

文章编号:1007-2780(2019)04-0410-07

融合 CFT 和 LSB 的高容量可逆数据隐藏

任克强*, 肖璐瑶

(江西理工大学 信息工程学院, 江西 赣州 341000)

摘要:针对可逆数据隐藏中图像质量和嵌入容量之间相互矛盾的问题,提出一种中心折叠技术与最低有效位替换相结合的可逆数据隐藏方法。该方法首先对原始图像中的像素进行位平面划分,以得到 2 个位平面;然后利用中心折叠技术将秘密数据折叠,并将折叠后的秘密数据嵌入到原始像素的最高有效位中,以生成 2 个隐秘像素;最后利用最低有效位替换将秘密数据嵌入到隐秘像素的最低有效位中,以进一步提高嵌入容量。实验结果表明,利用中心折叠技术与最低有效位替换来嵌入秘密数据,嵌入容量达到了 1 572 778 位,有效地提高了嵌入容量;当嵌入容量相同时,与嵌入秘密数据后的相关算法相比,图像的 PSNR 提高了约 2 dB,降低了图像失真,具有更好的不可感知性。

关键词:可逆数据隐藏;最低有效位替换;中心折叠;高容量

中图分类号:TP391 **文献标识码:**A **doi:**10.3788/YJYXS20193404.0410

High-capacity reversible data hiding based on CFT and LSB

REN Ke-qiang*, XIAO Lu-yao

(School of Information Engineering, Jiangxi University of Science and Technology,
Ganzhou 341000, China)

Abstract: Aiming at the contradictory problem between image quality and embedding capacity in reversible data hiding, a reversible data hiding method combining central folding technology with minimum effective bit replacement is proposed. Firstly, the pixel in the original image is divided into two bit planes. Then the secret data is folded by using the central folding technology, and the folded secret data is embedded into the highest effective bit of the original pixel to generate two hidden pixels. Finally, the secret data is embedded into the minimum effective bit of the hidden pixel with the least effective bit replacement to further improve the embedding capacity. The experimental results show that the embedding capacity is up to 1,572,778 bits by using the central folding technique and the minimum effective bit replacement to embed the secret data. When the embedding capacity is at the same time, compared with the relevant algorithms after embedding secret data, the PSNR of the image improves by about 2 dB, the image distortion is reduced, and has better imperceptibility.

Key words: reversible information hiding; least significant bit replacement; center folding; high capacity

收稿日期:2018-11-07;修订日期:2019-01-23.

基金项目:国家自然科学基金项目(No.61501210)

Supported by National Natural Science Foundation of China(No.61501210)

* 通信联系人, E-mail: jxrenkeqiang@163.com

1 引言

信息技术的快速发展使得多媒体数据在互联网上的传播变得越来越频繁,但互联网是一个开放空间,在传播过程中第三方可能会对数据进行非法监控、窃取、伪造或损坏。因此,多媒体数据的安全^[1-4]变得更加重要。数据隐藏技术是近年来为提高多媒体数据的安全性而广泛研究的领域之一,包括水印和隐写在内的数据隐藏技术可以分为不可逆的数据隐藏技术和可逆的数据隐藏技术^[5-6]。这种分类取决于通过提取秘密数据恢复原始图像的能力。

中心折叠技术(Center Folding Technique, CFT)和最低有效位(Least Significant Bit, LSB)替换方法是数据隐藏中常用的方法。中心折叠技术是折叠秘密数据并隐藏在双图像中。文献[7]提出了一种基于双图像的可逆数据隐藏方法,在将秘密数据嵌入载体图像之前,利用中心折叠的方法调整秘密数据的范围来减少图像的失真。提高了嵌入容量并且降低了图像失真。LSB替换方法^[8-9]是用秘密数据来替换像素的最低有效位。文献[10]提出了四像素差分 and 修改 LSB 替换的方法。秘密数据通过修改 k 位的 LSB 替换方法隐藏到每个像素中,其中 k 由四像素块的平均差值决定。文献[11]提出了基于 PVD 和 LSB 替换的隐写方法,使用 LSB 替换和最佳像素调整处理将秘密数据嵌入图像。在嵌入容量方面有很大提升,同时保持隐秘图像的质量,但算法复杂度高。文献[12]采用 Baker 算法进行图像置乱,利用人眼不敏感像素点的细微变化,利用 3 种颜色 R、G 和 B 的最低位用于图像隐藏。文献[13]提出一种改进的最低有效位(LSB)方法将一系列三进制秘密数据嵌入到载体图像中,使其易于嵌入和提取数据,同时具有高嵌入容量;但如果嵌入容量较低,隐秘图像的质量低。文献[14]提出一种基于位平面混合 PVD 和 LSB 高容量可逆数据隐藏,通过划分位平面,同时使用两种技术进行秘密数据嵌入,很大程度上提高了嵌入容量但隐秘图像质量还有待提高。

针对文献[13]的不足,本文提出一种基于中心折叠和最低有效位替换的大容量数据隐藏方法。首先将载体图像像素划分为两个位平面,然

后把秘密数据利用中心折叠技术进行折叠,实现秘密数据的嵌入,最后使用最低有效位替换方法在嵌入后的像素继续嵌入秘密数,以提高隐藏算法的性能。

2 相关工作

2.1 最低有效位替换

LSB 替换方法是隐写术在空间域中的替换方法,其原理用秘密数据比特替换 BMP 图像中的最低有效比特。这意味着,由于人眼对像素点的细微变化不敏感,3 种颜色 R、G 和 B 的最低位用于隐藏数据。因为数据隐藏在最低位,所以它相当于叠加微弱信号,因此很难在视觉上检测到它,但只要接收方知道隐藏数据的位置和嵌入时使用的算法,接收方就可以提取隐藏数据。

对于 k 比特 LSB 替换方法,可以将秘密比特嵌入到载体图像的像素中最右边的 k 个 LSB 中。设两个像素为 (p_i, p_{i+1}) , b_i 为秘密比特流,新像素 (p'_i, p'_{i+1}) 由式(1)得到。

$$(p'_i, p'_{i+1}) = \begin{cases} p_i - (p_i \bmod 2^k) + \sum_{i=0}^{k-1} b_i \\ p_{i+1} - (p_{i+1} \bmod 2^k) + \sum_{i=k}^{2k-1} b_i \end{cases}, \quad (1)$$

当 $k=2$ 时,给定两个像素 (145, 188), 通过用秘密位替换像素的 2 位 LSB 来获得新像素 (146, 191)。

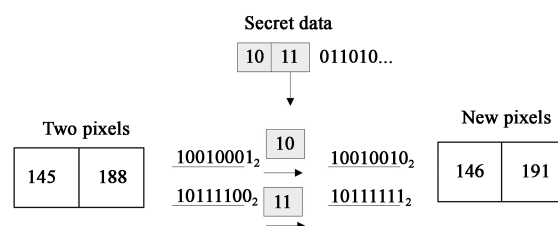


图1 LSB 替换示例($k=2$)

Fig.1 LSB substitution example($k=2$)

秘密比特可以直接从隐秘像素中提取而无需任何额外信息。

$$(b_i, b_{i+1}) = (p'_i \bmod 2^k, p'_{i+1} \bmod 2^k). \quad (2)$$

秘密比特 10_2 和 11_2 可以从图 1 中的 $146 = 100\ 10010_2$ 和 $191 = 10111111_2$ 中提取。

2.2 中心折叠技术

文献[7]使用中心折叠技术来减少秘密数据嵌入后的图像失真。选择 k 位二进制秘密数据并将其转换为十进制形式。秘密数据为 d , k 的秘密数据范围为 R , 使用中心折叠技术折叠秘密数据得到 $\bar{d}$ 。

$$\bar{d} = d - 2^k. \quad (3)$$

为了生成两个隐秘图像, 利用式(4)将 d 值分成两种类型。

$$\begin{cases} \bar{d}_1 = \lfloor \frac{2}{2} \rfloor \\ \bar{d}_2 = \lceil \frac{2}{2} \rceil \end{cases}. \quad (4)$$

将原始图像像素定义为 a , 将第一个隐秘图像像素定义为 $x'_{i,j}$, 第二隐秘图像像素定义为 $x''_{i,j}$, 利用式(5)将秘密数据嵌入到两个隐秘图像中。

$$\begin{cases} x'_{i,j} = x_{i,j} + \bar{d}_1 \\ x''_{i,j} = x_{i,j} - \bar{d}_2 \end{cases}, \quad (5)$$

当 $k=4$ 时, 像素值为 78, 通过中心折叠技术来获得新像素 75 和 80。

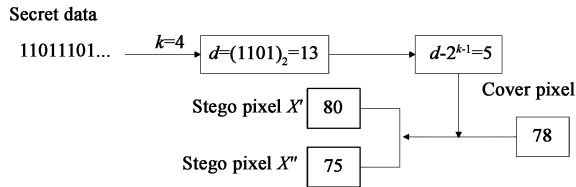


图 2 中心折叠技术示例($k=4$)

Fig.2 Framework of image measuring system

从 $x'_{i,j}$ 中减去隐秘像素 $x''_{i,j}$, 得到折叠的 $\bar{d}$, 然后通过中间值 2^{k-1} 恢复秘密比特 d 。

$$\begin{cases} \bar{d} = x'_{i,j} - x''_{i,j} \\ d = \bar{d} + 2^{k-1} \end{cases}, \quad (6)$$

将隐秘像素 $x'_{i,j}$ 和 $x''_{i,j}$ 进行平均获得原始像素 $x_{i,j}$ 。

$$x_{i,j} = \lceil \frac{x'_{i,j} + x''_{i,j}}{2} \rceil. \quad (7)$$

3 算法描述

3.1 融合中心折叠和最低有效位替换算法

通常, 传统的 LSB 替换方法只修改像素的两

个最低有效位, 从而可能会导致溢出。文献[13]是在最低有效位替换方法的基础上进行改进的。该方法可以在每个灰度像素中隐藏两个三进位数, 在嵌入之前, 通过在像素上加 1 或减 1 来解决溢出的问题, 使其变得容易嵌入和提取数据, 同时具有高嵌入容量。但是当嵌入容量较低时, 该方法并不比传统的 LSB 替换方法表现更好。为此, 本文引入了位平面的概念, 将载体图像的像素划分成两个位平面, 分别使用中心折叠技术和最低有效位替换方法嵌入秘密数据, 很好地解决了文献[13]中的问题, 同时, 很大程度上提高了嵌入容量。

3.2 嵌入过程

本文根据 k 的取值, 判断像素是否满足嵌入秘密数据的条件, 选取相应的像素采用融合中心折叠和最低有效位替换算法嵌入秘密数据, 嵌入秘密数据的方案如图 3 所示。

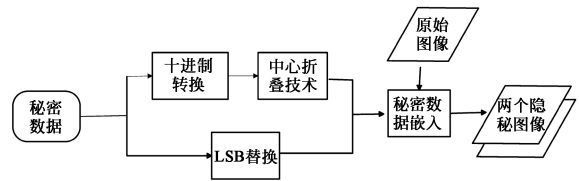


图 3 秘密数据嵌入方案流程图

Fig.3 Secret data embedding scheme flow chart

嵌入过程描述如下:

S1: 原始图像的像素记为: $X = \{x_{1,1}, x_{1,2}, x_{1,3}, \dots, x_{H,W}\}$ 其中 H 和 W 分别是图像的高度和宽度。判断像素 $x_{i,j}$ 的大小, 如果它在范围 $[2^k, 256 - 2^k]$ 内, 那么它可以用于嵌入。否则, 像素可能会导致溢出。溢出处理将在 3.4 节中描述。

S2: 利用式(8)将像素 $x_{i,j}$ 划分成两个位平面, 计算位平面的值 $(x_{i,j}^l, x_{i,j}^m)$ 。

$$\begin{cases} x_{i,j}^l = x_{i,j} \div 2^k \\ x_{i,j}^m = x_{i,j} \bmod 2^k \end{cases}, \quad (8)$$

其中: k 是秘密数据的个数, $x_{i,j}$ 为原始像素, $x_{i,j}^l$ 和 $x_{i,j}^m$ 是原始像素的两个位平面像素。

S3: 获取 k 个比特秘密数据 $S = \{s_1, s_2, s_3, \dots, s_k\}$ 并将其转换为十进制秘密符号 $d = \sum_{j=1}^k s_j 2^{k-1}$ 。为了避免由大的 d 值引起的图像失真, 使用中心折叠技术对 d 进行折叠。秘密符号的范围从 $R = \{0, 1, 2, 3, \dots, 2^{k-1}\}$ 变为 $\bar{R} =$

$\{-2^{k-1}, -2^{k-1}+1, \dots, -1, 0, 1, \dots, 2^{k-1}-2, 2^{k-1}-1\}$ 。使用式(9)将其相应地转移到新范围 $\bar{R}$, 以获得折叠的秘密符号 $\bar{d}$ 。

$$\bar{d} = d - 2^{k-1}, \quad (9)$$

其中: $\bar{d}$ 是折叠的秘密符号, 2^{k-1} 是中间值。使用式(9)将 d 转换为折叠的秘密符号 $\bar{d}$ 。当 $d < 2^{k-1}$, 它表示为负数。当 $d = 2^{k-1}$, 它表示为 0。当 $d > 2^{k-1}$, 它表示为正数。

S4: 将 $\bar{d}$ 代入式(6)中, 然后分成两部分: d_1 和 d_2 。通过平均方法将 $\bar{d}$ 嵌入到两个隐秘图像中以提高图像质量。

$$\begin{cases} x'_{i,j} = x_{i,j}^m + d_1 \\ x''_{i,j} = x_{i,j}^m - d_2 \end{cases}, \quad (10)$$

其中: d 被分成 d_1 和 d_2 , 它们被嵌入像素 $x_{i,j}^m$ 中以形成两个隐秘像素 $x'_{i,j}$ 和 $x''_{i,j}$ 。

S5: 将像素转化成二进制, 获取新的嵌入位 $n=k$, 将 $2n$ 比特秘密消息 $S = \{s_i | k \leq i \leq n+k, s_i \in \{0,1\}\}$ 和 $S = \{s_i | n+k \leq i \leq n+2k, s_i \in \{0,1\}\}$ 分别嵌入到隐秘像素 $x'_{i,j}$ 和 $x''_{i,j}$ 的低位平面, 并计算隐秘像素的和。

$$\begin{cases} x'_{i,j} = (x'_{i,j}^m \times 2^k) + \sum_{i=0}^{n-1} b_i^{l1} \\ x''_{i,j} = (x''_{i,j}^m \times 2^k) + \sum_{i=n}^{2n-1} b_i^{l2} \end{cases}. \quad (11)$$

S6: 重复 S1~S5 直到载体图像中的像素嵌入秘密比特流。

对于像素 $x_i = 45$, 秘密数据 $m = 110110_2$ 和 $n=k=2$, 获得 $x_i^m = 45 \div 2^2 = 11$ 和 $d = (11)_2 = 3$ 。将 d 进行折叠得到 $\bar{d} = d - 2^{n-1} = 1$ 。将秘密比特嵌入像素, 获得新像素 $x_i'^m = x_i^m + \lfloor \bar{d}/2 \rfloor = 11$ 和 $x_i''^m = x_i^m - \lceil \bar{d}/2 \rceil = 10$ 。接下来, 选择两个秘密比特 $b_i^l = 01_2$ 和 $b_i^l = 11_2$ 以嵌入每个像素。结果最终获得位平面的 $(x'_i, x''_i) = (11 \times 2^2 + 01_2, 10 \times 2^2 + 10_2) = (45, 42)$ 。

3.3 提取过程

提取秘密数据是反向嵌入的过程, 首先从隐藏像素的最低有效部分提取秘密数据, 再通过平均像素值恢复图像并提取秘密数据, 提取秘密数据的方案如图 4 所示。

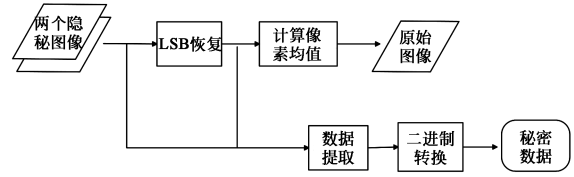


图4 秘密数据提取方案流程图

Fig. 4 Secret data extraction scheme flow chart

提取过程描述如下:

S1: 判断隐秘像素 $x'_{i,j}$ 和 $x''_{i,j}$ 是否相等, 如果 $x'_{i,j} = x''_{i,j}$ 并且该值不在 $[2^k, 256-2^k]$ 内, 则表示没有嵌入秘密数据, 即像素是原始像素。相反, 如果隐秘像素 $x'_{i,j}$ 或 $x''_{i,j}$ 在该范围内, 则表示嵌入了秘密数据。给定隐秘图像, 可以在不参考原始图像的情况下容易地提取嵌入的消息, 得到 $2k$ 比特秘密数据。

$$(b_i^l, b_i^m) = (x'_{i,j} \bmod 2^n, x''_{i,j} \bmod 2^n), \quad (12)$$

S2: 在同一平面上计算新像素 $(x'_{i,j}, x''_{i,j})$, 提取秘密数据。

$$(x_i'^m, x_i''^m) = \begin{cases} (x'_i - (x'_i \bmod 2^k)) \div 2^k \\ (x''_i - (x''_i \bmod 2^k)) \div 2^k \end{cases}, \quad (13)$$

$$\bar{d} = x_i'^m - x_i''^m, \quad (14)$$

$$d = \bar{d} + 2^{k-1}. \quad (15)$$

使用式(14)计算折叠的 $\bar{d}$, 将其代入式(15)中以计算 d 。然后将后者转换为二进制形式以获得 k 个秘密数据。

S3: 在图像恢复期间, 对隐秘像素 $x'_{i,j}$ 和 $x''_{i,j}$ 进行平均以获得原始像素 $x_{i,j}^m$ 。

$$x_{i,j}^m = \left\lceil \frac{x'_{i,j} + x''_{i,j}}{2} \right\rceil \times 2^{k-1}. \quad (16)$$

S4: 重复 S1~S3 直到秘密比特流全部提取。

对于两个隐秘像素 $(x'_i, x''_i) = (45, 42)$ 和 $k=2$ 。可以分别提取两个秘密比特 $(b_i^{l1}, b_i^{l2}) = (45 \bmod 4, 42 \bmod 4) = (1, 2) = (01_2, 10_2)$ 。接下来, 计算 $(x_i'^m, x_i''^m) = ((x'_i - (x'_i \bmod 2^k)) \div 2^k, x''_i - (x''_i \bmod 2^k) \div 2^k) = (11, 10)$ 。最终可以提取秘密比特流 $d = (11 - 10) + 2^{2-1} = 3 = 11_2$ 。

3.4 溢出处理

在秘密数据嵌入的过程中, 当原始像素大于 $256 - 2^{k-1}$ 或小于 2^{k-1} 时, 会发生溢出的问题。在保证不加剧图像失真的前提下, 采用不嵌入或修

改像素的方法来解决这个问题。在信息提取和图像恢复过程中,如果两个隐秘图像的像素相等并且大于 $256 - 2^{k-1}$ 或小于 2^{k-1} ,那么此时的隐秘像素就是原始像素。

例如,当像素 $x_{i,j} = 3$ 和 $n = 3$ 时,嵌入范围是 $[2^{3-1}, 256 - 2^{3-1}] = [4, 252]$ 。由于像素 $x_{i,j} = 3$ 不在该范围内,所以隐秘像素是 $x'_{i,j} = 3$ 和 $x''_{i,j} = 3$ 。在提取期间, $x'_{i,j} = x''_{i,j} = 3$ 不在该范围内,因此确定数据未隐藏在该像素中。当像素 $x_{i,j} = 6$ 时,该值在该范围内,因此它可以嵌入数据。假设隐藏数据为 $m = 0011100$ 和 $k = 2$,此时 $d = 1$,折叠 d 得到 $\bar{d} = -3$,生成的隐秘像素为 $x'_{i,j} = 3$ 和 $x''_{i,j} = 12$ 。在提取期间, $x''_{i,j}$ 超出范围,但 $x'_{i,j}$ 仍然在范围内。由于这两个值不相等,这意味着数据被隐藏在其中。可以提取数据并按照上述过程恢复像素。

4 实验结果与分析

本文算法在 Windows 10 + MATLAB 2016 平台来验证其性能,在标准灰度测试图数据库中选取了 Lena、Airplane、Boat 和 Baboon 这 4 幅具有不同纹理特征的 512×512 的标准灰度图像作为原始图像,如图 5 所示。

本文算法的性能通过测量峰值信噪比(Peak



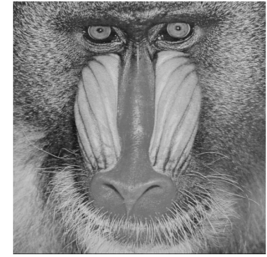
(a) Lena



(b) Airplane



(c) Boat



(d) Baboon

图 5 原始图像

Fig.5 Original image

Signal to Noise Ratio, PSNR) 和嵌入容量(Embedding Capacity, EC)来进行评估。秘密数据的嵌入容量意味着可以嵌入原始图像中的秘密数据量,峰值信噪比意味着隐秘图像的失真程度。PSNR 定义为:

$$\begin{cases} K_{\text{PSNR}} = 10 \times \lg \frac{255^2}{K_{\text{MSE}}} \\ K_{\text{MSE}} = \frac{1}{W \times H} \sum_{i=1}^W \sum_{j=1}^H (X_{i,j} - X'_{i,j})^2 \end{cases}, \quad (17)$$

其中: K_{MSE} 是均方误差 (Mean Square Error, MSE), $W \times H$ 是整个图像的大小, $X_{i,j}$ 是载体图像中 (i, j) 点的像素值, $X'_{i,j}$ 是隐秘图像中 (i, j) 点的像素值。

3 种算法的嵌入容量 (EC) 和峰值信噪比 (PSNR) 的实验结果如表 1 所示。文献[13]平均可以嵌入 960 065 位秘密数据,平均 PSNR 为 37.65 dB。文献[14]将平均嵌入容量提高到了 1 051 542。相比文献[13]和文献[14]的算法,本文算法很大程度上提高了嵌入容量,平均嵌入容量为 1 572 778 位。从实验结果可以看出,本文算法在嵌入容量和图像质量之间保持了很好的平衡,即提高嵌入容量的同时很好地保证了图像的质量。

表 1 不同算法的最大嵌入容量和视觉图像质量的比较

Tab.1 Comparison of maximum embedding capacity and visual image quality of different algorithms

图像	文献[13]		文献[14]		本文算法	
	EC /bits	PSNR /dB	EC /bits	PSNR /dB	EC /bits	PSNR /dB
Lena	960 100	37.64	1 049 742	33.21	1 572 764	35.92
Airplane	960 102	37.63	1 050 973	34.56	1 572 858	35.91
Boat	958 970	37.66	1 054 327	31.74	1 572 630	35.88

续表

图像	文献[13]		文献[14]		本文算法	
	EC /bits	PSNR /dB	EC /bits	PSNR /dB	EC /bits	PSNR /dB
Baboon	961 088	37.69	1 051 124	32.84	1 572 858	35.90
平均值	960 065	37.65	1 051 542	33.09	1 572 778	35.90

图6是Lena、Airplane、Boat和Baboon4幅标准灰度图像中不同秘密数据的嵌入容量与PSNR之间的关系比较。从图6中3种算法的性能曲线中看出,文献[14]基于文献[13]提高了一定的嵌入容量,但相应地,对于相同的嵌

入能力,图像质量略有下降。本文算法的性能优于比较的文献[13]和文献[14],提高嵌入容量的同时图像的质量也得到提高。本文算法的平均嵌入容量为1 572 778 bit,平均PSNR为35.90 dB。

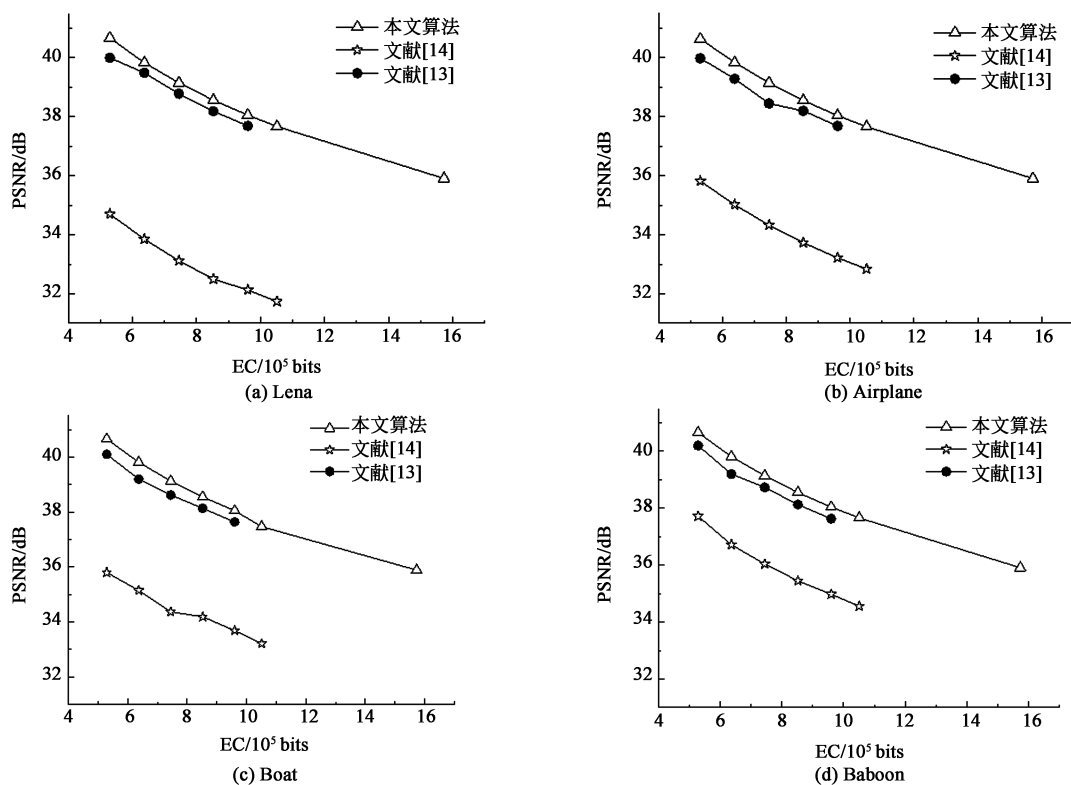


图6 3种算法性能的比较

Fig.6 Performance comparison of three algorithms

5 结 论

针对嵌入容量较低时隐秘图像质量较低的问题,本文提出了一种大容量的基于中心折叠和最低有效位替换的数据隐藏方法。在同一位平面中同时使用中心折叠技术和最低有效位替换来提高

嵌入容量。首先在每个像素上生成两个位平面。在最高有效位中使用中心折叠技术,并且在位平面中的 k 位区域上应用最低有效位替换。实验结果表明,与文献[13]和文献[14]相比,本文算法的嵌入容量增加了512 236~612 713位;图像的质量提高了约2 dB,是一种有效可行的数据隐藏方法。

参 考 文 献:

- [1] KHAN A, SIDDIQA A, MUNIB S, *et al.* A recent survey of reversible watermarking techniques [J]. *Information Sciences*, 2014, 279: 251-272.
- [2] 姚军财. 基于人眼对比敏感视觉特性的彩色图像盲水印算法[J]. 液晶与显示, 2017, 32(8): 642-649.
YAO J C. Blind watermarking algorithm for colour image based on human visual contrast sensitivity characteristics [J]. *Chinese Journal of Liquid Crystals and Displays*, 2017, 32(8): 642-649. (in Chinese)
- [3] DING H Y, LI Z C, YANG Y X, *et al.* High quality data hiding in halftone image based on block conjugate [J]. *Chinese Journal of Electronics*, 2018, 27(1): 150-158.
- [4] 韩佳伶, 赵晓晖. 基于图像梯度预测的可调节大容量可逆数据隐藏[J]. 吉林大学学报: 工学版, 2016, 46(6): 2074-2079.
HAN J L, ZHAO X H. Adjustable reversible data hiding algorithm with large embedded capacity based on image gradient prediction [J]. *Journal of Jilin University (Engineering and Technology Edition)*, 2016, 46(6): 2074-2079. (in Chinese)
- [5] SUBHEDAR M S, MANKAR V H. Current status and key issues in image steganography: A survey [J]. *Computer Science Review*, 2014, 13-14: 95-113.
- [6] 刘芳, 汪玉凯. 基于插值预测和块分类的低失真可逆数据隐藏[J]. 光电子·激光, 2013, 24(7): 1392-1398.
LIU F, WANG Y K. Reversible data hiding with low distortion based on interpolation prediction and dividing blocks model [J]. *Journal of Optoelectronics · Laser*, 2013, 24(7): 1392-1398. (in Chinese)
- [7] LU T C, WU J H, HUANG C C. Dual-image-based reversible data hiding method using center folding strategy [J]. *Signal Processing*, 2015, 115: 195-213.
- [8] YANG W X, TANG S Y, Li M Q, *et al.* Steganalysis of low embedding rates LSB speech based on histogram moments in frequency domain [J]. *Chinese Journal of Electronics*, 2017, 26(6): 1254-1260.
- [9] FRIDRICH J, GOLJAN M. Practical steganalysis of digital images: state of the art [C]//*Proceedings of the Security and Watermarking of Multimedia Contents IV*. San Jose, California, United States: SPIE, 2002.
- [10] LIAO X, WEN Q Y, ZHANG J. A steganographic method for digital images with four-pixel differencing and modified LSB substitution [J]. *Journal of Visual Communication and Image Representation*, 2011, 22(1): 1-8.
- [11] KHODAEI M, FAEZ K. New adaptive steganographic method using least significant-bit substitution and pixel-value differencing [J]. *IET Image Processing*, 2012, 6(6): 677-686.
- [12] 牛振喜. 基于 LSB 及置乱的图像隐藏算法研究[J]. 西北工业大学学报, 2013, 31(2): 300-304.
NIU Z X. An effective hiding algorithm based on LSB (Least Significant Bit) and scrambling [J]. *Journal of Northwestern Polytechnical University*, 2013, 31(2): 300-304. (in Chinese)
- [13] XU W L, CHANG C C, CHEN T S, *et al.* An improved least-significant-bit substitution method using the modulo three strategy [J]. *Displays*, 2016, 42(5): 36-42.
- [14] JUNG K H. Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane [J]. *Journal of Real-Time Image Processing*, 2018, 14(1): 127-136.

作者简介:



任克强(1959—),男,湖南汨罗人,硕士,教授,1993年于华中理工大学获得硕士学位,现为江西理工大学教师,主要从事图像与视频处理、信息隐藏方面的研究。E-mail: jxrenkeqiang@163.com