的 PSNR 值见表 2.

表 2 不同 (n_1, n_2) 时含水印图像 PSNR 值 (dB)

(n_1,n_2)	Lena	Boat	Peppers
(1,1)	52.52	51.92	52.21
(4,1)	52.52	51.92	52.21
(4,2)	52.52	51.92	52.21
(27,3)	52.52	51.92	52.21
(35,4)	52.52	51.92	52.21
(47,5)	52.52	51.92	52.21

由表 2 可知选取不同参数对(n_1,n_2)并不会影响解密后含水印图像的质量.

4.2 不可见性测试

峰值信噪比 PSNR 值可以说明含水印明文图像中水印的不可见性, PSNR 值越大, 说明水印的不可见性越好. 本文算法在不同嵌入容量下, 解密得到的含水印图像的 PSNR 值及平均 PSNR 值. 见表 3.

表 3 不同嵌入容量下 PSNR 值及平均值 (dB)

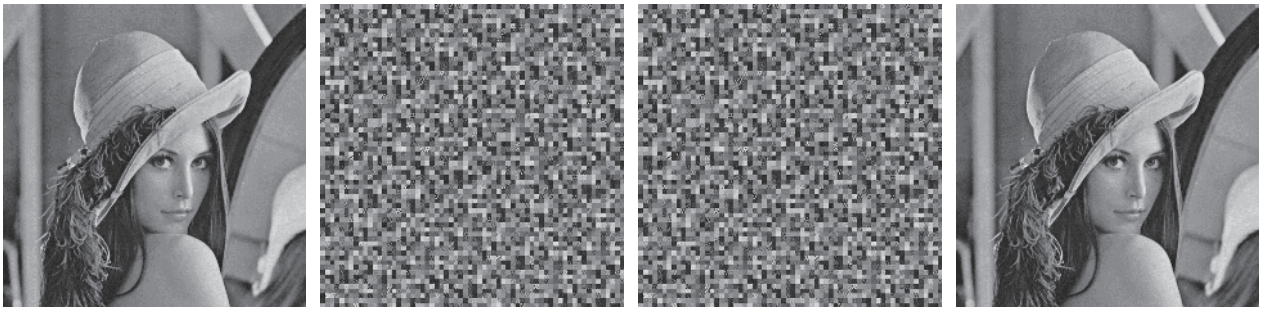
原始图像	0.0039 bpp	0.0156 bpp	0.0625 bpp	0.25 bpp
Lena	51.58	52.22	52.81	53.67
Airfield	51.09	51.72	52.57	54.02
Barbara	51.81	52.25	52.83	53.89
Baboon	51.80	52.30	53.08	54.56
Boat	51.60	51.92	52.76	54.00
Camera	52.21	52.51	53.17	53.55
Couple	51.26	51.70	52.58	53.81
Peppers	52.01	52.21	52.79	53.76
Plane	51.23	51.77	52.55	53.42
Truck	50.92	51.43	52.35	53.88
平均值	51.55	52.00	52.75	53.86

通过表 3 不难看出, 本文算法在水印嵌入后, PSNR 平均值都在 51 dB 以上, 且随着嵌入容量的增加, PSNR 值有所提升.

嵌入率为 0.0156 bpp, 载体图像为 Lena 图时在密文中嵌水印实验结果, 如图 4.

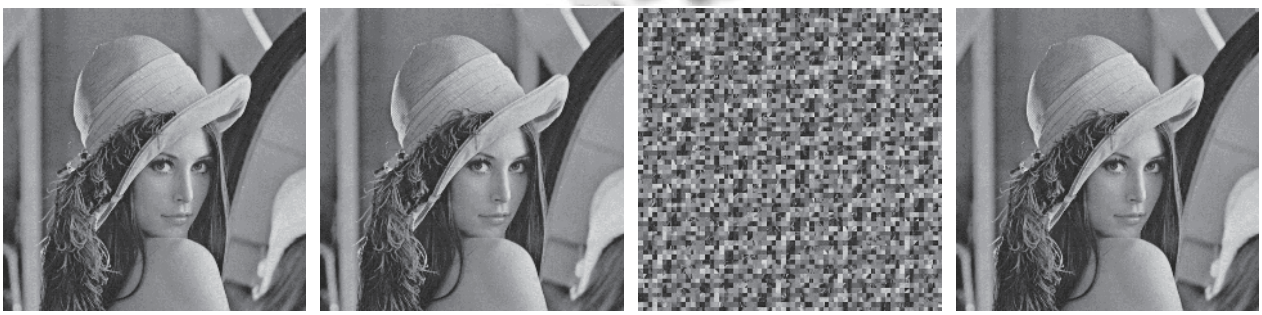
嵌入率为 0.0156 bpp, 载体图像为 Lena 图时在明文中嵌水印实验结果, 如图 5.

通过图 4 和图 5 可以看出在密文域或明文域中嵌水印, 解密后含水印图像质量较高, 水印不可见性好.



(a) 原始图像 (b) 密文图像 (c) 含水印密文图像 (d) 解密后含水印图像

图 4 密文域嵌水印实验结果



(a) 原始图像 (b) 含水印图像 (c) 含水印密文图像 (d) 解密后含水印图像

图 5 明文嵌水印实验结果

本文还与文献 [7–9] 中相关经典算法进行对比, 见表 4.

表 4 算法性能对比

图像	参数	文献[7]	文献[8]	文献[9]	本文算法
Lena	容量 (bpp)	0.11	0.0039	0.26	0.25
	PSNR (dB)	48.92	51.33	45.65	53.67
Baboon	容量 (bpp)	0.03	0.0039	0.23	0.25
	PSNR (dB)	48.70	50.08	40.08	54.56
Barbara	容量 (bpp)	0.075	0.0039	0.22	0.25
	PSNR (dB)	48.83	49.05	45.44	53.89
Plane	容量 (bpp)	0.15	0.0039	0.21	0.25
	PSNR (dB)	49.03	49.48	46.05	53.42
Truck	容量 (bpp)	0.069	0.0039	0.24	0.25
	PSNR (dB)	48.82	50.62	47.63	53.88

与文献 [7]、文献 [8] 算法对比, 可以看出本文算法在 PSNR 值与嵌入容量上占优; 与文献 [9] 对比, 在嵌入容量相近时, 本文算法 PSNR 值也要更高.

4.3 可逆性测试

通过归一化系数 NC 值来判断是否有可逆性. 本文给出了 10 幅 512×512 大小的灰度图像的 NC 值, 见表 5.

从表 5 中可以看出, 所有图像的 NC 值均为 1, 说明恢复图像与原始图像一样. 而且提取出的水印错误率为 0, 说明本算法具有可逆性.

表 5 可逆性测试

图像	NC值
Airfield	1
Barbara	1
Baboon	1
Boat	1
Camera	1
Couple	1
Lena	1
Peppers	1
Plane	1
Truck	1

4.4 算法效率测试

本实验还进行了算法效率测试, 在不同嵌入容量下, 对 10 幅灰度图分别进行 10 次测试, 最后取平均值, 结果见表 6.

表 6 不同嵌入容量下各算法的运行时间 (s)

效率测试	0.0039 bpp	0.0156 bpp	0.0625 bpp	0.25 bpp
加密&嵌水印	0.26	0.41	0.73	2.8
解密&提取水印	0.24	0.31	0.32	1.2

由表 6 可知, 随着数据量的增大, 算法所需时间有所增长, 但总体满足效率要求.

5 结束语

本文提出的基于 Arnold 置换的交换加密水印算法, 实现了加密操作与水印操作的交换, 解密后的含水印图像质量高, 水印的不可见性好. 算法中两次置换加密提高了载体图像在使用及分发时的安全性, 不仅能有效保护与恢复载体图像, 而且从含水印密文图像或解密后的含水印图像中都能提取水印信息, 对于身份认证与版权保护有着重要作用, 可以广泛地应用于医学、军事等领域.

参考文献

1 冯登国, 张敏, 张妍, 等. 云计算安全研究. 软件学报, 2011, 22(1): 71–83. [doi: 10.3724/SP.J.1001.2011.03958]

2 Jiang L, Xu ZQ, Xu YY. Commutative encryption and watermarking based on orthogonal decomposition. Multimedia Tools and Applications, 2014, 70(3): 1617–1635. [doi: 10.1007/s11042-012-1181-2]

3 方毅. Arnold 置乱变换图像加密算法研究 [硕士学位论文]. 赣州: 江西理工大学, 2018.

4 Tian J. Reversible data embedding using a difference expansion. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(8): 890–896. [doi: 10.1109/TCSVT.2003.815962]

5 Celik MU, Sharma G, Tekalp AM. Lossless watermarking for image authentication: A new framework and an implementation. IEEE Transactions on Image Processing, 2006, 15(4): 1042–1049. [doi: 10.1109/TIP.2005.863053]

6 贾玉洁. 基于图像像素直方图平移的可逆信息隐藏优化算法研究 [硕士学位论文]. 合肥: 安徽大学, 2020.

7 Luo H, Yu FX, Chen C, *et al*. Reversible data hiding based on block median preservation. Information Sciences, 2011, 181(2): 308–328. [doi: 10.1016/j.ins.2010.09.022]

8 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. 郑州大学学报 (理学版), 2018, 50(2): 29–34.

9 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.

10 Jiang L, Xu ZQ. Combination algorithm of active and passive security protection for image based on arnold transform. Proceedings of 2010 International Conference on Multimedia Information Networking and Security. Nanjing: IEEE, 2010. 625–629.

11 Roy S, Pal AK. A robust reversible image watermarking scheme in DCT domain using Arnold scrambling and histogram modification. International Journal of Information and Computer Security, 2018, 10(2–3): 216–236.

12 Katzenbeisser S. First Summary Report on Hybrid Systems. European Project IST-2002-507932, ECRYPT-Network of Excellence in Cryptology, 2005.

13 佟德宇. 矢量地理数据交换密码水印模型和算法研究 [博士学位论文]. 南京: 南京师范大学, 2018.

14 柯彦, 张敏情, 刘佳, 等. 密文域可逆信息隐藏综述. 计算机应用, 2016, 36(11): 3067–3076, 3092. [doi: 10.11772/j.issn.1001-9081.2016.11.3067]

15 Steinebach M, Zmudzinski S, Bolke T. Audio watermarking and partial encryption. Proceedings of SPIE 5681, Security, Steganography, and Watermarking of Multimedia Contents VII. San Jose: SPIE, 2005.

16 中山大学. 一种结合加密和水印的多媒体信息安全保障方法: 中国, 200912192270.6. 2010-02-10.

17 杨洋. 基于 Arnold 变换的数字图像加密算法 [硕士学位论文]. 广州: 华南理工大学, 2015.

18 郭琳琴, 张新荣, 李震. 基于 Arnold 逆变换的图像置乱恢复算法. 计算机应用与软件, 2010, 27(9): 265–267. [doi: 10.3969/j.issn.1000-386X.2010.09.083]

19 Ni ZC, Shi YQ, Ansari N, *et al*. Reversible data hiding. IEEE Transactions on Circuits and Systems for Video Technology, 2006, 16(3): 354–362. [doi: 10.1109/TCSVT.2006.869964]