自适应的密文彩色图像可逆数据隐藏算法

张秋余 冯玉春
(兰州理工大学计算机与通信学院 甘肃 兰州 730050)

摘 要 为了提高直方图平移算法嵌入率和图像感知质量,提出一种自适应的密文彩色图像可逆数据隐藏算法。利用 Logistics 混沌置乱加密算法对彩色图像进行加密;对加密后的图像块根据设定的波动阈值自适应地分成平滑块和陡峭块;对平滑块进行高平面位比特替换,对陡峭块进行直方图平移和多比特位嵌入来提升嵌入率和图像质量。实验结果表明,该算法具有较高嵌入容量且感知质量较好,当嵌入率为 1.142 bpp 时,峰值信噪比可达 35 dB 以上,并且抵抗噪声、剪切攻击时鲁棒性较好。

关键词 可逆数据隐藏 密文域彩色图像 Logistics 混沌置乱加密 直方图平移

中图分类号 TP391.1 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2020.02.049

ADAPTIVE REVERSIBLE DATA HIDING ALGORITHM OF CIPHERTEXT COLOR IMAGE

Zhang Qiuyu Feng Yuchun
(*School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, Gansu, China*)

Abstract In order to improve the embedding rate and image perceptual quality of histogram shifting algorithm, this paper proposes an adaptive reversible data hiding algorithm of ciphertext color image. It used Logistics chaotic scrambling encryption algorithm for color image. The encrypted image blocks were adaptively divided into smooth blocks and steep blocks according to the set fluctuation threshold. Then, the smooth block was replaced by high plane bits, and histogram shifting was performed on the steep block to embed several bits to improve the embedding rate and image quality. The experimental results show that the proposed algorithm has higher embedding capacity and a good perceptual quality. When embedding capacity is 1.142 bpp, the peak signal-to-noise ratio can reach more than 35 dB, and it has a good robustness against noise and shear attacks.

Keywords Reversible data hiding Encrypted color image Logistics chaotic scrambling encryption Histogram shifting

0 引 言

为了更好地实现隐秘通信以及提高保护传输图像数据的安全性,通常需要对图像进行加密,然后进行数据隐藏。因此,基于加密域图像的可逆数据隐藏技术成为了近年来的研究热点,被广泛应用于军事、医学和法律等应用领域[1]。

现有加密图像可逆数据隐藏算法主要分为:LSB 算法[2-4],通过翻转最低有效位进行秘密数据的嵌入;差值扩展算法[4-5],计算相邻像素间的差值,并扩展差值后嵌入秘密信息;直方图转换算法[6-10],首先找到的峰值点和零值点像素对,然后通过平移进行秘密数据嵌入等。2011 年,Zhang[2] 提出了密文域可逆数据隐藏算法,在流密码加密的图像中反转 3 个 LSB 嵌入秘密数据,该方法利用原始图像的平滑度进行数据提取。为提高数据的嵌入量,王子驰等[3] 提出了一种多比特嵌入的可逆信息隐藏算法,对分块后的图像根据嵌入密钥在每块中生成多个集合,通过修改集合中的数进行多比特位嵌入,从而很大程度上提高了容量。鄢舒等[4] 采用异或-置乱的加密方法,来提高算法的安全性,秘密信息的嵌入式同过比特替换来执行,但是嵌

收稿日期:2019-03-05。张秋余,研究员,主研领域:网络与信息安全,信息隐藏和隐写分析,图像理解与识别,多媒体通信技术。冯玉春,硕士生。

入容量相对较低。后来,Jung 等[5]提出了一种大容量的可逆数据隐藏算法,将图像分成不重叠的 3×1 的子块,进行升值排序计算最大和最小差值,然后将数据(两位数)嵌入在差值中形成新的像素,具有较高的嵌入容量和图像质量。Shiu 等[6]在图像加密之前预先计算相邻像素对的差值,然后对差值进行加密再进行秘密数据的嵌入,嵌入容量相对较低。在此基础上,Wu 等[7]提出了一种预测差值的差值直方图转换的可逆数据隐藏算法,将信息嵌入到两次预测差值直方图中,该算法具有较高的嵌入容量和较低的失真率。为进一步提高嵌入的容量,钱华山等[8]利用双层嵌入的方法,将原始图像划分为不同的类型,即水平分块和垂直分块,并找到不同类型的最大绝对差,由于像素的 LSB 位对图像质量的影响很小,因此信息嵌在第一个像素和第三个像素的 LSB 中,通过求绝对差和多层嵌入来提高嵌入容量。为增大嵌入容量,基于多维直方图转换[9-10]的方法被提出。Li 等[9]提出一种基于二维差值直方图转换的方法,Xue 等[10]提出一种自适应调整的差值对映射,相比文献[9]更好地利用了图像的冗余性,嵌入容量较高,图像失真度较低。Yin 等[11]提出了一种基于多层加密和块直方图转换的可逆数据隐藏技术,用约瑟夫遍历和流密码相结合的加密方法,改善了原始图像的安全性,但是嵌入容量较低。文献[12]和文献[13]采用公钥对图像进行加密,但嵌入容量非常低,并且在直接解密的情况下图像失真也很严重。为解决这一问题,Nyuyen 等[14]在图像加密前先预留空间然后进行秘密数据嵌入,然而,该方法未利用相邻性素间的相关性,并且定位图在一定程度上影响嵌入容量。由以上文献分析可知,现有方法存在着嵌入容量相对较低,或者在嵌入较大容量时图像的感知质量相对降低等问题在实际应用中,彩色图像比灰度图像和二值图像的应用更普遍。因此,研究密文彩色图像可逆数据隐藏技术具有重要的理论意义和实用价值。

针对以上问题,本文结合混沌加密和块直方图转换算法,提出了一种自适应的密文彩色图像可逆数据隐藏算法。该方法首先用 Logistics 混沌置乱算法对原始图像进行加密,再根据设定的波动阈值将加密后的图像块自适应地分成平滑块和陡峭块,选择陡峭块进行直方图平移嵌入,平滑块进行比特位替换嵌入。实验表明,该算法在具有较大嵌入容量的同时感知质量也较好,并且进行噪声和剪切攻击时鲁棒性较好,接收端也能够提取秘密信息并无失真地恢复出原始图像。

1 相关理论

1.1 混沌置乱加密

混沌系统[15]加密的序列是由系统迭代产生,混沌系统具有随机性以及敏感性等。从混沌系统的方程中通常很难推断出其初始值。其数学公式定义如下:

$$x_{i+1}=\mu x_i-\mu x_i^2 \tag{1}$$

式中:控制参数 $\mu\in(0,4]$,$x_i\in[0,1]$,$i\in\mathbf{Z}$,并且该映射所产生的序列由 μ 和 x 的初始值 x_0 控制。图像置乱[16]的实质是破坏相邻像素间的相关性,通过位置空间的变换来置乱像素,这样只是打乱了像素的位置,然而像素的大小并没有发生变化,因此加密后图像的直方图也不会变。如果将置乱算法看作是映射关系,那么原始图像和加密后图像就是一一对应的。假设原始图像为 Y_0,并且映射关系用字母 σ 表示,并得到置乱后的图像 Y_1,则图像之间的映射关系可以表示为:

$$Y_0\xrightarrow{\sigma}Y_1 \tag{2}$$

1.2 波动阈值

对直方图峰值点较高、图像陡峭的块,不仅可以改动较少的像素点而且还能嵌入更多的秘密数据;对于峰值点低、图像平滑的块,不仅需要改动更多的像素点而且嵌入的容量也小。因此,对波动阈值[17]进行改进,根据改进后的波动阈值 T_f 将图像分成陡峭块和平滑块,选择不同的块进行不同方法的秘密数据嵌入。阈值的计算公式如下:

$$T_f=\left[g_{\max}-\frac{1}{l-1}\sum_{i=1}^{l-1}g_i\right]^2 \tag{3}$$

式中:l 表示块的长度,$g_{\max}$ 表示峰值点的个数,g_i 表示峰值点相邻像素的像素数,通过对峰值点数和相邻像素点数的平均值做差取平方,近而放大差距程度,更加直观地反映出直方图的波动情况。当波动阈值 T_f 越小时,直方图越平滑,嵌入的秘密信息就越少;当波动阈值 T_f 越大时,直方图越陡峭,嵌入的秘密数据容量就越大。

1.3 块直方图平移

基于块直方图平移[18]的可逆数据隐藏算法主要通过峰值和零值点对的平移来嵌入秘密数据,假设每个图像块 Q 中的像素为 $q_{i,j}$,对每个图像块进行扫描,找出块直方图中的两个峰值点 $q_{i,l}$、$q_{i,r}$,根据下式,判断出最大峰值点 $g_{i,r}$和次大峰值点 $g_{i,l}$:

$$\begin{aligned}g_{i,l}&=\min(q_{i,l},q_{i,r})\\g_{i,r}&=\max(q_{i,l},q_{i,r})\end{aligned} \tag{4}$$

式中: $q_{i,l}$和 $q_{i,r}$分别代表两个峰值点像素，用 $g_{i,r}$代表最大峰值点像素，$g_{i,l}$代表最小峰值点像素。

对小于峰值点 $g_{i,l}$的像素和大于峰值点 $g_{i,r}$的像素分别进行向左和向右平移，否则像素值保持不变。

$$q'_{i,j}=\begin{cases}q_{i,j} & g_{i,l}<q_{i,j}<g_{i,r}\\ q_{i,j}-3 & q_{i,j}<g_{i,l}\\ q_{i,j}+3 & q_{i,j}>g_{i,r}\end{cases} \tag{5}$$

式中: $q_{i,j}$代表每个图像块中的像素，$q'_{i,j}$代表像素平移之后的像素值。

将嵌入的秘密数据 $x(x=0,1,2,3)$ 通过对峰值点像素的平移进而实现秘密信息的嵌入，具体嵌入过程如下式所示:

$$q'_{i,j}=\begin{cases}q_{i.j}-x & q_{i,j}=g_{i,l}\\ q_{i,j}+x & q_{i,j}=g_{i,r}\end{cases} \tag{6}$$

算法原理如图 1 所示。

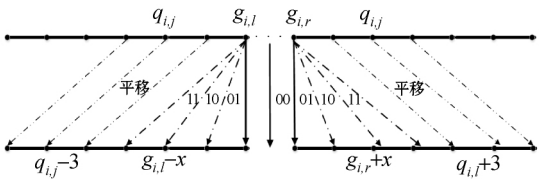


图 1　直方图平移原理

按照上述方法处理完成图像块的直方图平移嵌入。

1.4　位置定位图

在直方图平移前，采用直方图收缩的方法来防止像素值的上溢和下溢，也就是对图像要先进行预处理，通过对饱和像素进行平移并做标记，来防止嵌入过程中像素的上下溢出[11]。本文首先对每个图像块 Q 中的像素 q 进行扫描，对于 l 比特的灰度图像，它的像素取值范围应是 $0\sim2^l-1$。当像素值 $q_{i,j}\in\{3,2^l-1-3\}$ 时，像素值的大小不变; 当像素值 $q_{i,j}\in\{0,2^l-1\}$ 时，如果像素是饱和像素，对其改变的值在位置映射图 H 中标记为 0，对未改变的像素值标记为 1，否则不标记。

$$q_{i,j}=\begin{cases}2^l-1-3 & 2^l-1-3<q_{i,j}<2^l-1\\ q_{i,j}-3 & q_{i,j}<3\\ q_{i,j} & \text{其他}\end{cases} \tag{7}$$

2　算法设计

首先，将原始彩色图像分成 R、G、B 三个色彩分量，并在分离的基础上分别对三个分量进行混沌置乱加密; 然后对加密后的图像块根据块直方图的波动情况，自适应地将图像分成陡峭块和平滑块，分别对平滑块和陡峭块进行秘密数据的嵌入; 最后通过算法的逆运算提取出秘密数据，并且得到解密图像，同时恢复出原始彩色图像，即载体图像。本文提出的自适应的密文彩色图像可逆数据隐藏算法的原理框图如图 2 所示。

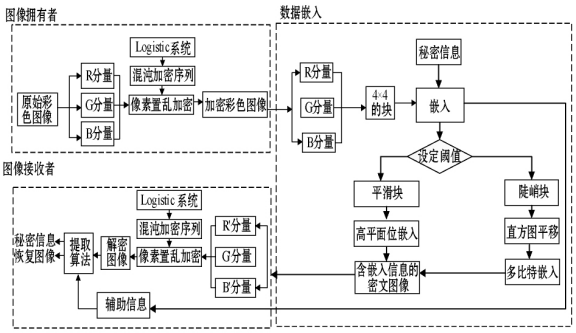


图 2　自适应的密文彩色图像可逆数据隐藏算法

2.1　图像加密

首先我们采用 Logistics 混沌置乱加密算法对 $N\times N$ 的原始彩色图像 C 进行加密，具体加密步骤如下:

步骤 1　将明文图像 C 分成 R、G、B 三个色彩分量，并将 $N\times N$ 的数字图像转化为 $N\times N$ 的参数矩阵。即: 红色分量: $R=C(:,:,1)$，绿色分量: $G=C(:,:,2)$，蓝色分量: $B=C(:,:,3)$。

步骤 2　用加密密钥 μ 和 m_0 作为初始值，通过 Logistics 混沌映射生成 $N\times N$ 的混沌序列 $\boldsymbol{A}$。然后将序列 $\boldsymbol{A}$ 中的每个元素扩大 $N\times N$ 倍以获得新的整数序列 $\boldsymbol{W}$。

步骤 3　用整数序列 W 产生随机坐标，将 W 中每个像素对 N 取整，随机产生行坐标 x，对 N 取余，随机产生列坐标 y，然后将 $R(i,j)$ 像素值赋给 $R'(x,y)$，最后得到新的加密后的图像 R'。

步骤 4　然后对 G'、B'分别按照步骤 2 和步骤 3 进行像素位置的置乱，最后将 R'、G'、B'合并得到最终加密的彩色图像 C'。

2.2　数据嵌入

在获得加密图像 C'后，对加密图像 C'嵌入秘密数据。具体嵌入步骤如下:

步骤 1　将加密图像 C'分成 R'、G'、B'三个通道。基本原则是在通道分离过程中，将剩余的两个置零，然后依次进行处理。

步骤 2　首先对红色通道 R'进行分块，分成互不重叠的图像块，假设每块图像的大小为 $u\times u$，本文每块图像的大小为 4×4，即 $u=4$。

步骤 3　根据式(3)计算图像中每块的波动值，然后将其和设定的阈值 T_f 进行比较，当计算的波动值小于阈值 T_f 时，图像被分为平滑块; 当计算的波动值大

于阈值 T_f 时，图像被分为陡峭块，然后对不同的块自适应地采取不同的嵌入方法。

步骤 4 对平滑块，先将块中的像素转化成八个平面位，再从最高平面位找非零的比特位平面，然后该平面位与设定的阈值 $t=4$ 进行差运算，即得到嵌入比特位数，进而自适应地逐个进行秘密数据的比特位替换，然后将嵌入后的数值转化成十进制的数。

步骤 5 对陡峭块，首先进行像素值上下溢出的预处理，对可能溢出的像素按照式(7)进行平移并做标记，得到定位图 H。

步骤 6 在直方图中找到最大峰值点 $g_{i,r}$ 和第二峰值点 $g_{i,l}$，以第二峰值点在最大峰值点左边为例，然后找出两对零值点。

步骤 7 根据直方图的分布，将小于 $g_{i,l}$ 的像素值像左平移三位，将大于 $g_{i,r}$ 的像素值向右平移三位，其他像素值保持不变。

步骤 8 按顺序扫描载体图像，当扫描到的像素值是 $g_{i,r}$ 时，如果嵌入的秘密数据是 00，则像素值不变；秘密数据是 01，则像素值加 1；秘密数据是 10，则像素值加 2；秘密数据是 11，则像素值加 3。当扫描到的像素值是 $g_{i,l}$ 时，如果嵌入的秘密数据是 00，则像素值不变；秘密数据是 01，则像素值减 1；秘密数据是 10，则像素值减 2；秘密数据是 11，则像素值减 3。如果最大峰值点在第二峰值点左边时，只需调整平移方向即可，将嵌入秘密数据的位置标记为 1，生成定位图 map，再将定位图 H 和 map 进行异或加密，然后嵌入到载体中。

步骤 9 按上述方法分别对 G'、B' 进行秘密数据的嵌入，得到嵌入有效数据的单通道密文图像，然后合并三个色彩通道，得到隐秘载体图像 S。

2.3 图像的解密

当接收端对接收到的图像先进行解密，解密过程是加密的逆过程，具体过程如下：

步骤 1 将提取秘密信息后的图像 S 分成三个色彩分量，然后再将每个分量转化成参数矩阵。

步骤 2 接收端根据解密密钥，利用 Logistics 混沌映射原理产生混沌序列 A'。

步骤 3 将得到的新混沌序列 A' 中的每个元素乘以 $N\times N$ 得到新的整数序列 W'。

步骤 4 由整数序列 W' 随机生成横坐标 x 和纵坐标 y，然后将像素值赋给 $R''(x,y)$，最后得到解密后的图像 R''。

步骤 5 然后对 G''、B'' 分别按照步骤 3 和步骤 4 进行像素位置的还原，最后将 R''、G''、B'' 合并得到，得到图像 S''。

2.4 数据提取

步骤 1 按照与数据嵌入方法相同的方式，将含有秘密数据的解密图像分成三个色彩分量，然后再对每个分量进行分块。

步骤 2 根据辅助信息和嵌入算法的逆过程，先将平滑块中的像素转化成八个平面位，然后找非零的比特位平面，再根据设定的阈值计算出嵌入的比特位数，进而自适应地逐个提取出秘密数据。

步骤 3 将陡峭块按嵌入数据的顺序对图像进行扫描，仍以最大峰值点在第二峰值点右边为例，当发现像素值是 $g_{i,l}$ 时，提取出的数据为 00；当发现像素值是 $g_{i,l}-1$ 时，提取的数据为 01；当发现像素值是 $g_{i,l}-2$ 时，提取的数据为 10；当发现像素值是 $g_{i,l}-3$ 时，提取的数据为 11；当发现像素值是 $g_{i,r}$ 时，提取的数据为 00；当发现像素值是 $g_{i,r}+1$ 时，提取的数据为 01；当发现像素值是 $g_{i,r}+2$ 时，提取的数据为 10；当发现像素值是 $g_{i,r}+3$ 时，提取的数据为 11。如果最大峰值点在第二峰值点左边，只需调整平移方向即可。扫描完成后，秘密数据提取完毕。

步骤 4 恢复原始载体图像，按嵌入数据的顺序扫描，像素点为 $g_{i,l}-1$、$g_{i,l}-2$、$g_{i,l}-3$ 的像素值都变为 $g_{i,l}$，像素点为 $g_{i,r}+1$、$g_{i,r}+2$、$g_{i,r}+3$ 的像素值都变为 $g_{i,r}$，将大于 $g_{i,r}$ 的像素值都减 3，将小于 $g_{i,l}$ 的像素值都加 3，扫描完成后合并三个通道，得到恢复后的载体图像。

3 实验结果及分析

本文采用的实验硬件平台为：AMD phenom II X4 CPU，8GB，3.01 GHz，实验环境是 Windows 7 操作系统下的 MATLAB R2013a。从 USC-SIPI 标准彩色图像库中选择具有不同纹理特征的 4 幅 24 位彩色图像(512×512) Lena、Airplane、Baboon、Peppers 图像作为测试载体图像，如图 3 所示。秘密数据选择随机的二进制数。

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

图 3 实验采用的载体图像

3.1 图像质量评价指标

该实验通过峰值信噪比(PSNR)和嵌入率来评估恢复质量和嵌入容量，分析算法性能。

1) 峰值信噪比。PSNR 定量地评价了明文图像和

嵌入秘密数据后图像的相似度，PSNR 值越大图像保真度越好，其计算公式如下:

$$PSNR = 10\lg\left[\frac{255^2}{MSE}\right] \tag{8}$$

式中: MSE 是明文图像 C 和隐密载体 S 之间的均方误差，其被定义为:

$$MSE = \frac{1}{M \times N} \times \sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j) - S(i,j))^2 \tag{9}$$

2) 嵌入容量。嵌入容量用来评价嵌入数据的多少，使用嵌入率(ER) 代表嵌入容量，其定义为:

$$ER = \frac{capacity}{M \times N} \times 100\% \tag{10}$$

式中: $capacity$ 为嵌入的总数据位的个数，M、N 是图像长和宽。

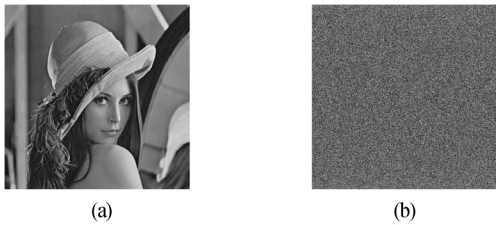
3) 结构相似度(SSIM) 。结构相似度[19] 将亮度和对比度从图像的结构信息中分离，并结合结构信息对图像质量进行评价。该方法是目前最常用的评价图像质量的方法，通常与 PSNR 结合起来全面地评价图像质量。其定义为:

$$SSIM(x,y) = l(x,y)\,C(x,y)\,S(x,y) \tag{11}$$

式中: $l(x,y)$、$C(x,y)$、$S(x,y)$ 分别为 x 与 y 的亮度函数、对比度函数和结构函数。

3.2　加密性能分析

首先，选择 512 × 512 的 Lena 测试图像进行实验，原始图像如图 4(a) 所示，经过加密后得到图像 4(b) ，可以看出，加密后的图像变得杂乱无章，并且在视觉上是不可见的。再将加密后的图像分成 4 × 4 的不重叠块，同时随机的生成 2 413 比特，即将嵌入率为 0.009 2 bpp 的秘密数据嵌入到加密图像中，如图(c) 所示。图 4(d) 是根据解密密钥将含秘密信息的图像解密后得到的图像，峰值信噪比为 56.41 dB，可以看出，解密后含有秘密数据的图像已经几乎接近明文图像。图 4(e) 是提取秘密数据后恢复的载体图像，为了更进一步说明加密算法的恢复效果，将恢复出来的图像与原图像做差运算，得到的差值如图 4(f) 所示，可以看出: 差值接近于 0，即恢复出的图像几乎接近于明文图像，因此该算法实现了加密域数据的可逆嵌入和提取以及图像的恢复。



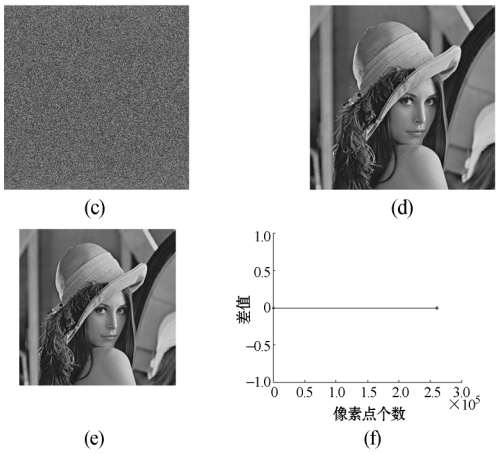


图 4　加密图像的嵌入和提取以及图像的恢复

3.3　图像感知质量与嵌入率性能分析

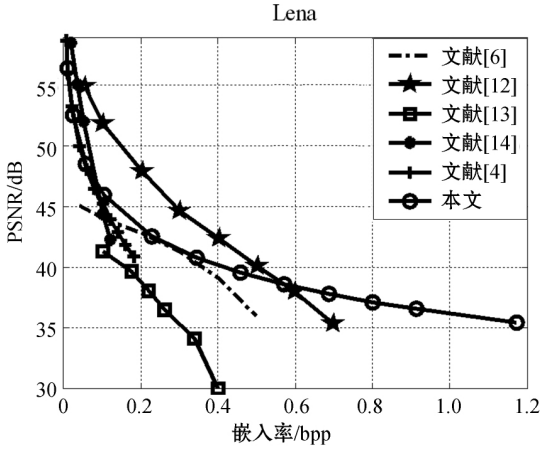
表 1 为本文方法在不同嵌入容量时分别选择 Lena、Baboon、Airplane、Peppers 图像作为测试载体图像的 PSNR 值和 SSIM 值。

表 1　不同嵌入容量下的 PSNR 和 SSIM 值

嵌入率/bpp	Lena		Peppers		Baboon		Airplane	
	PSNR/dB	SSIM	PSNR/dB	SSIM	PSNR/dB	SSIM	PSNR/dB	SSIM
0.009	56.41	0.992	55.87	0.991	54.10	0.992	56.03	0.990
0.050	48.53	0.990	48.08	0.989	46.10	0.990	44.18	0.973
0.103	45.96	0.984	45.57	0.948	43.48	0.987	41.53	0.964
0.343	40.77	0.967	40.53	0.923	38.27	0.963	39.69	0.947
0.687	37.76	0.921	37.69	0.907	35.22	0.947	36.58	0.921
0.921	36.50	0.890	36.49	0.893	33.47	0.901	35.33	0.890

由表 1 可知，随着嵌入率的逐渐增大，峰值信噪比和结构相似度也随之逐渐减小。当嵌入率达到 0.687 bpp时，4 幅图像的峰值信噪比都在 35 dB 以上，这表明加密后的含秘图像的不可感知性较好。

为了更进一步说明本文方法的图像质量、嵌入容量和结构相似度等性能，通过与文献 [14]、文献 [6]、文献 [12]、文献 [13] 和文献 [14] 的算法进行比较，结果如图 5 所示。



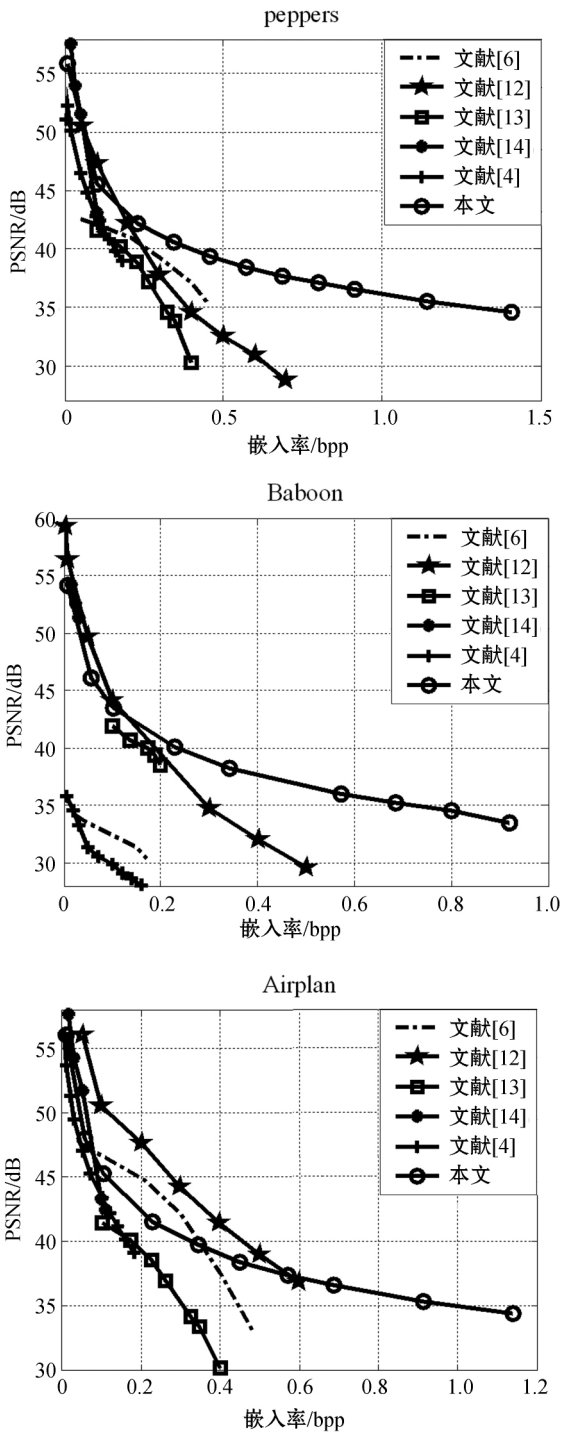
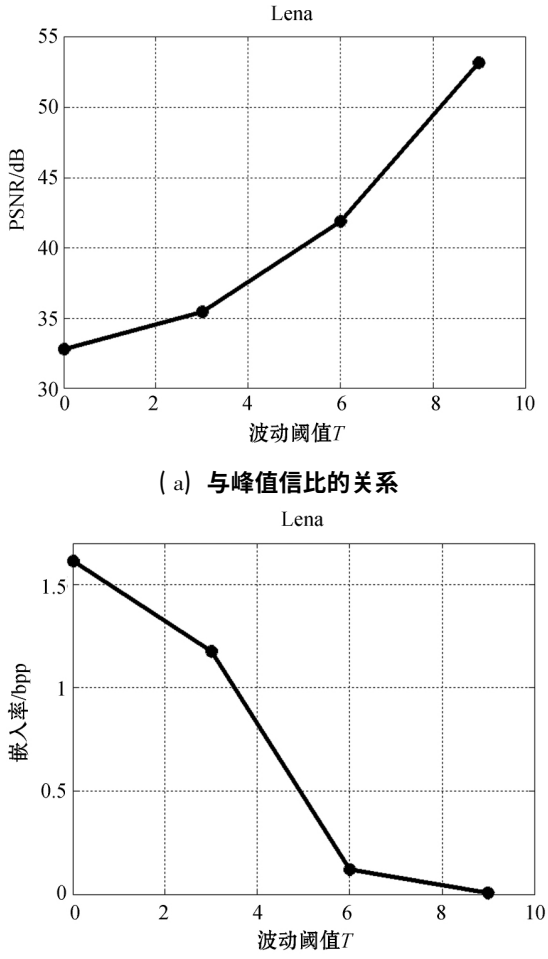


图 5 不同算法的性能比较

图 5 的 4 幅图分别为图像 Lena、、Peppers、Baboon、Airplane 利用本文算法和现有算法在不同嵌入数据的情况下峰值信噪比的对比图。可以看出，本文提出的方法有效提高了嵌入率，并且峰值信噪比均在 33 dB 以上，具有较好的图像质量。本文根据设定的阈值对图像块进行分类，对陡峭块采用直方图平移的多比特嵌入，对平滑块的高平面位像素进行替换嵌入。在嵌入容量相同的情况下，本文算法的图像恢复质量相比于文献 [6]、文献 [13] 和文献 [4] 方法有一定的提高；在峰值信噪比一定的情况下，本文算法比文献 [14] 和文献 [12] 方法更适合嵌入大容量秘密数据。这是因为本文算法在秘密数据嵌入的过程中，只对像素点集中的块，即陡峭块，进行直方图平移嵌入，因为平滑块像素点相对较分散，嵌入的秘密数据不仅少而且对图像质量影响也很大，因此，相比于文献 [6] 和文献 [4] 的方法，当嵌入容量相同时，本文算法具有较好的峰值信噪比；又因为本文算法在直方图嵌入中进行多比特嵌入，对平滑块也进行高平面位秘密数据嵌入，并且对定位图进行了缩减，减少了辅助信息的嵌入，因此，与文献 [14] 和文献 [12] 的方法相比，能嵌入更多的嵌入容量，更适用于大容量秘密数据的嵌入。

3.4 波动阈值与峰值信噪比和嵌入率关系分析

以 Lena 图像作为测试载体，取不同的波动阈值 T，分析随着波动阈值的变化峰值信噪比和最大嵌入率随之变化的情况，结果如图 6 所示。



(a) 与峰值信比的关系

(b) 与嵌入率的关系

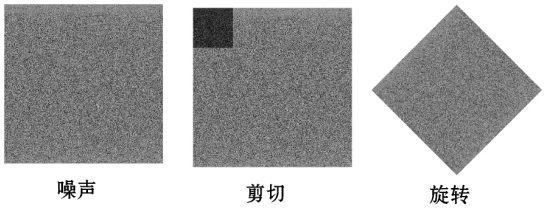
图 6 波动阈值与峰值信噪比和嵌入率之间的变化关系

从图 6 中可以看出，当波动阈值增大时，峰值信噪比随之增大，但嵌入率随之降低，也就是说，可以通过改变波动阈值的大小来调整嵌入率和峰值信噪比。因

而根据嵌入者的需求，可以灵活调整嵌入率和图像质量之间的关系。本算法为了使嵌入率和峰值信噪比相对达到平衡，在实验过程中取波动阈值 $T=3$。

3.5　鲁棒性分析

为了验证算法的鲁棒性，对嵌有秘密信息的图像进行噪声、剪切和旋转攻击，对抗攻击性能进行分析。以 Lena 图像为载体，图 7(a) 分别是受到均值 $M=0$，方差 $V=0.0001$ 的噪声攻击、1/16 的剪切攻击和逆时针旋转 45 度的攻击图片，图 7(b) 分别是恢复后的图片。



(a) 攻攻后的隐密载体

(b) 攻击恢复后的载体

图 7　攻击前后的图像载体

表 2 为图像 Airplane、Lena、Baboon、Peppers 四种不同彩色图像在相同嵌入率下受到噪声、剪切和旋转攻击之后的峰值信噪比变化情况。

表 2　相同嵌入容量下不同攻击的 PSNR 值

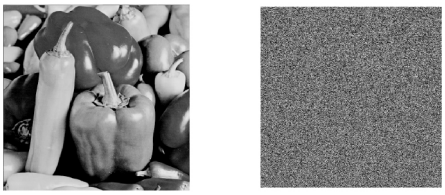
载体图像	嵌入率 /bpp	攻击后的 PSNR/dB		
		噪声	剪切	旋转
Airplane	0.929	32.413	31.600	27.439
Lena	0.929	34.017	33.478	28.901
Baboon	0.929	31.334	30.460	26.674
Peppers	0.929	34.755	33.992	28.118
平均	0.929	33.129	32.382	27.783

从表 2 中可看出，噪声和剪切攻击的平均 PSNR 值在 32 dB 以上，抗噪声和剪切功能相对较好，但是抗旋转攻击相对抗噪声和剪切攻击能力较弱。

3.6　安全性分析

3.6.1　加密算法的安全性分析

(1) 敏感度分析。为说明加密算法的安全性，分析了加密密钥的灵敏度。假设攻击者已经知道加密图像，我们对解密图像的安全性进行分析。文献 [16] 证明图像在加密和信息嵌入的过程中对密钥的变化特别灵敏，只要密钥稍微改变，就会改变混沌映射的初始状态，最后得到错误的解密图像，从而导致图像最终不能被恢复。如当加密密钥 0.700 被错误输成 0.699 时，接收端就会出现解密错误。如图 8 所示，(a) 、(b) 分别为正确密钥和错误密钥的解密效果示意图。因此，攻击者在已知加密图像的情况下，提供的加密算法相对是安全的。



(a) 正确密钥　　(b) 错误密钥

图 8　正确密钥和错误密钥的解密效果图

(2) 相关性分析。相关性[20] 用于表示图像中两个相邻像素点之间的密切程度，可以非常直观地反映出图像中的像素点被打乱的情况。如果相关性越低，那么表示像素点被打乱的越完全，反之则说明像素点的混乱程度还不够。通过相关系数来验证相关性，并且相邻像素的相关系数可以反映出图像像素的扩散程度。相关系数越接近于 0，说明图像的像素点间越不具备相关性，越接近于 1，则像素之间越具有相关性。相关系数的计算公式如下:

$$r_{xy}=\frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{12}$$

$$cov(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{13}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \quad E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{14}$$

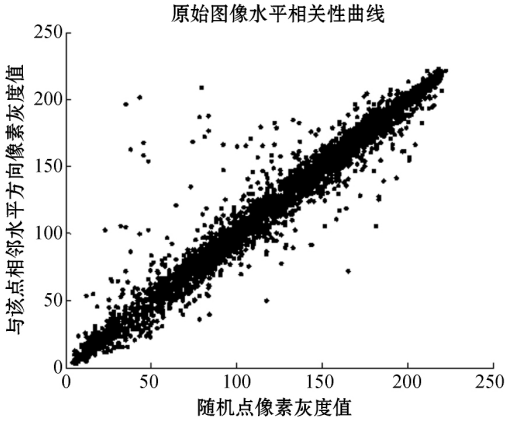
式中: x 和 y 分别是两个邻近像素点的灰度值，r_{xy} 表示相关系数。

从明文图像和加密图像中分别随机抽取 5 000 对相邻像素，并分别从水平方向、垂直方向和对角线方向测试相邻像素间的相关性。按照式(12) - 式(14) 计算每对的相关系数，结果列于表 3 中。

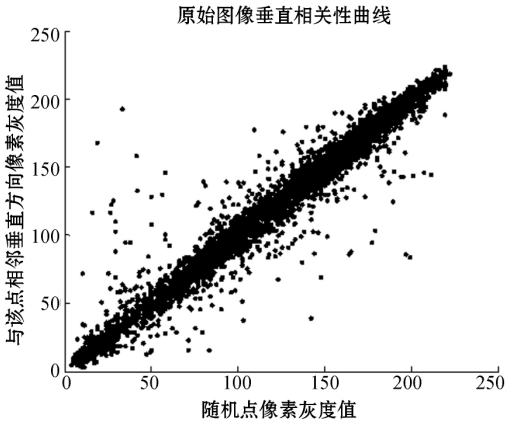
表 3　Peppers 图像相关性分析

方向	明文图像	加密图像
水平方向	0.979 4	-0.002 3
垂直方向	0.978 6	0.004 1
对角线方向	0.966 0	-0.013 0

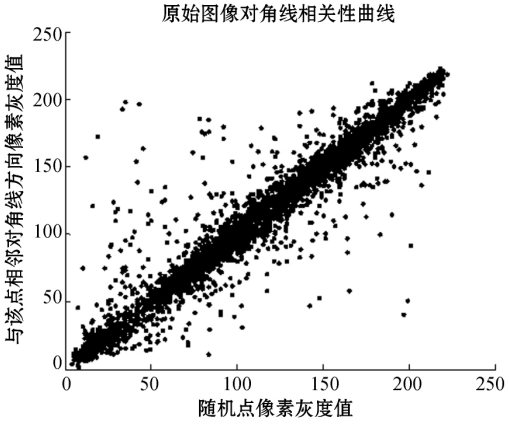
可以看出，明文图像的相关系数均超过了 0.9，说明明文图像相邻像素的相关性很强，而加密图像相邻像素的相关系数均小于 0.01，说明加密图像相邻像素的相关性很弱。为了更清楚地显示结果，以 Peppers 图像为例，图 9 给出了明文图像与加密图像的相关性分布图。



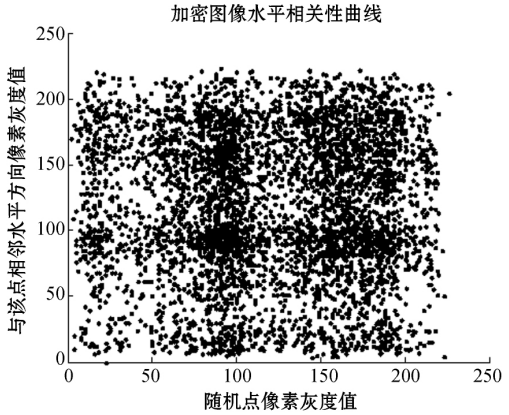
(a)



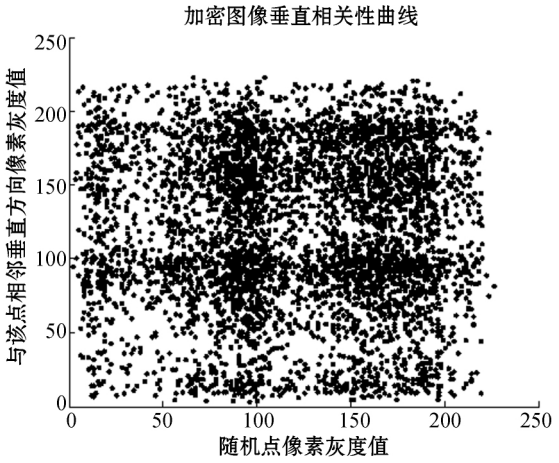
(b)



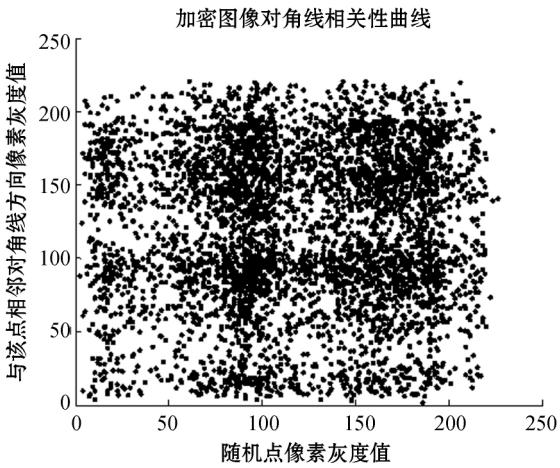
(c)



(d)



(e)



(f)

图 9 Peppers 图像水平、垂直和对角线相关性分布图

图 9(a) -(c) 是明文图像分别在水平、垂直和对角线方向上的相关性分布图，可以看出，像素点聚集在一条对角线附近，说明像素间的相关性很明显。图 9(d) -(f) 是加密图像的水平方向、垂直方向和对角线方向的相关性分布图，像素点零散的分布在整个平面上，表明加密图像各个方向上像素间的相关性很弱。

3.6.2 嵌入算法的安全性分析

假设攻击者已经知道图像的恢复和秘密数据的提取过程，我们分两种情况讨论: 不知道解密图像、知道解密图像。

首先，在提取秘密数据和恢复图像之前要获得解密图像，但是根据上述加密安全性分析可知，直接获得解密图像是不容易的。因此，攻击者在不知道解密图像的情况下，是很难提取出秘密数据并恢复出原始图像。

其次，如果攻击者已经知道解密图像，但是在数据提取和图像的恢复过程中是要知道辅助信息，比如位置图和秘密数据的比特位，然而在嵌入的过程中对辅

助信息已经进行了异或加密，假设辅助信息的长度为 n，那么攻击者获得辅助信息的概率为 $1/2^n$。因此，攻击者难以准确地提取秘密数据并恢复原始图像。

4 结　语

为解决现有算法嵌入容量低以及在嵌入容量较大时图像感知质量较低等问题，本文提出了一种自适应的密文彩色图像可逆数据隐藏算法，根据设定的阈值自适应地对陡峭块进行直方图多比特位嵌入来提高嵌入容量; 对平滑块进行平面位的替换进行秘密数据嵌入，进而提高图像的不可感知性。实验结果表明，当嵌入率为 1.142 bpp 时，峰值信噪比可达 35 dB 以上，且进行噪声、剪切攻击时鲁棒性较好，与现有方法相比在增大嵌入率的同时提高了图像感知质量，并且图像能得到很好的恢复。本文算法的不足之处在于抵抗外界的旋转攻击能力较差。

下一步的研究计划是将该方法应用到频域中，从而提高算法的鲁棒性。

参 考 文 献

[1] 刘宇，杨百龙，赵文强，等. 基于自适应块参照值的密文域可逆信息隐藏 [J]. 计算机科学，2018 (8): 29.

[2] Zhang X. Reversible data hiding in encrypted image [J]. IEEE signal processing letters，2011，18(4): 255 – 258.

[3] 王子驰，张媛，张新鹏. 多比特嵌入的加密图像中可逆信息隐藏方法 [J]. 小型微型计算机系统，2014，35(10): 2331 – 2335.

[4] 鄢舒，陈帆，和红杰. 异或-置乱框架下邻域预测加密域可逆信息隐藏 [J]. 计算机研究与发展，2018，55(6): 1211 – 1221.

[5] Jung K H. A high-capacity reversible: data hiding scheme based on sorting and prediction in digital images [J]. Multimedia Tools and Applications，2017，76(11): 13127 – 13137.

[6] Shiu C W，Chen Y C，Hong W. Encrypted image-based reversible data hiding with public key cryptography from difference expansion [J]. Signal Processing: Image Communication，2015，39: 226 – 233.

[7] Wu H Z，Wang H X，Shi Y Q. PPE-based reversible data hiding [C] //Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security. ACM，2016: 187 – 188.

[8] 钱华山，田丽华，李晨. 基于三像素块差值的多层可逆图像水印算法 [J]. 计算机应用与软件，2017，34(3): 252 – 259.

[9] Li X，Zhang W，Gui X，et al. A novel reversible data hiding scheme based on two-dimensional difference-histogram modification [J]. IEEE Transactions on Information Forensics and Security，2013，8(7): 1091 – 1100.

[10] Xue B，Li X，Wang J，et al. Improved reversible data hiding based on two-dimensional difference-histogram modification [J]. Multimedia Tools and Applications，2017，76(11): 13473 – 13491.

[11] Yin Z，Abel A，Tang J，et al. Reversible data hiding in encrypted images based on multi-level encryption and block histogram modification [J]. Multimedia Tools and Applications，2017，76(3): 3899 – 3920.

[12] Li M，Xiao D，Zhang Y，et al. Reversible data hiding in encrypted images using cross division and additive homomorphism [J]. Signal Processing: Image Communication，2015，39: 234 – 248.

[13] Zhang X，Long J，Wang Z，et al. Lossless and reversible data hiding in encrypted images with public-key cryptography [J]. IEEE Transactions on Circuits and Systems for Video Technology，2016，26(9): 1622 – 1631.

[14] Nguyen T S，Chang C C，Chang W C. High capacity reversible data hiding scheme for encrypted images [J]. Signal Processing: Image Communication，2016，44: 84 – 91.

[15] 徐兵，袁立. 基于改进 Logistic 混沌映射的数字图像加密算法研究 [J]. 计算机测量与控制，2014，22(7): 2157 – 2159.

[16] 黄璐. 基于三维混沌映射的彩色图像置乱加密 [J]. 数字技术与应用，2013(7): 172 – 173.

[17] Xuan G，Tong X，Teng J，et al. Optimal histogram-pair and prediction-error based image reversible data hiding [M] // Digital Forensics and Watermaking. Springer Berlin Heidelberg，2012: 368 – 383.

[18] Yin Z，Abel A，Zhang X，et al. Reversible data hiding in encrypted image based on block histogram shifting [C] // 2016 IEEE International Conference on Acoustics，Speech and Signal Processing (ICASSP). IEEE，2016: 2129 – 2133.

[19] Xiao D，Cai H，Wang Y，et al. High-capacity separable data hiding in encrypted image based on compressive sensing [J]. Multimedia Tools and Applications，2016，75(21): 13779 – 13789.

[20] 杨吉云，吴昊. 基于混沌系统和动态 DNA 编码与运算的彩色图像加密算法 [J]. 计算机工程，2018，44(2): 151 – 157.