



基于Paillier加密的大容量双图像可逆信息隐藏

牛宇航, 申淑媛, 吕浩杰, 林焕桀

引用本文:

牛宇航,申淑媛,吕浩杰,林焕桀. 基于Paillier加密的大容量双图像可逆信息隐藏[J]. 液晶与显示, 2022, 37(3): 376–385.

NIU Yu-hang, SHEN Shu-yuan, LYU Hao-jie, LIN Huan-jie. High-capacity dual-image reversible data hiding based on Paillier[J]. *Chinese Journal of Liquid Crystals and Displays*, 2022, 37(3): 376–385.

在线阅读 View online: <https://doi.org/10.37188/CJLCD.2021-0220>

您可能感兴趣的其他文章

Articles you may be interested in

融合CFT和LSB的高容量可逆数据隐藏

High-capacity reversible data hiding based on CFT and LSB

液晶与显示. 2019, 34(4): 410–416 <https://doi.org/10.3788/YJYXS20193404.0410>

基于二维串联调制耦合映射的图像加密-秘密分享算法

Image encryption-secret sharing algorithm based on two-dimensional cascade modulation coupling map

液晶与显示. 2019, 34(12): 1210–1217 <https://doi.org/10.3788/YJYXS20193412.1210>

一种基于新超混沌Chen系统的置乱替代相结合的加密算法

Encryption algorithm based on scrambling substitution of new hyperchaotic Chen system

液晶与显示. 2020, 35(1): 91–97 <https://doi.org/10.3788/YJYXS20203501.0091>

基于人眼对比敏感视觉特性的彩色图像盲水印算法

Blind watermarking algorithm for colour image based on human visual contrast sensitivity characteristics

液晶与显示. 2017, 32(8): 642–649 <https://doi.org/10.3788/YJYXS20173208.0642>

基于遗传-超混沌的数字图像加密算法设计

Digital image encryption algorithm design based on Genetic-hyperchaos

液晶与显示. 2017, 32(6): 474–481 <https://doi.org/10.3788/YJYXS20173206.0474>

文章编号:1007-2780(2022)03-0376-10

基于 Paillier 加密的大容量双图像可逆信息隐藏

牛宇航, 申淑媛*, 吕浩杰, 林焕桀

(华南师范大学 软件学院, 广东 佛山 528225)

摘要: 双图像可逆信息隐藏由于其具有更好的安全性、嵌入率和图像视觉质量, 成为信息安全领域重要的研究方向。Bhardwaj 等人提出了密文域上的双图像可逆信息隐藏算法, 进一步提升了安全性, 但是该算法嵌入秘密信息的数量有限。本文提出了一种新的嵌入策略, 先将图像的每个像素分解成 3 个单元, 并使用 Paillier 算法对其加密。根据改进的最大失真控制编码表, 采用平均法动态地嵌入秘密信息, 即每次嵌入秘密信息的位数是变化的。实验结果表明, 本文的方法比 Bhardwaj 等人的方法嵌入率提升了 0.72 bpp; 与原始的最大失真控制方法相比, 嵌入率提升了 0.25 bpp。同时能够无损地恢复原始图像, 保证其可逆性, 可以满足大容量场景下隐私保护和秘密通信的双重需求。

关键词: 可逆信息隐藏; 双图像; Paillier 加密; 大容量

中图分类号: TP391.4 **文献标识码:** A **doi:** 10.37188/CJLCD.2021-0220

High-capacity dual-image reversible data hiding based on Paillier

NIU Yu-hang, SHEN Shu-yuan*, LYU Hao-jie, LIN Huan-jie

(School of Software, South China Normal University, Foshan 528225, China)

Abstract: Dual-image reversible data hiding (RDH) has become an important research direction in the field of information security due to its better security, embedding rate and image visual quality. Bhardwaj *et al.* proposed a dual-image RDH algorithm on encrypted domain to further improve the security, but the embedding capacity of this algorithm is limited. In this paper, we propose a new embedding strategy by decomposing each pixel of an image into three units and encrypting them using the Paillier algorithm. According to the improved maximum distortion control coding table, the secret messages are embedded dynamically using the averaging method, *i.e.*, the number of bits of secret information is varied for each embedding. The experimental results show that the embedding rate of our method is improved by 0.72 bpp compared with the method of Bhardwaj *et al.* and 0.25 bpp compared with the original maximum distortion control method. At the same time, the original image can be recovered losslessly, so the reversibility is guaranteed. It can meet the dual requirements of privacy protection and secret communication in high-capacity scenarios.

Key words: reversible data hiding; dual-image; paillier encryption; high capacity

收稿日期: 2021-08-19; 修订日期: 2021-09-30.

基金项目: 广东省基础与应用基础研究基金 (No.2020B1515120089, No.2021A1515011171)

Supported by Basic and Applied Basic Research Foundation of Guangdong Province (No.2020B1515120089, No. 2021A1515011171)

* 通信联系人, E-mail: ssyuan16@m.scnu.edu.cn

1 引言

5G 的普及和各种互联网技术的快速发展给人们的生活带来了许多便利,但也给信息安全带来了许多前所未有的挑战。信息隐藏以不可见、隐蔽的方式将秘密信息嵌入到多媒体载体中,接收方通过特定的算法提取载体中秘密信息,从而实现版权保护^[1-2]、秘密通信等功能^[3-4],有效地解决信息安全问题。大部分信息隐藏算法可以将秘密信息正确地提取出来,但会对多媒体载体造成永久的损害。然而在军事、医学和遥感等特殊的场景,不仅要求嵌入的秘密信息能够被完整提取,多媒体载体也要能够无损地恢复。为了满足这些需求,可逆信息隐藏技术^[5]应运而生,接收方在提取出秘密信息的同时可以完整地重建原始载体,具有很高的应用价值。

可逆信息隐藏可分为单图像和双图像两大类。单图像可逆信息隐藏主要包括无损压缩^[6]、差值扩展^[7]、直方图平移^[8]、预测误差扩展^[9]等。双图像可逆信息隐藏是可逆信息隐藏的另一个重要组成部分,近些年被许多学者关注和研究。顾名思义,双图像可逆信息隐藏技术将产生两张相似的载密图像,只有同时拥有两张载密图像才能正确地提取秘密信息并恢复原始载体图像。与单图像方法相比,双图像可逆信息隐藏技术具有更高的安全性和嵌入率。常见的双图像可逆信息隐藏方法分为基于 EMD (Exploiting modification direction) 和基于中心折叠两大类。

Chang 等^[10]在 2007 年首先将 EMD 技术和双图像结合,这种方法通过模函数产生一个 256×256 大小的模函数矩阵,两个秘密像素的值通过 5×5 大小的子矩阵对角线的值决定。Qin 等^[11]使用 EMD 方法在第一张载密图像上嵌入秘密信息,并根据第一张载密图像自适应地修改第二张载密图像,该方法产生的两张载密图像质量是不一样的,第一张载密图像的视觉质量要明显好于第二张。Chen 等^[12]充分利用 EMD 矩阵的特征,将一位秘密信息和一个五进制的数嵌入到一对像素中。文献^[13]于 2015 年提出了基于中心折叠策略的双图像可逆信息隐藏技术, k 位二进制秘密信息被转换为十进制后,再通过中心折叠策略和平均法嵌入到两张载密图像中。文献^[14]将中

心折叠技术和最低有效位结合,提升了载密图像的视觉质量。Meikap 等人^[15]在 2021 年将多方向像素值排序技术和中心折叠技术结合,提升了载密图像的嵌入容量。Lu 等人^[16]采用最大失真控制编码表策略,进一步折叠了十进制秘密信息的大小。

以上这些都是明文域上的双图像可逆信息隐藏方法。Bhardwaj 等^[17]首次提出了密文域上的双图像可逆信息隐藏方法。该方法先将图像的每个像素分解成 3 个单元,并将分解后的单元使用 Paillier 算法^[18]加密。然后将秘密信息转化为三进制,即 0,1,2,三进制秘密信息对应 3 种不同的嵌入操作。根据三进制秘密信息的值对加密后的密文值进行不同的修改,产生两个载密的密文。

但是该方法嵌入秘密信息的数量有限,仍有提升空间。本文采用改进的最大失真控制编码表,先将分解后的图像采用 Paillier 算法加密,然后通过平均法动态地嵌入秘密信息(每次嵌入的秘密信息位数是变化的)。最后产生的载密密文具有更高的嵌入率,同时能够无损地恢复出原始载体图像。本文将密码学技术和信息隐藏技术结合,能更好地保护隐私和传递秘密信息。

2 相关工作

2.1 Paillier 加密

Paillier 加密^[18]是一种典型的同态非对称加密算法,加密使用的密钥(公钥)和解密使用的密钥(私钥)是不同的。不同于对称密钥算法,此加密算法不需要在发送方和接收方共享密钥,具有更好的安全性。Paillier 加密算法包括密钥生成、数据加密、数据解密 3 部分:

(1) 密钥生成:随机选择两个大质数 p 和 q , 计算 $N = pq$ 和 $\lambda = L_{\text{lcm}}(p-1, q-1)$, L_{lcm} 表示最小公倍数。再随机选择 $(1, n^2)$ 上的正整数 g , 即 $g \in Z_{N^2}^*$, 并满足:

$$G_{\text{gcd}}(S(g^\lambda \bmod N^2), N) = 1, \quad (1)$$

其中: G_{gcd} 表示最大公约数, $\bmod$ 为取模操作。 $S(x)$ 定义如下: $S(x) = \frac{x-1}{n}$ 。

Paillier 加密算法中的公钥为 (g, N) , 私钥为 λ 。

(2) 数据加密:对于任意待加密整数 $m \in Z_N$,

任意选择随机数 r , 使用公钥 (g, N) 加密得到密文:

$$C = E[m] = g^m r^N \bmod N^2. \quad (2)$$

(3) 数据解密: 对于密文 C , 通过私钥进行解密得到明文, 计算方法如下:

$$m = D[C] = \frac{S(C^\lambda \bmod N^2)}{S(g^\lambda \bmod N^2)} \bmod N. \quad (3)$$

通过加密操作公式(2)可以看出, 当选择的随机数 r 不同时, 对同一个明文加密得到的密文值不一定相同, 这使得 Paillier 算法的安全性和可靠性进一步提升。

同时 Paillier 算法满足加法同态, 对于任意的明文 m_1 和 m_2 , 假设

$$E[m_1] = g^{m_1} r_1^N \bmod N^2, E[m_2] = g^{m_2} r_2^N \bmod N^2,$$

则:

$$\begin{cases} E[m_1]E[m_2] = g^{m_1+m_2} (r_1 r_2)^N \bmod N^2 \\ D[E[m_1]E[m_2] \bmod N^2] = (m_1 + m_2) \bmod N \end{cases} \quad (4)$$

2.2 最大失真控制双图像可逆信息隐藏方法

Lu 等^[14]在 2020 年提出了基于最大失真控制的双图像可逆信息算法。此算法中编码数量 (Number of codes, NC) 和最大失真 (Maximum distortion, MXD) 用来调整失真程度, 并生成对应的编码组合表。其中, NC 表示每个编码组合中编码的数量, MXD 表示编码组合造成的最大失真。表 1 展示了 NC=3, MXD=2 时的所有编码组合, 其中 d 代表秘密信息十进制值, E 表示损失值。

最大失真控制通过变量 MXD 有效地将载密图像损失控制在一个可控的范围, 提升载密图像的视觉质量, 但是该方法不能充分利用编码组合表。表 1 中共有 25 种编码组合, 而每次可以嵌入二进制秘密信息的位数 $k = \log_2 25 = 4$ 。

4 位二进制秘密信息对应的十进制为 (0, 15), 只需要表 1 中的前 16 个编码组合即可, 后面 9 个编码组合并没有被利用到。如果嵌入 5 位二进制秘密信息, 需要 32 个编码组合, 则需要增大 NC 或者 MXD 的值。增大它们的值后, 编码表的组合也会随之增大, 仍会有部分编码组合没有被充分利用。为了解决此问题, 本文的算法嵌入秘密信息的位数将采用 4 位和 5 位相结合的方式, 从而更好地利用编码表。

表 1 NC=3 和 MXD=2 时所有编码组合

Tab.1 All code combinations for NC=3 and MXD=2

s	d	Sd_1	Sd_2	Sd_3	E
0000	0	0	0	0	0
0001	1	0	0	1	1
0010	2	0	1	0	1
0011	3	1	0	0	1
0100	4	-1	0	0	1
0101	5	0	-1	0	1
0110	6	0	0	-1	1
0111	7	0	1	1	2
1000	8	1	0	1	2
1001	9	1	1	0	2
1010	10	-1	0	1	2
1011	11	-1	1	0	2
1100	12	0	-1	1	2
1101	13	1	-1	0	2
1110	14	0	1	-1	2
1111	15	1	0	-1	2
—	16	-1	-1	0	2
—	17	-1	0	-1	2
—	18	0	-1	-1	2
—	19	0	0	2	2
—	20	0	2	0	2
—	21	0	0	2	0
—	22	-2	0	0	2
—	23	0	-2	0	2
—	24	0	0	-2	2

3 嵌入和提取恢复过程

本节将详细描述本文所提出的方法, 算法整体的流程如图 1 所示。具体可分为秘密信息嵌入、秘密信息提取及原始图像恢复 3 部分。

3.1 秘密信息嵌入过程

(1) 预处理图像。将原始图像的每个像素 p_i 分解成 x_i, y_i, z_i 三个单元, 即 $p_i = x_i + y_i + z_i$ 。后续的嵌入操作中, 三单元将作为一个整体进行

嵌入。具体分解规则如下:

$$\begin{cases} x_i = p_i - 2, y_i = z_i = 1, 2 < p_i < 254 \\ x_i = p_i, y_i = z_i = 0, \text{ else} \end{cases} \quad (5)$$

(2) 使用 Paillier 算法对 x_i, y_i, z_i 三个单元加密, 加密后的 3 个单元记作 (x_i^*, y_i^*, z_i^*) , 得到加密的密文 E 。

(3) 复制密文 E , 得到两个相同的密文 E_1 和 E_2 。

(4) 构造新的编码表。原始像素被分解成 3 个单元, 因此 $NC=3$; 同时为了保证从载密密文中提取出载密明文图像的视觉质量, $MXD=2$ 。进一步, 为了充分利用编码表, 新的编码表对应嵌入二进制信息的位数 k 可能是 4 位, 也可能是 5 位。新编码表如表 2 所示, 其中 s 代表二进制的秘密信息。

(5) 确定本次嵌入秘密信息的位数 k 。从表 2 可以看出, 当 4 位秘密信息十进制值小于等于 6, 则 $k=4$; 如果 4 位秘密信息对应的十进制值大于

表 2 $NC=3$ 和 $MXD=2$ 时优化编码组合

Tab.1 Optimal code combinations for $NC=3$ and $MXD=2$

s	d	Sd_1	Sd_2	Sd_3	E
0000	0	0	0	0	0
0001	1	0	0	1	1
0010	2	0	1	0	1
0011	3	1	0	0	1
0100	4	-1	0	0	1
0101	5	0	-1	0	1
0110	6	0	0	-1	1
01110	14	0	1	1	2
01111	15	1	0	1	2
10000	16	1	1	0	2
10001	17	-1	0	1	2
10010	18	-1	1	0	2
10011	19	0	-1	1	2
10100	20	1	-1	0	2
10101	21	0	1	-1	2
10110	22	1	0	-1	2
10111	23	-1	-1	0	2
11000	24	-1	0	-1	2
11001	25	0	-1	-1	2
11010	26	0	0	2	2
11011	27	0	2	0	2
11100	28	0	0	2	0
11101	29	-2	0	0	2
11110	20	0	-2	0	2
11111	31	0	0	-2	2

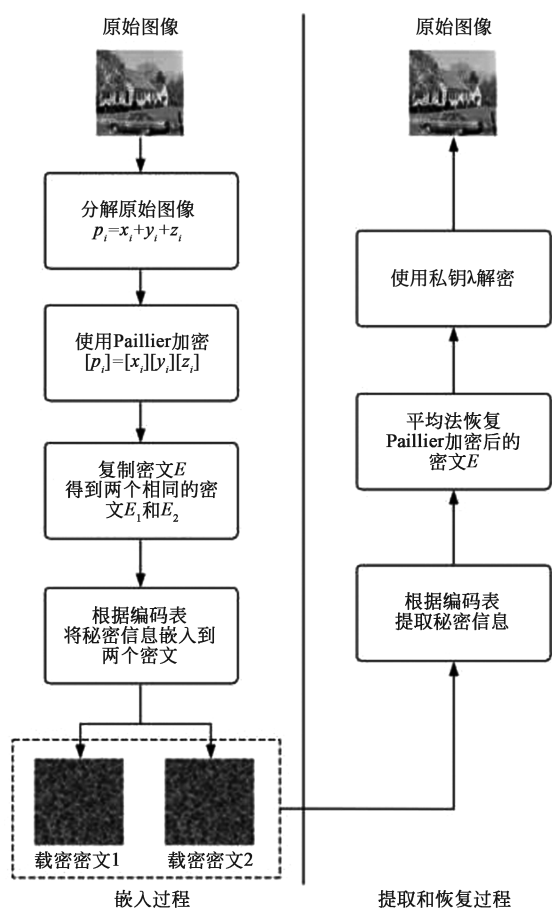


图 1 本文的算法流程图

Fig.1 Flow chart of the proposed method

6, 则 $k=5$ 。具体计算方法如下:

$$k = \begin{cases} 4, d_{s4} \leq 6 \\ 5, d_{s4} > 6 \end{cases} \quad (6)$$

(6) 采用平均法将秘密信息嵌入到密文 E_1 和 E_2 中。为了保证不产生溢出问题, $y_i = z_i = 0$ 对应的组不嵌入任何秘密信息, 即对这样的组不会做任何操作。根据编码表, 找到当前 k 位秘密信息对应的 Sd_1, Sd_2, Sd_3 。具体嵌入操作如公式 (7) 所示, 其中 x'_i 和 x''_i 分别表示密文 E_1 和 E_2 的 x_i^* 单元对应的载密密文值。这里只给出了对

x_i^* 单元的修改操作, y_i^* 和 z_i^* 单元的修改操作和 x_i^* 单元类似, 只需把 Sd_1 分别换为 Sd_2 和 Sd_3 , 不再重复表述。

$$\begin{cases} x'_i = x_i^* + \left\lfloor \frac{Sd_1}{2} \right\rfloor \\ x''_i = x_i^* - \left\lfloor \frac{Sd_2}{2} \right\rfloor \end{cases} \quad (7)$$

(7) 重复步骤(5)~(6), 直到将所有的秘密信息嵌入完毕, 获得载密密文 E'_1 和 E'_2 。

3.2 秘密信息提取及原始图像恢复过程

(1) 预处理图像, 恢复 Paillier 加密后的密文 E 。和嵌入过程类似, 载密密文 E'_1 和 E'_2 的每组元素是包含 (x'_i, y'_i, z'_i) 或 (x''_i, y''_i, z''_i) 3 个单元的密文。采用平均法恢复出 (x_i^*, y_i^*, z_i^*) , 计算方法如公式(8)所示, y_i^* 和 z_i^* 的恢复方法和 x_i^* 类似, 这里不再重复。

$$x_i^* = \left\lfloor \frac{x'_i + x''_i}{2} \right\rfloor. \quad (8)$$

(2) 恢复原始图像。采用 Paillier 对 (x_i^*, y_i^*, z_i^*) 解密得到明文 (x_i, y_i, z_i) , 所以原始像素 $p_i = x_i + y_i + z_i$ 。

(3) 根据编码表提取秘密信息。在嵌入阶段, $y_i = z_i = 0$ 对应的组没有秘密信息。因为已经恢复出原始图像, 所以在提取秘密信息时, 将跳过原始像素 $p_i \leq 2$ 和 $p_i \geq 245$ 的这些像素。由 (x'_i, y'_i, z'_i) 和 (x''_i, y''_i, z''_i) 可以计算出当前组对应的 Sd_1, Sd_2, Sd_3 :

$$\begin{cases} Sd_1 = x'_i - x''_i \\ Sd_2 = y'_i - y''_i \\ Sd_3 = z'_i - z''_i \end{cases} \quad (9)$$

(4) 重复第 3 步, 直到所有的秘密信息提取完毕。

4 实验结果和分析

本节将给出本文算法的实验结果, 并与其他算法进行实验结果比较。8 张大小为 512×512 的标准灰度图像被用来进行测试, 分别是 Lena、Baboon、Barbara、Airplane、Boat、Elaine、Lake、Peppers, 如图 2 所示, 秘密信息是随机生成的二进制数。将从图像的不可感知性和嵌入率两方面评估算法性能。

采用峰值信噪比(Peak signal-to-noise ratio,



图 2 8 幅标准测试图像

Fig.2 Eight standard test images

PSNR) 和结构相似度 (Structural similarity, SSIM) 来衡量载密图像的不可感知性。载密图像失真越小, 图像的视觉质量和不可感知性就越好, 说明载密图像和原始图像越接近, 反之亦然。PSNR 从基于像素点误差衡量载密图像的不可感知性和失真, PSNR 值越大, 载密图像和原始载体图像越接近。对于灰度图像来说, 当 PSNR 大于 35 dB 时, 人眼基本无法察觉载密图像和原始图像的差别。这里的载密图像指的是从嵌入过程最后产生的载密密文中提取出来的图像, 而不是载密密文。因为载密密文是无法理解的密文, 不能直接拿来和原始图像计算 PSNR。假设 (x'_i, y'_i, z'_i) 解密后对应值为 $(m'_{1i}, m'_{2i}, m'_{3i})$, 实验中我们将 N 设置的足够大, 保证 $m'_{1i} + m'_{2i} + m'_{3i} < N$, 那么 $(m'_{1i} + m'_{2i} + m'_{3i}) \bmod N = m'_{1i} + m'_{2i} + m'_{3i} = m'$ 。因为 Paillier 加密满足加法同态, 根据公式(4)将密文 (x'_i, y'_i, z'_i) 相乘并对 N^2 取模, 对取模的结果进行解密, 便可得到 (x'_i, y'_i, z'_i) 三单元载密像素 m' 。 (x''_i, y''_i, z''_i) 对应的载密像素 m'' 计算方法也是如此, 这里不再赘述。表 3 展示了本文方法在嵌入容量分别为 10 000, 20 000, 30 000 bit 时的 PSNR, 其中 PSNR_1, PSNR_2, PSNR_Avg 分别表示从第一张载密图像、第二张载密图像以及 2 张图像的平均 PSNR。从表 3 中可以看出, 在 8 张标准测试图像上, 当嵌入容量为 10 000, 20 000, 30 000 bit 时对应的平均 PSNR 分别为 50.55, 47.57, 45.81 dB。PSNR 从对应像素点误差的角度去评价图像质量, 没有考虑到人类视觉系统对亮度差异、对比度差异等的敏感性。

SSIM 认为图像是高度结构化的, 从亮度、对比度和结构 3 方面衡量载密图像和原始图像之间的相似性。取值范围为 $(0, 1)$, 其值越接近于 1,

表 3 本文方法的 PSNR 值(嵌入容量分别为 10 000,20 000,30 000 bit)
Tab.3 PSNR(dB) of our method (EC of 10 000, 20 000 and 30 000 bit, respectively)

比特数	评价标准	Airplane	Barbara	Boat	Baboon	Lena	Peppers	Lake	Elaine	Average
10 000	PSNR_1/dB	50.65	50.54	50.67	50.50	50.70	50.59	50.55	50.47	50.58
	PSNR_2/dB	50.56	50.47	50.62	50.51	50.61	50.53	50.39	50.52	50.52
	PSNR_Avg/dB	50.60	50.50	50.64	50.50	50.65	50.56	50.47	50.50	50.55
20 000	PSNR_1/dB	47.63	47.59	47.60	47.59	47.82	47.46	47.52	47.54	47.60
	PSNR_2/dB	47.49	47.49	47.59	47.55	47.71	47.37	47.55	47.62	47.55
	PSNR_Avg/dB	47.56	47.54	47.60	47.57	47.77	47.42	47.54	47.58	47.57
30 000	PSNR_1/dB	45.71	45.74	45.83	45.74	45.94	45.80	45.82	45.85	45.80
	PSNR_2/dB	45.81	45.87	45.78	45.74	45.95	45.74	45.77	45.91	45.82
	PSNR_Avg/dB	45.76	45.80	45.81	45.74	45.94	45.77	45.79	45.88	45.81

表明两张图像之间越相似。表 4 给出了嵌入容量为 30 000 bit 时,本文方法在 8 张测试图像上的 SSIM 值,其中 SSIM_1, SSIM_2, SSIM_Avg 分别表示从第一张载密图像、第二张载密图像以及两张图像的平均 SSIM 值。当嵌入容量为 30 000 bit 时,本文方法的平均 SSIM 值为 0.97,这从另一角度验证了本算法产生的载密图像具有较好的视觉质量。

表 4 本文方法嵌入容量为 30 000 bit 对应的 SSIM 值
Tab.4 SSIM of our method for an EC of 30 000 bit

Image	SSIM_1	SSIM_2	SSIM_Avg
Airplane	0.97	0.98	0.97
Barbara	0.98	0.97	0.97
Boat	0.98	0.98	0.98
Baboon	0.98	0.97	0.97
Lena	0.97	0.97	0.97
Peppers	0.97	0.97	0.97
Lake	0.98	0.98	0.98
Elaine	0.97	0.98	0.97
Average	0.97	0.97	0.97

为了更直观地展示本文方法的有效性,图 3 展示了图像 Lena 在嵌入容量为 30 000 bit 时的结果,其中图 3(a)和图 3(b)是对应的第一张和第二张载

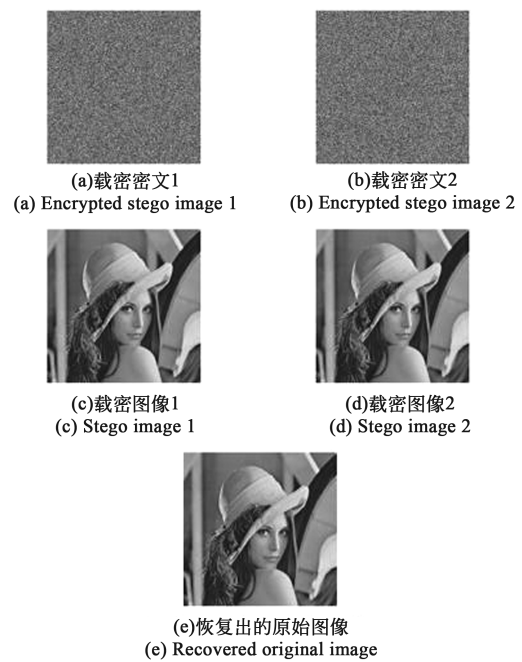


图 3 图像 Lena 在嵌入容量为 30 000 bit 时的实验结果

Fig.3 Experimental results of image Lena for an EC of 30 000 bit

密密文,图 3(c)和图 3(d)是从第一张和第二张载密密文中提取的载密图像,图 3(e)是从两张载密密文中恢复得到的载体图像。可以看出,载密图像(图 3(c)和图 3(d))和原始图像没有明显的差别,人眼无法区分。恢复出的原始图像图 3(e)和原始

图像是完全相同的,即每个像素对应的像素值都相等,这是可逆信息隐藏的最主要特性。从嵌入过程和提取恢复过程的数学表达式中,可以推导出算法是严格可逆的。图 4 展示了图像 Lena 不同嵌入容量提取秘密信息的错误率,本文算法从载密密文中提取的秘密和嵌入的秘密信息是完全一致的。二进制秘密信息能够准确无误全部提取是可逆信息隐藏的基本要求之一。其他图像的实验结果和 Lena 相似,由于篇幅原因不再展示。在实际应用中,本文的方法是在密文域进行的,传送给接收方的是载密密文。接收方可以直接从两个载密密文中提取出秘密信息并恢复出原始图像,并不需要进行从载密密文中(图 3(a),(b))提取载密图像(图 3(c),(d))这一操作。因此这里只展示了本文方法的 PSNR 和 SSIM 值,并没有和其他明文域的方法进行对比。但仍然可以看到,本

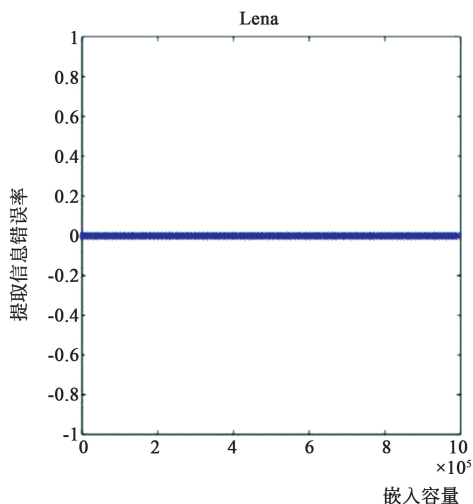
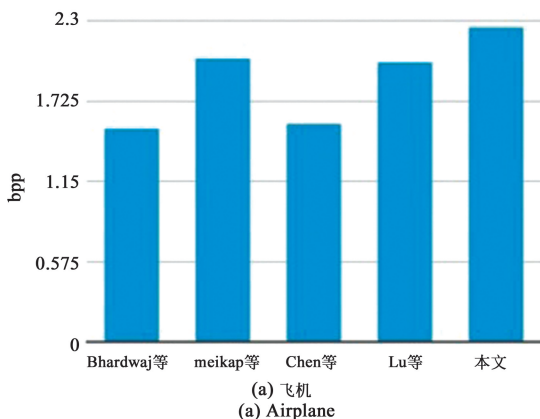


图 4 嵌入容量和错误率的关系

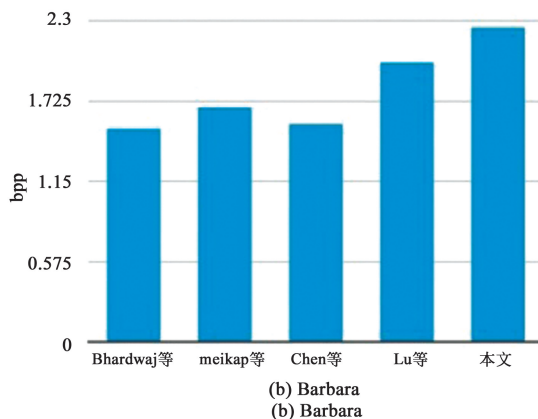
Fig.4 Error rate and the EC of the experiment results



(a) 飞机
(a) Airplane

文方法在嵌入容量分别为 10 000, 20 000, 30 000 bit 时对应的 PSNR 均在 35 dB 以上, 30 000 bit 对应的平均 SSIM 值为 0.97, 满足实际应用中对载密图像视觉质量的要求。

图 5 展示了本文方法和 Bhardwaj 等^[17]、Chen 等^[12]、Meikap 等^[15]以及 Lu 等^[16]的方法在 8 张标准测试图像上的最大嵌入率。对于双图像信息隐藏方法, 嵌入率等于嵌入容量除以图像尺寸后再除以 2。嵌入率越高, 表明算法可以嵌入越多的秘密信息, 算法的性能就越好。与密文域的双图像方法相比, Bhardwaj 等^[17]将秘密信息转化为三进制, 即 0, 1, 2。然后根据秘密信息的值分 3 种不同的操作方式, 将秘密信息嵌入到 Paillier 加密后密文中, 达到了 1.53 bpp 的平均嵌入率, 本文方法嵌入率较其方法提升了 0.72 bpp。与明文域的方法相比, Chen 等^[12]的方法充分利用 EMD 矩阵的特征, 将一位秘密信息和一个五进制的数嵌入到一对像素中, 平均嵌入率为 1.56 bpp, 本文方法嵌入率较其方法提升了 0.69 bpp。Meikap 等^[13]在 2021 年将多方向像素值排序技术和中心折叠技术结合, 该方法依赖于像素值排序技术, 因此在平滑图像上的嵌入率要高于纹理图像的嵌入率。但是本文的方法在每张测试图像上的最大嵌入率仍然高于 Meikap 等人^[15]的方法。Lu 等人^[16]在同年提出了基于最大失真控制的方法, 根据 2.2 节的分析, 本文算法改进了失真编码表, 每次嵌入的秘密信息不再是固定的位数, 更充分利用了编码表, 最大嵌入率由 2 bpp 提升到 2.25 bpp, 提高了 12.5%。通过与以上最新的双图像可逆信息隐藏算法在嵌入率方面进行对比, 可以看出本文算法在嵌入率方面有显著的提升。



(b) Barbara
(b) Barbara

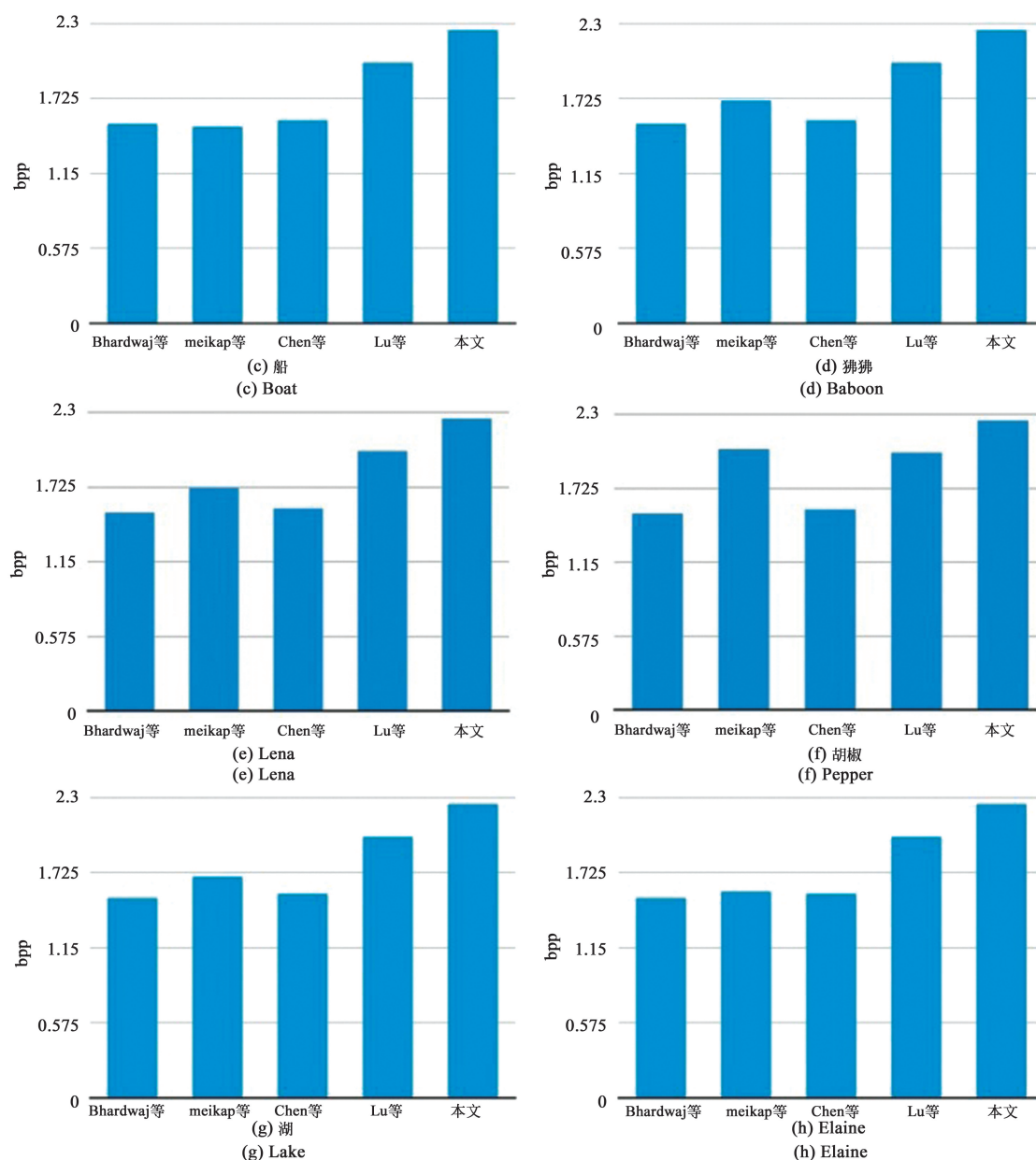


图5 本文方法和其他4种方法最大嵌入率对比

Fig.5 Comparison of maximum embedding rate between our method and other four methods

5 结 论

本文在 Bhardwaj 等人基础上提出了一种基于 Paillier 加密的双图像可逆信息隐藏方法。为了进一步提升嵌入率,将图像分解加密后,采用改进后的最大失真编码表,每次嵌入秘密信息的位数是动

态变化的,因此能更充分地利用失真编码表。实验结果表明,本文算法的嵌入率比 Bhardwaj 等人的方法提升了 0.72 bpp。与原始的失真控制方法相比嵌入率提升了 12.5%。本文方法需要先恢复原始图像,再提取秘密信息。设计一种提取秘密信息和恢复原始图像可以分离的算法是一个值得研究的方向,是未来工作的重点。

参 考 文 献:

- [1] 丁国绅,乔延利,易维宁,等.基于光谱图像空间的 F-SIFT 特征提取与匹配[J].光学精密工程,2021,29(5):

- 1180-1189.
- DING G S, QIAO Y L, YI W N, *et al.* Feature extraction and matching of F-SIFT based on spectral image space [J]. *Optics and Precision Engineering*, 2021, 29(5): 1180-1189. (in Chinese)
- [2] BENDER W, GRUHL D, MORIMOTO N, *et al.* Techniques for data hiding [J]. *IBM Systems Journal*, 1996, 35(3/4): 313-336.
- [3] 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)
- [4] 赵家旺, 张运海, 王发民, 等. 线扫描虚拟结构调制共聚焦显微成像[J]. 中国光学, 2021, 14(2): 431-445.
- ZHAO J W, ZHANG Y H, WANG F M, *et al.* Line-scanning confocal microscopic imaging based on virtual structured modulation [J]. *Chinese Optics*, 2021, 14(2): 431-445. (in Chinese)
- [5] NI Z C, SHI Y Q, ANSARI N, *et al.* Reversible data hiding [J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2006, 16(3): 354-362.
- [6] CELIK M U, SHARMA G, TEKALP A M. Lossless watermarking for image authentication: a new framework and an implementation [J]. *IEEE Transactions on Image Processing*, 2006, 15(4): 1042-1049.
- [7] TIAN J. Reversible data embedding using a difference expansion [J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2003, 13(8): 890-896.
- [8] 张启龙, 温涛, 宋晓莹, 等. 基于自适应直方图修改的网格可逆信息隐藏[J]. 东北大学学报(自然科学版), 2020, 41(3): 316-320, 360.
- ZHANG Q L, WEN T, SONG X Y, *et al.* Reversible data hiding algorithm based on adaptive histogram modification for 3D mesh models [J]. *Journal of Northeastern University (Natural Science)*, 2020, 41(3): 316-320, 360. (in Chinese)
- [9] THODI D M, RODRÍGUEZ J J. Expansion embedding techniques for reversible watermarking [J]. *IEEE Transactions on Image Processing*, 2007, 16(3): 721-730.
- [10] CHANG C C, KIEU T D, CHOU Y C. Reversible data hiding scheme using two steganographic images [C]// *Proceedings of the TENCON 2007-2007 IEEE Region 10 Conference*. Taipei, China: IEEE, 2007: 1-4.
- [11] QIN C, CHANG C C, HSU T J. Reversible data hiding scheme based on exploiting modification direction with two steganographic images [J]. *Multimedia Tools and Applications*, 2015, 74(15): 5861-5872.
- [12] CHEN X F, HONG C Q. An efficient dual-image reversible data hiding scheme based on exploiting modification direction [J]. *Journal of Information Security and Applications*, 2021, 58: 102702.
- [13] 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.
- [14] 任克强, 肖璐瑶. 融合 CFT 和 LSB 的高容量可逆数据隐藏[J]. 液晶与显示, 2019, 34(4): 410-416.
- REN K Q, XIAO L Y. High-capacity reversible data hiding based on CFT and LSB [J]. *Chinese Journal of Liquid Crystals and Displays*, 2019, 34(4): 410-416. (in Chinese)
- [15] MEIKAP S, JANA B. Improved center-folding based directional pixel value ordering for reversible data hiding scheme [J]. *Multimedia Tools and Applications*, 2021, 80(4): 5617-5652.
- [16] LU T C, CHANG T C, SHEN J J. An effective maximum distortion controlling technology in the dual-image-based reversible data hiding scheme [J]. *IEEE Access*, 2020, 8: 90824-90837.
- [17] BHARDWAJ R, AGGARWAL A. Hiding clinical information in medical images: an encrypted dual-image reversible data hiding algorithm with base-3 numeral framework [J]. *Optik*, 2019, 181: 1099-1112.
- [18] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes [C]// *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*. Czech Republic: Springer, 1999: 223-238.

作者简介:



牛宇航(1996—),女,河南洛阳人,硕士研究生,2018年于河南农业大学获得学士学位,研究方向为可逆信息隐藏、图像处理等。E-mail: connerniu@scnu.edu.cn



申淑媛(1977—),女,湖南邵东人,博士,讲师,2015年于湖南大学获得博士学位,主要从事信息隐藏、神经网络水印等方面的研究。E-mail: ssyuan16@m.scnu.edu.cn