

结合 2D Logistic 映射与 2D-DCT 的数字图像隐藏技术^①



程东升¹, 隆广庆², 朱小玲²

¹(深圳信息职业技术学院 软件学院, 深圳 518172)

²(南宁师范大学 数学与统计学院, 南宁 530299)

通信作者: 程东升, E-mail: chengds@sziit.edu.cn

摘要: 为了应对日益增大的图像安全问题, 提出一种结合二维 Logistic 映射与二维离散余弦变换 (2D-DCT) 的数字图像隐藏算法。首先, 利用二维 Logistic 映射产生的混沌序列对秘密图像进行像素扩散与置乱, 从而达到对秘密图像的加密效果。接着, 分块对载体图像进行二维离散余弦变换, 然后把扩散与置乱后的图像信息分存在变换后每块的右下角。最后再进行二维离散余弦反变换 (2D-IDCT), 并得到隐密图像。实验结果也表明, 该算法安全可行且隐藏效果良好。

关键词: 二维 Logistic 映射; 二维离散余弦变换; 图像隐藏; 混沌序列; 图像置乱; 隐私保护

引用格式: 程东升, 隆广庆, 朱小玲. 结合 2D Logistic 映射与 2D-DCT 的数字图像隐藏技术. 计算机系统应用, 2022, 31(5):382–387. <http://www.c-s-a.org.cn/1003-3254/8495.html>

Digital Image Hiding Technology Combining 2D Logistic Mapping and 2D-DCT

CHENG Dong-Sheng¹, LONG Guang-Qing², ZHU Xiao-Ling²

¹(School of Software Engineering, Shenzhen Institute of Information Technology, Shenzhen 518172, China)

²(Department of Mathematics and Statistics, Nanning Normal University, Nanning 530299, China)

Abstract: To cope with increasingly serious problems related to image security, this study proposes a digital image hiding algorithm based on two-dimensional (2D) Logistic mapping and 2D discrete cosine transform (2D-DCT). Firstly, the chaotic sequence generated by the 2D Logistic mapping is used to diffuse and scramble pixels of the secret image so that the secret image can be encrypted. Then, 2D-DCT is performed on the host image in blocks, and the image information after diffusion and scrambling is stored in the lower right corner of each block after 2D-DCT. Finally, 2D inverse discrete cosine transform (2D-IDCT) is carried out to yield the stego image. Experimental results also show that the proposed algorithm is safe, feasible, and effective in image hiding.

Key words: 2D Logistic mapping; 2D discrete cosine transform (2D-DCT); image hiding; chaotic sequence; image scrambling; privacy protection

计算机和智能通信技术的快速发展, 使得信息的传播、共享也变得越来越便捷, 但同时对信息安全的问题提出了新挑战。而传统信息安全的保障手段——密码术能有效地保障信息安全, 但是进入移动互联

网、大数据时代, 传统的加密技术也暴露出其中的不足, 因为加密数据是异常数据, 容易成为数据分析挖掘的重点目标, 从而容易引起大量的攻击。因此大家又把目光投向一种古老的技术——信息隐写技术 (信息隐

^① 基金项目: 广东省自然科学基金 (2020A1515010566); 广西研究生教育创新计划 (YCSW2021278); 深圳市科技计划 (JCYJ20170306095959113); 广西省自然科学基金 (2017JJD110009, 2019AC04004)

收稿时间: 2021-07-20; 修改时间: 2021-08-18; 采用时间: 2021-09-29; csa 在线出版时间: 2022-04-11

藏技术)^[1-10], 信息隐藏技术其实自古就有, 例如在古代为了隐秘地传递机密信息, 会把传递信息的士兵剃光头后写上军事机密, 然后等他的头发长长后传递信息, 接收时再剃光那位士兵的头发就能看到机密信息. 而在计算机时代, 则对信息隐藏技术提出更高的要求, 信息隐藏不仅要让人肉眼无法分辨, 而且要实现对抗计算机视觉识别.

混沌系统具有对初始条件和控制参数敏感、伪随机和不可预测性等一系列特性, 这些特性与密码学的要求相一致. 因此, 混沌系统经常被用在图像加密中^[11-15], 利用混沌系统产生的混沌序列对图像进行扩散与混淆, 从而达到加密的效果. 而通过 2D-DCT, 可以把图像的主要能量集中在左上角, 这样只要把秘密图像的信息替换除左上角外的其它地方, 就既能减少失真度, 又达到良好的隐藏效果.

本文首先利用二维 Logistic 映射生成的混沌序列对秘密图像进行扩散, 从而改变秘密图像的像素值, 然后再利用混沌序列生成的置乱矩阵对扩散后的图像进行置乱. 接着分块对载体图像进行 2D-DCT, 并根据混沌系统产生的混沌序列自适应地把置乱后图像的信息替换每块变换 DCT 后的右下角, 然后对替换后的矩阵进行 2D-IDCT, 从而得到隐密图像. 我们的算法不论在扩散与置乱阶段还是替换隐藏阶段都受到混沌系统的控制, 从而所提算法对密钥非常敏感. 在实验中, 我们采用峰值信噪比 (PSNR)、均方根误差 (RMSE) 与结构相似性 (SSIM) 这 3 个指标, 从不同角度来衡量载体图像与隐密图像相似度, 能全面准确地反映本文算法所得隐密图像的失真度. 实验结果表明, 载体图像与隐密图像的 PSNR 达到 62.615, RMSE 为 0.188 7, 而 SSIM 等于 0.999 7, 这些都反映了算法良好的隐藏效果. 与现有的隐藏算法相比较, 我们算法的 PSNR 更大, 从而说明我们算法具有更优的隐藏性能.

1 二维 Logistic 映射与 2D-DCT

1.1 二维 Logistic 映射

经典的二维 Logistic 映射^[13]可表述为:

$$\begin{cases} x_{k+1} = x_k + \lambda(x_k - x_k^2 + y_k) \\ y_{k+1} = y_k + \lambda(y_k - y_k^2 + x_k) \end{cases} \quad (1)$$

当 $0.6 < \lambda \leq 0.686$ 时, 式 (1) 处于混沌状态. 关于参数 λ 的分岔图如图 1 所示.

1.2 二维离散余弦变换

2D-DCT 是与傅里叶变换相关的一种变换, 它类似于离散傅里叶变换, 但是只使用实数. 因此, 在对语音、图像信号变换中, 2D-DCT 变换被认为是一种准最佳变换. 通过 2D-DCT 可以将图像信号从时域映射到空间频率域, 使得图像在时域所表现出的能量发散形式变换为频域能量相对集中的形式, 以便与对图像信息进行各种处理. 2D-DCT 将图像的主要能量集中在左上角, 这样可以将秘密信息嵌入到中高频的右下方, 且能有效地减少载体图像的失真度.

2D-DCT 的公式为:

$$F(u, v) = c(u)c(v) \sum_{x,y=0}^{N-1} f(x, y) \cos \frac{\pi(2x+1)u}{2N} \cos \frac{\pi(2y+1)v}{2N} \quad (2)$$

其中, $u, v = 0, 1, \dots, N-1$, $c(u) = c(v) = \begin{cases} 1/\sqrt{2}, & u=0 \text{ 或 } v=0 \\ 1, & u, v = 1, 2, \dots, N-1 \end{cases}$

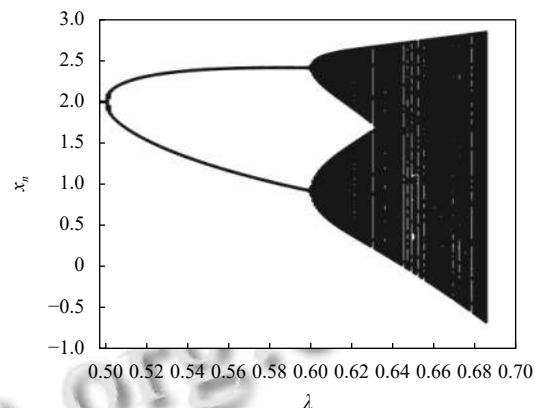


图 1 二维 Logistic 映射的分岔图

2D-IDCT 的公式为:

$$f(x, y) = \sum_{u,v=0}^{N-1} c(u)c(v)F(u, v) \cos \frac{\pi(2x+1)u}{2N} \cos \frac{\pi(2y+1)v}{2N} \quad (3)$$

其中, $x, y = 0, 1, \dots, N-1$, $c(u) = c(v) = \begin{cases} 1/\sqrt{2}, & u=0 \text{ 或 } v=0 \\ 1, & u, v = 1, 2, \dots, N-1 \end{cases}$

2 图像隐藏方案

图像隐藏方案包含两个步骤, 首先是对待隐藏图像的预处理, 其次是把预处理后的待隐藏图像隐藏到载体图像中. 我们先对待隐藏图像进行加密, 然后通过分块分存的方法把预处理后的图像隐藏在载体图像 S 中, 这样为图像提供了二重安全保障. 现记待隐藏图

像为 I , 其大小为 $N \times N$, 而载体图像的大小为 $4N \times 4N$, 并记为 S . 则关于图像隐藏方案的详细步骤如下:

步骤 1. 通过迭代二维 Logistic 映射(1), 生成两个长度为 $L = N^2$ 的混沌序列, 并分别记为 $X = \{x_1, x_2, \dots, x_L\}$ 与 $Y = \{y_1, y_2, \dots, y_L\}$.

步骤 2. 根据式(2)把混沌序列 X 与 Y 映射到 $[0, 255]$ 上的整数, 从而获得两个整数序列 W_1 和 W_2 .

$$\begin{cases} w_{1i} = \text{mod}(\text{round}(10^k x_i), 256) \\ w_{2i} = \text{mod}(\text{round}(10^k y_i), 256) \end{cases} \quad (4)$$

其中, $i = 1, 2, \dots, L$, $\text{round}(\cdot)$ 为取最近整数运算.

步骤 3. 分别从 $X = \{x_1, x_2, \dots, x_L\}$ 与 $Y = \{y_1, y_2, \dots, y_L\}$ 上各截取 N 个元素, 从而得到两个新序列与 $Z_1 = \{z_{11}, z_{12}, \dots, z_{1N}\}$ 与 $Z_2 = \{z_{21}, z_{22}, \dots, z_{2N}\}$. 然后根据 $Z_1 = \{z_{11}, z_{12}, \dots, z_{1N}\}$ 与 $Z_2 = \{z_{21}, z_{22}, \dots, z_{2N}\}$ 这两个序列中元素值的大小进行排序从而得到它们对应排序序列 $L_1 = \{l_{11}, l_{12}, \dots, l_{1N}\}$ 与 $L_2 = \{l_{21}, l_{22}, \dots, l_{2N}\}$, 其中 l_{1i}, l_{2i} 的值为 1 到 N 之间的整数.

步骤 4. 利用序列 $Z_1 = \{z_{11}, z_{12}, \dots, z_{1N}\}$ 与 $Z_2 = \{z_{21}, z_{22}, \dots, z_{2N}\}$, 根据式(5)可以得到值为 0 或 1 的序列 $K_1 = \{k_{11}, k_{12}, \dots, k_{1N}\}$ 与 $K_2 = \{k_{21}, k_{22}, \dots, k_{2N}\}$.

$$\begin{cases} k_{1i} = \text{mod}(\text{round}(10^k z_{1i}), 2) \\ k_{2i} = \text{mod}(\text{round}(10^k z_{2i}), 2) \end{cases} \quad (5)$$

步骤 5. 分别对序列 $Z_1 = \{z_{11}, z_{12}, \dots, z_{1N}\}$ 与 $Z_2 = \{z_{21}, z_{22}, \dots, z_{2N}\}$ 中的元素按从小到大的顺序进行排序, 从而得到排序后的序列 Z'_1 与 Z'_2 . 通过 Z_1 与 Z'_1 , Z_2 与 Z'_2 可以得到两个满足等式 $Z_1 = M_1 Z'_1$ 与 $Z_2 = M_2 Z'_2$ 的置乱矩阵 M_1 与 M_2 .

步骤 6. 重新排列整数序列 W_1 与 W_2 , 从而得到两个大小为 $N \times N$ 的矩阵 H_1 与 H_2 . 然后利用这两个矩阵对待隐藏图像 I 进行扩散, 其扩散的数学表示为:

$$M = ((I + H_1) \bmod 256) \oplus H_2 \quad (6)$$

其中, 符号 \oplus 表示异或操作.

步骤 7. 利用置乱矩阵 M_1 与 M_2 , 根据式(7)对扩散后得到矩阵 M 进行置乱并得到图像 F , 然后对图像 F 进行归一化处理, 即令 $E = F/255$, 这样我们得到加密图像 E .

$$F = M_1 \times M \times M_2 \quad (7)$$

步骤 8. 把载体图像分成 N^2 个 4×4 大小的块, 然后再对每一小块进行二维离散余弦变换. 接着根据序列 L_1, L_2, K_1 与 K_2 , 把余弦变换后每一小块中的右下角的其中一个元素用加密图像 E 中的元素进行替换, 从而得到隐含加密图像 E 的矩阵 D . 具体的 Matlab 程序如下:

```
D=blkproc(S, [4 4], 'dct2');
for i=1:N
    for j=1:N
        D(l1i*4-k1i, l2j*4-k2j)=E(i, j);
    end
end
```

步骤 9. 把矩阵 D 分成 N^2 个 4×4 大小的块, 然后再对每一小块进行二维离散余弦变换的逆变换(IDCT), 从而得到隐含秘密图像的隐密图像 S_I .

3 实验结果与分析

记二维 Logistic 映射的控制参数 λ 和初值 x_0, y_0 为预处理过程中的密钥, 为了方便起见记密钥为 (λ, x_0, y_0) . 取 $(\lambda, x_0, y_0) = (0.65, 1, 0.01)$, 并选择大小为 128×128 的 Circuit 图像作为秘密图像, 大小为 512×512 的 Lena 图像当作载体图像. 实验结果如图 2 所示, 其中图 2(a) 是 Circuit 图像, 图 2(b) 是图 2(a) 预处理后的加密图像, 图 2(c) 是 Lena 图像, 图 2(d) 是嵌入秘密图像的隐密图像, 图 2(e) 是利用正确密钥 $(0.65, 1, 0.01)$ 进行解密后恢复的图像, 图 2(f) 是利用错误密钥 $(0.65 + 10^{-14}, 1, 0.01)$ 进行解密后恢复的图像. 由图 2 结果可见, 所提算法对密钥非常敏感, 因为对于参数 λ, x_0, y_0 只要轻微的扰动则不能正确恢复.

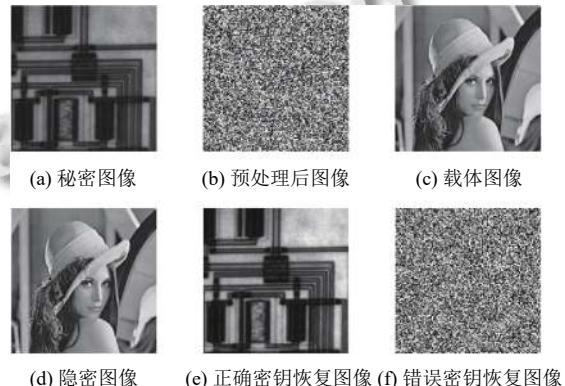


图 2 图像隐藏与恢复效果

众所周知, 图像的直方图反映了像素的统计特性. 因此, 若对于加密算法, 加密图像的直方图越趋于均衡则说明加密效果越好; 若对于图像隐藏技术, 嵌入秘密图像后的隐密图像与载体图像的直方图越接近则说明隐藏效果越佳. 图 3(a) 和图 3(b) 显示了秘密图像预处理前后图像的直方图, 其中, 图形底部的灰度条表示 Lena 图像的灰度级, 0 代表黑色, 255 代表白色, 而 0~255

之间的数值代表不同级别的灰度值。如图可直观看出预处理后的直方图呈现均匀化，因此窃取者无法通过密文的直方图获得秘密图像有效的统计信息。图3(c)

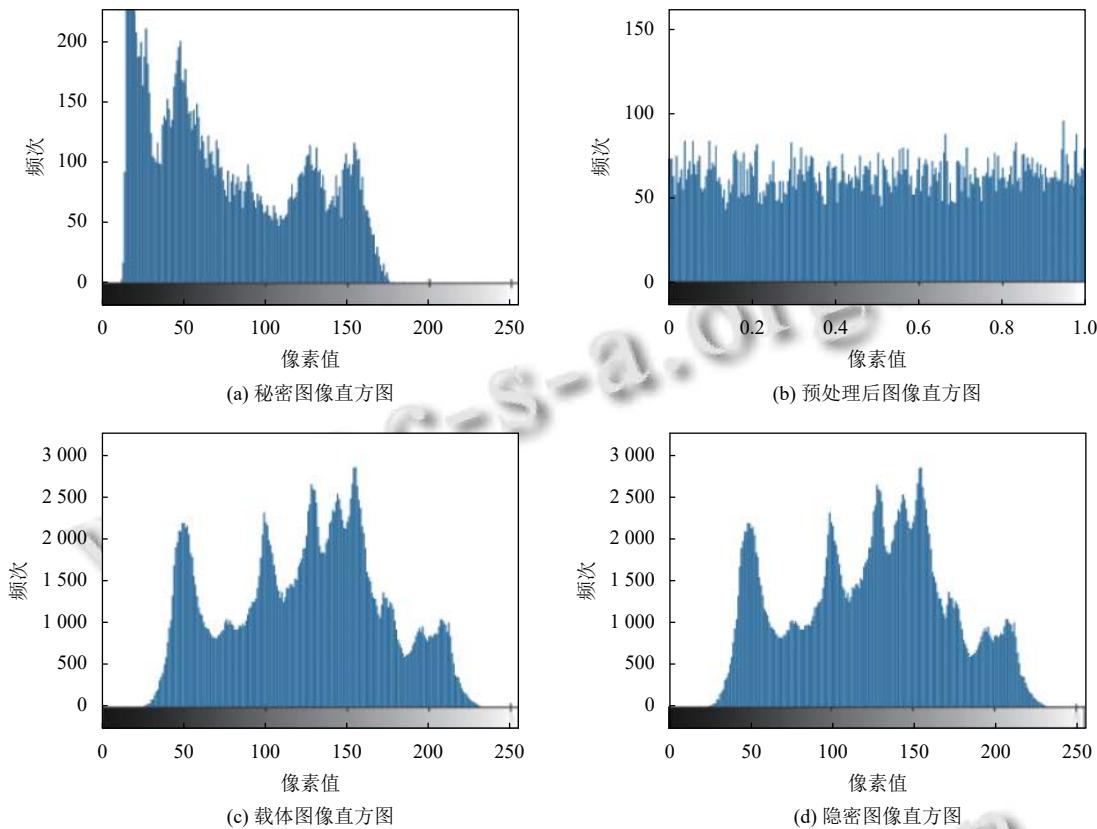


图3 直方图

为了检测算法抗剪切能力，对隐密图像做剪切攻击实验。图4(a)–图4(c) 分别剪切了隐密图像的 1/64, 1/16 与 1/4 的像素，而图4(d)–图4(f) 则是它们对应恢复的图像。由实验结果可看出所提算法能有效地把剪切攻击的影响控制在局部的范围，从而受到攻击后仍能有效地恢复大部分秘密图像的信息。

为了进一步对检验图像隐藏的效果的性能，从而引入峰值信噪比(PSNR)和均方根误差(RMSE)来衡量两幅图像之间的相似度^[10–12]。设两幅图像分别用 S 与 S_I 表示，则它们的 PSNR 与 RMSE 分别定义为：

$$PSNR = 10 \log 10 \left[\frac{M \times N \times 255^2}{\sum_{i=1}^M \sum_{j=1}^N [S(i,j) - S_I(i,j)]^2} \right] \quad (8)$$

和图3(d) 为载体图像和隐密图像的直方图，由图可看出载体图像与隐密图像的直方图肉眼观察几乎完全一致的，这说明所提算法的隐藏效果非常好。

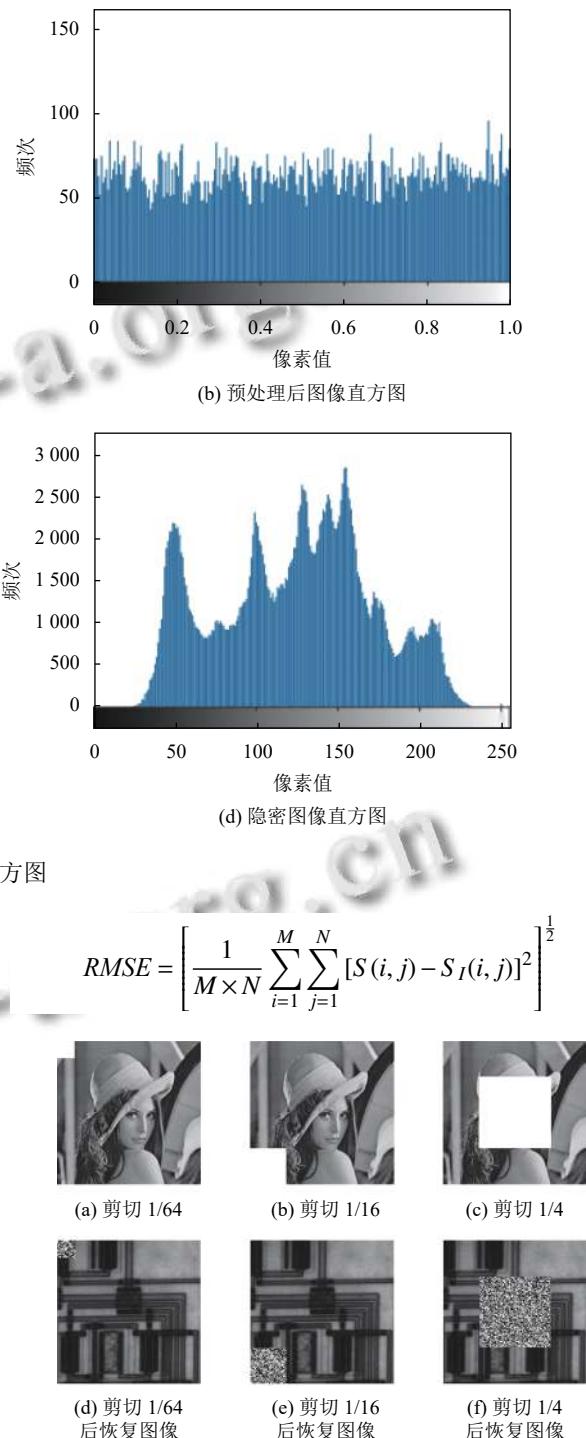


图4 剪切攻击及恢复的图像

由它们的定义，可以看出它们的 PSNR 值越大或 RMSE 值越小，说明两幅图像越接近，即两幅图像的相

似度度越高。

结构相似性(*SSIM*)，也是一种有效衡量两幅图像相似度的指标。两张图像的结构相似性可通过下式计算：

$$SSIM = \frac{(2\mu_S\mu_{S_I} + c_1)(2\sigma_S\sigma_{S_I} + c_2)(\sigma_{SS_I} + c_3)}{(\mu_S^2 + \mu_{S_I}^2 + c_1)(\sigma_S^2 + \sigma_{S_I}^2 + c_2)(\sigma_S\sigma_{S_I} + c_3)} \quad (10)$$

其中， μ_S 是 S 的平均值， μ_{S_I} 是 S_I 的平均值， σ_S 是 S_I 的方差， σ_{S_I} 是 S_I 的方差， σ_{SS_I} 是 S 与 S_I 的协方差。

$c_1 = (k_1 L)^2$, $c_2 = (k_2 L)^2$ 与 $c_1 = \frac{c_2}{2}$ 为常数，避免分母接近于0时造成的不稳定性，而 L 是图像像素值的动态范围， $k_1=0.01$, $k_2=0.03$. *SSIM*的值域为[0, 1]，值越接近1说明两幅图像相似度越高，反之越接近0说明两幅图像的差别越大。

利用*PSNR*, *RMSE*与*SSIM*定义的计算方法，通过计算可得出4组图像的*PSNR*, *RMSE*和*SSIM*的值并列于表1中。4组图像有秘密图像与预处理后图像的对比，载体图像和隐密图像的对比，秘密图像与正确密钥恢复图像的对比，以及错误密钥恢复图像与秘密图像的对比。

表1 效果分析

图像	PSNR	RMSE	SSIM
图2(a)与图2(b)	9.1613	88.8127	0.0068
图2(c)与图2(d)	62.6150	0.1887	0.9997
图2(a)与图2(e)	Inf	0	1
图2(a)与图2(f)	7.8986	102.7095	0.0038

通过表1的实验数据可以看出，秘密图像与预处理后图像的*PSNR*较小，*RMSE*较大，*SSIM*接近于0，这些都说明秘密图像与预处理后的图像差别很大，是完全不一样，从而验证了对秘密图像预处理的加密效果好；载体图像和隐密图像的*PSNR*大于30 (*PSNR*大于30时，人眼就无法分辨)，*RMSE*较小，而*SSIM*接近于1，3个指标结果都说明了这两幅图像的相似度很高，这证明了所提算法的图像隐藏效果很好；秘密图像与正确密钥恢复图像的*PSNR*趋于无穷大，*RMSE*的值等于0，而*SSIM*接近于1，都说明这两幅图像是完全一样，即秘密图像能完全恢复；错误密钥恢复图像与秘密图像的*PSNR*较小，*RMSE*较大，而*SSIM*接近于0，这表明错误密钥恢复的图像与秘密图像完全不一样，即所提算法对密钥非常敏感，密钥的微小扰动(10^{-14})则不能从恢复的图像中得到有效的秘密图像信息。

一般而言，隐藏算法的嵌入容量越大，则对应的载

体图像失真越明显，即对应的*PSNR*的值越小。因此，对于不同的隐藏算法若其中有一种算法的嵌入容量最大，而其对应的*PSNR*的值也最大，说明该隐藏算法的隐藏效果比其它算法好。从表2可以看出，我们所提算法、林纯等的算法^[16]、冯丹青等的算法^[17]与翁子盛的算法^[18]在采用相同大小的Lena作为载体图像，不同的嵌入容量的条件下，我们所提算法在嵌入容量比其它3种高的情况下，对应的*PSNR*的值却明显高于其他算法，这表明我们所提算法的隐藏效果更好。

表2 不同算法比较

指标	本文	文献[16]	文献[17]	文献[18]
<i>PSNR</i> (dB)	62.6150	54.185	54.44	47.77
嵌入容量 (bit)	139264	32768	32768	1592

4 结束语

本文提出了一种基于二维 Logistic 映射与 DCT 的分块图像隐藏算法。首先对秘密图像进行预处理，利用二维 Logistic 映射产生混沌序列对秘密图像进行扩散与置乱操作，从而达到对秘密图像第一重保护的目的。然后通过 DCT 把预处理后的加密图像的信息分存在载体图像中以达到信息隐藏的效果，从而对秘密图像起到第二重保护的作用。实验结果表明，本文所提算法具有良好的抗剪切效果，隐藏效果也非常好，并且可以实现秘密图像的无损复原。

参考文献

- 1 丁玮, 齐东旭. 数字图像变换及信息隐藏与伪装技术. 计算机学报, 1998, 21(9): 838–843. [doi: 10.3321/j.issn:0254-4164.1998.09.012]
- 2 王育民, 张彤, 黄继武, 等. 信息隐藏: 理论与技术. 北京: 清华大学出版社, 2006: 30–38.
- 3 Zhang XP. Reversible data hiding in encrypted image. IEEE Signal Processing Letters, 2011, 18(4): 255–258. [doi: 10.1109/LSP.2011.2114651]
- 4 Hong W, Chen TS, Wu HY. An improved reversible data hiding in encrypted images using side match. IEEE Signal Processing Letters, 2012, 19(4): 199–202. [doi: 10.1109/LSP.2012.2187334]
- 5 黄慧青. 基于 DCT 和混沌的图像隐藏技术. 计算机系统应用, 2013, 22(6): 105–107, 118. [doi: 10.3969/j.issn.1003-3254.2013.06.024]
- 6 黄慧青. 基于混沌系统的图像隐藏技术. 计算机系统应用,

- 2013, 22(11): 183–186. [doi: [10.3969/j.issn.1003-3254.2013.11.035](https://doi.org/10.3969/j.issn.1003-3254.2013.11.035)]
- 7 Ma KD, Zhang WM, Zhao XF, *et al.* Reversible data hiding in encrypted images by reserving room before encryption. *IEEE Transactions on Information Forensics and Security*, 2013, 8(3): 553–562. [doi: [10.1109/TIFS.2013.2248725](https://doi.org/10.1109/TIFS.2013.2248725)]
- 8 柳玲, 陈同孝, 曹晨, 等. 一种随机嵌入抗 SPAM 检测的可逆数据隐藏算法. *计算机应用研究*, 2013, 30(7): 2111–2114. [doi: [10.3969/j.issn.1001-3695.2013.07.048](https://doi.org/10.3969/j.issn.1001-3695.2013.07.048)]
- 9 Qian ZX, Zhang XP, Feng GR. Reversible data hiding in encrypted images based on progressive recovery. *IEEE Signal Processing Letters*, 2016, 23(11): 1672–1676. [doi: [10.1109/LSP.2016.2585580](https://doi.org/10.1109/LSP.2016.2585580)]
- 10 Jiang RQ, Zhou H, Zhang WM, *et al.* Reversible data hiding in encrypted three-dimensional mesh models. *IEEE Transactions on Multimedia*, 2018, 20(1): 55–67. [doi: [10.1109/TMM.2017.2723244](https://doi.org/10.1109/TMM.2017.2723244)]
- 11 叶瑞松, 黄慧青. 基于奇 Logistic 映射的混沌序列的图像加密算法. *仪器仪表学报*, 2008, 29(4): 109–111.
- 12 黄慧青, 许鸿儒. 基于三维 Arnold 混沌系统的图像加密算法. *嘉应学院学报*, 2012, 30(11): 23–26. [doi: [10.3969/j.issn.1006-642X.2012.11.006](https://doi.org/10.3969/j.issn.1006-642X.2012.11.006)]
- 13 Huang HQ, Yang SZ. Colour image encryption based on logistic mapping and double random-phase encoding. *IET Image Processing*, 2017, 11(4): 211–216. [doi: [10.1049/iet-ipr.2016.0552](https://doi.org/10.1049/iet-ipr.2016.0552)]
- 14 Huang HQ. Novel scheme for image encryption combining 2D logistic-sine-cosine map and double random-phase encoding. *IEEE Access*, 2019, 7: 177988–177996. [doi: [10.1109/ACCESS.2019.2958319](https://doi.org/10.1109/ACCESS.2019.2958319)]
- 15 Sahari ML, Boukemara I. A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption. *Nonlinear Dynamics*, 2018, 94(1): 723–744. [doi: [10.1007/s11071-018-4390-z](https://doi.org/10.1007/s11071-018-4390-z)]
- 16 林纯, 吴晓新, 郭晓丽, 等. DCT 域可逆图像隐藏技术研究. *微电子学与计算机*, 2014, 31(7): 61–64. [doi: [10.19304/j.cnki.issn1000-7180.2014.07.014](https://doi.org/10.19304/j.cnki.issn1000-7180.2014.07.014)]
- 17 冯丹青, 陈亮. 一种改进的奇异值奇偶区间量化图像隐藏算法. *科学技术与工程*, 2019, 19(26): 283–287. [doi: [10.3969/j.issn.1671-1815.2019.26.044](https://doi.org/10.3969/j.issn.1671-1815.2019.26.044)]
- 18 翁子盛. 一种基于格雷码的图像隐藏算法. *科学技术创新*, 2019, 2019(25): 87–88.