计 算 机 研 究 与 发 展
Journal of Computer Research and Development
https://crad.ict.ac.cn
62(4): 1050−1064, 2025

基于颜色通道关联性和熵编码的彩色密文图像可逆信息隐藏

高光勇[1,2] 季 驰[1,2] 夏志华[3]

[1](数字取证教育部工程研究中心(南京信息工程大学) 南京 210044)

[2](南京信息工程大学计算机学院、网络空间安全学院 南京 210044)

[3](暨南大学网络空间安全学院 广州 510632)

(gaoguangyong@163.com)

Reversible Data Hiding in Color Encrypted Images Based on Color Channels Correlation and Entropy Coding

Gao Guangyong[1,2], Ji Chi[1,2], and Xia Zhihua[3]

[1](*Engineering Research Center of Digital Forensics* (*Nanjing University of Information Science & Technology*), *Ministry of Education*, *Nanjing* 210044)

[2](*School of Computer Science*, *School of Cyber Science and Engineering*, *Nanjing University of Information Science & Technology*, *Nanjing* 210044)

[3](*College of Cyber Security*, *Jinan University*, *Guangzhou* 510632)

Abstract With the continuous development of cloud computing technology, the reversible data hiding in encrypted images (RDHEI) has received more and more attention. But most of the reversible data hiding in encrypted images are based on grey-scale, which have great limitations in application scenario compared with color images. Moreover, since the current reversible data hiding methods in the encrypted domain mainly focus on grey-scale images, and there are few optimizations for the characteristics of color images, it is hard to obtain better performance by applying these algorithms, so it is of high value to further investigate the reversible data hiding algorithm in color encrypted images. In this paper, we propose a high-performance RDHEI of color images algorithm for the first time based on color channels correlation and entropy encoding (RDHEI-CE) for cloud computing. First, the RGB channels of the color image are separated and the prediction errors are derived separately. Next, the embedding space is generated by adaptive entropy encoding and prediction errors histogram. The correlation between color channels is then used to further expand the embedding space and embed secret message on the encrypted image. Finally, the marked encrypted image must be scrambled in order to resist a ciphertext-only attack. Compared with most state-of-the-art RDHEI methods, experimental results show that the RDHEI-CE method provides a greater embedding rate and better security and broadens the application scene of reversible data hiding in the cloud.

Key words reversible data hiding; encrypted images; color images; color channels correlation; entropy encoding

摘 要 随着云计算领域数据安全和用户隐私的需求发展,密文图像可逆信息隐藏(reversible data hiding in encrypted images, RDHEI)技术已经越来越受到人们的关注,但目前大多数的密文图像可逆信息隐藏都是基于灰度图像,它们与彩色图像相比在应用场景上有很大局限性.此外,由于目前关于密文域的可逆信

收稿日期: 2023-10-31; **修回日期**: 2024-06-17

基金项目: 国家重点研发计划项目(2022YFB3103100); 国家自然科学基金项目(61662039, 62122032, U1936118)

This work was supported by the National Key Research and Development Program of China (2022YFB3103100) and the National Natural Science Foundation of China (61662039, 62122032, U1936118).

通信作者: 夏志华(xia_zhihua@163.com)

息隐藏方法主要集中于灰度图像，同时针对彩色图像的特性优化较少，往往无法对彩色载体图像实现更好的性能，所以进一步加强对基于彩色密文图像的可逆信息隐藏算法的研究具有很高的价值. 首次提出了一种可以用于云计算环境的基于颜色通道相关性和熵编码的高性能彩色密文图像可逆信息隐藏算法（RDHEI-CE）. 首先，原始彩色图像的RGB通道被分离并分别得出预测误差. 接下来，通过自适应熵编码和预测误差直方图生成嵌入空间. 之后通过颜色通道相关性进一步扩展嵌入空间，并将秘密信息嵌入加密图像中. 最后，对载密图像进行可逆置乱以抵御唯密文攻击. 与大多数最先进的可逆信息隐藏方法相比，实验表明RDHEI-CE算法提供了更高的嵌入率和更好的安全性，并且拓宽了可逆信息隐藏在云端的应用场景.

关键词 可逆信息隐藏；密文图像；彩色图像；颜色通道相关性；熵编码

中图法分类号 TP309

DOI: 10.7544/issn1000-1239.202330880 **CSTR:** 32373.14.issn1000-1239.202330880

随着向云端上传信息的普及，在保护隐私信息的同时，使得云端服务器能够轻松管理信息至关重要，特别是对于需要大量内存空间的图像或视频. 为了管理和验证图像的完整性，信息隐藏作为一种常见的解决策略，已经引起了研究界的广泛关注. 然而，大多数传统的信息隐藏方法在信息嵌入过程中会引入无法修复的载体失真[1-6]，这在包括医疗图像在内的某些图像的处理中是不被允许的. 为了解决上述问题，可逆信息隐藏（reversible data hiding, RDH），也被称作无损信息隐藏的新技术被提出，该技术可以同时提取嵌入的秘密信息和恢复载体介质. 目前的RDH算法主要基于以下3种方法，即差分扩展（differential extension, DE）[7-8]、预测误差扩展（prediction error expansion, PEE）[9-15]，以及直方图平移（histogram shifting, HS）[16-18]. 上述方法通常使用像素之间的局部空间相关性，如像素值的统计信息或预测误差等来嵌入秘密信息. 但它们只适合于未加密的图像，因为与加密图像的像素是不相关的.

随着互联网的普及和高速发展，用户对云端隐私保护的需求越来越大，密文域可逆信息隐藏（reversible data hiding in encrypted images, RDHEI）技术为密文图像处理提供了一种新的途径和可能性. RDHEI技术并非将秘密信息嵌入到明文图像中，而是加密图像中，应用一般的RDHEI算法可以在将图像发送到云端之前，数据隐藏者不知道原始明文图像或加密密钥的情况下将秘密信息嵌入到加密图像中，具有保护图像内容和可逆秘密信息的双重功能[19-26]. 在Puech等人[19]于2008年提出相关开创性工作以来，众多RDHEI方案被提出，目前主要分为3类：加密后产生嵌入空间（vacating room after encryption, VRAE）[20-21]、通过加密腾出嵌入空间（vacating room by encryption, VRBE）[22-23]以及加密前保留嵌入空间（reserve room before encryption, RRBE）[24-26]. 由于VRAE方法在加密过程破坏了原始明文图像像素的空间相关性，所以其很难获得令人满意的嵌入率（embedding rate, ER）. 对于VRBE方法，为了保护原始明文图像的机密性采用各种专门的加密方法进行加密，并在加密图像中保留部分空间相关性以便进行信息提取等后续处理. 然而，由于上述操作导致的空间相关性并没有得到充分的利用，因此VRBE方法中的嵌入率效果并不理想，可能导致嵌入的秘密信息不够多，影响后续的应用效果. 而在RRBE方法中，通过充分利用原始明文图像像素之间的相关性来保留嵌入空间，可以获得更高的嵌入率. RDHEI技术一般包括3个部分：内容拥有者、信息隐藏者和接收者[27-32]. 其中，内容拥有者根据图像加密密钥对原始图像进行加密，并将其上传到云端. 信息隐藏者只使用信息隐藏密钥将秘密信息嵌入到加密的图像中. 接收者可以使用信息隐藏密钥或图像加密密钥来提取秘密信息或恢复载体图像.

近年来，图像在网络上传播的频次和数量越来越大，其中彩色图像占据了绝大部分. 现有的基于彩色图像的RDH技术已经取得了一定程度的进展，其中，Xu等人[33]在2019年提出了一种基于3D预测误差扩展映射的可逆信息隐藏算法. Zhou等人[34]在2020年提出了一种使用递归编码构造来优化灰度不变性可逆信息隐藏算法，该算法使生成的彩色标记图像具有与主彩色图像相同的灰度. Chan等人[35]在2020年开发了一个基于矢量量化的可逆颜色灰度转换算法的信息嵌入框架. Yang等人[36]在2022年提出一种基于自适应分块的彩色图像RDH算法. 然而，RDH算法仍旧局限在明文域对彩色图像进行处理，虽然

将信息隐藏在明文域有隐藏通信过程和降低对图像的质量和视觉效果的影响的作用,但其已经难以适应如今云中存储多媒体信息的场景中对保护和管理相关信息的需求,需要对其进行加密处理,因为加密后的信息不再是可读的明文.

相比之下,RDHEI 方法更加适用,因为其能够在嵌入更多秘密信息的同时保证信息安全,相关领域的研究和发展也越来越引起人们的关注. 目前关于 RDHEI 算法的较新研究主要是基于灰度图像的 RDHEI 研究,并且已经取得了一定的研究进展,且能够获得相对令人满意的嵌入率效果[37-40],但如果上述灰度图像的算法没有针对彩色图像进行优化,即使其能够在灰度图像中呈现较好的实验结果,由于没有对彩色图像所具有的特性进行分析和运用,直接将上述算法套用在彩色图像上无法实现更好的性能.

同时,也有部分关于彩色图像的 RDHEI 算法被提出,例如张秋余等人[41]在 2020 年提出的算法. 但是通常都是对彩色图像的单一颜色通道进行分别处理(例如将原始彩色图像分离成 R, G, B 通道,并在分离的基础上进行加密处理),同时采用较为简单的方法进行数据的嵌入(例如置乱与直方图平移),并未特别对彩色图像的整体特性进行有针对性的优化和分析,实际上其本质仍旧是灰度图像 RDHEI 算法. 同时由于其仅是对目标图像进行简单的嵌入操作,故而对图像的处理能力远不如现今基于灰度图像的 RDHEI 算法,最终的嵌入效果相较而言并不理想.

此外,由于彩色图像中的 R, G, B 通道具有一定的相关性,针对性地基于彩色密文图像的可逆信息隐藏算法可以更好地利用这些相关性,提高信息隐藏的效果和可靠性,并更好地保证图像的视觉效果和质量,使得隐藏的信息更难被察觉. 因此,基于彩色密文图像的整体特征进行可逆信息隐藏算法研究具有广阔的研究和应用前景,对于保护和管理云中的多媒体信息也具有重要的实际意义. 在优化安全需要和提升嵌入率效果的前提下,本文提出了基于颜色通道相关性和熵编码的彩色密文图像可逆信息隐藏算法(RDHEI-CE),该算法能够有效提高云端彩色密文图像安全性和嵌入容量,具有广泛的应用前景和研究价值.

本文的主要贡献包括 3 个方面:

1)首次将彩色图像的整体特征引入彩色密文图像可逆信息隐藏算法. 通过彩色通道间的相关性进一步扩展嵌入空间,充分考虑通道间像素值的空间与纹理特征,实现了更高的嵌入容量.

2)提出了自适应熵编码,通过与彩色通道间的相关性结合,寻找到嵌入空间最大的最佳阈值,从而达到提升嵌入率的目标.

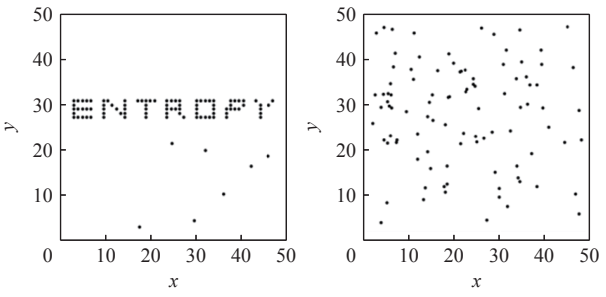
3)分析了目前已有 RDHEI 算法采用的流密码加密方法在唯密文攻击下的缺陷,提出了改善 RDHEI 算法在流密码攻击安全性的策略. 该策略简单易行,有力提高了载体图像和嵌入信息的安全性.

1 概念研究

由于本文所提出的 RDHEI-CE 算法通过改进的自适应熵编码配合彩色通道之间的相关性,以进一步扩展嵌入空间,实现更高的嵌入容量,所以本节将首先补充介绍熵编码的基本原理,之后将简单介绍关于彩色图像通道应用的分析,以简述如何考量灰度图像和彩色图像的区别并进行相对应的处理和应用. 关于 RDHEI-CE 算法在自适应熵编码和彩色通道相关性的应用等方面的改进详见第 2 节.

1.1 熵编码的基本原理

熵最初由德国物理学家克劳修斯在 1865 年提出. 熵的本质是一个系统的“内在无序程度”,例如图 1 就形象地说明了熵的意义:图 1(b)的熵比图 1(a)的熵大,因为图 1(b)中的内部更加无序.



(a) 较为有序的图 (b) 较为无序的图

Fig. 1 Meaning of entropy

图 1 熵的意义

信息熵是信息论中的一个基本概念,用于描述特定类型信息的出现概率. Shannon 在 20 世纪 40 年代从热力学中引入了这个概念,并给出了计算信息熵的数学表达式,称其为去除冗余后信息的平均数量. 当信息的出现概率越高时,信息熵越低,反之亦然. 在信息的传递过程中,信息的熵会增加,从而增加了系统的不确定性,一般来说,一个信息项出现的概率越高,就意味着它的传播范围越广,也就是引用的范围越大. 通过这种方式,我们可以衡量信息的价值,并对知识分配问题做出更多推论. 信息熵的计算

过程为：

$$Entropy(S)=-\sum_{i=1}^{n}P_i\mathrm{lb}P_i, \tag{1}$$

其中随机变量的输出用i来表示，P_i是输出的概率函数. 熵的值越大，表示随机变量的不确定性越高. 而当随机变量的输出完全确定时，熵的值为 0. 除了表示随机变量的不确定性程度，熵还可以用来衡量系统的有序化程度. 如果系统的状态是高度有序的，则熵的值将较低；反之，如果系统的状态是高度混乱的，则熵的值将较高.

1.2 关于彩色图像通道应用的分析

在 RDHEI 算法中，为了达到更高的嵌入率效果，需要在信息嵌入之前对目标载体图像进行相关特征的分析，以生成足够的嵌入空间. 对基于彩色图像的 RDHEI 算法来说，在进行特征分析之前，需要关注彩色图像有别于灰度图像的特性.

对于灰度图像来说，由于是单通道图像，其中每个像素只携带有关光强度的信息. 这些图像完全由灰色阴影组成，且有着相对应的灰度范围，通常此数值范围是 0~255. 与灰度图像不同的是，彩色图像由 R, G, B 通道组成，其中的每个像素均是由此 3 通道组成，每个通道代表一种颜色. 当分别处理彩色图像的 3 个通道时，可以输出 3 张相似但不同的灰度图像，这是因为彩色图像虽然和灰度图像一样由像素组成，但其像素实际上是一系列由颜色代码表示的原色组合而成. 在这种情况下，对应此图像的各个通道分别代表此颜色信息且与彩色图像大小相同的灰度矩阵，且仅由这些原色(R, G, B)之一构成. 所以对彩色图像的 3 个通道分别进行通道处理后，对应此图像每个通道的每个像素现在只需要处理其中一个通道的相关信息，所以它们是依照光强度通过灰色显示的. 所以，通道是彩色图像的灰度图像，它仅由构成彩色图像的 1 种原色组成. 借助上文所述彩色图像通道的特性，如果分别对彩色图像的 3 个通道进行处理，则针对此情况下的每个通道，其信息可以视作为对应 R, G, B 原色的光强度图像信息，可以视作一张灰度图像，因而可以较为简单地通过使用灰度图像的密文域可逆信息隐藏方法对彩色图像在此通道内的信息进行处理. 之后，再将分别得到的 3 个通道所含的相关信息进行统一整理，最终得到针对彩色图像密文域可逆信息隐藏的完整结果.

虽然上述方法可以将灰度密文图像可逆信息隐藏方法应用于彩色图像当中，也是目前出现的基于彩色图像的 RDHEI 算法使用的方法[41]，但这种算法仅是对目标图像的单一颜色通道进行分别处理，并在此基础上进行简单的加密与数据嵌入处理，本质上仍然是灰度密文图像 RDHEI 算法，而其对目标图像进行特征提取和信息嵌入的能力远不如现今基于灰度图像的 RDHEI 算法，最终实现的嵌入容量也较低. 同时，考虑到彩色图像中的 R, G, B 通道具有一定的相关性，若能在算法中进一步分析与运用彩色图像的整体特征，考虑彩色通道之间的相关性，有助于提高信息隐藏的效果和可靠性，最终实现更高的嵌入容量，同时更好地保证图像的视觉效果和质量.

2 本文算法

本文提出的基于颜色通道相关性和熵编码的彩色密文图像可逆信息隐藏算法 RDHEI-CE 的框架如图 2 所示. 该框架包括预测误差的生成、通过颜色通道相关性和熵编码生成嵌入空间、图像加密、信息隐藏、图像置乱、信息提取和图像还原共 7 个部分. 其中使用阴影标示并用独立方框示意的步骤为颜色通道关联性的分析与处理和自适应熵编码处理，是 RDHEI-CE 算法的创新点.

首先，内容拥有者将彩色图像的 R, G, B 通道分离，并分别得出 3 通道的预测误差. 接下来，通过自适应熵编码生成嵌入空间，从而达到高嵌入率. 然后，在此基础上，通过整体分析图像，引入颜色通道之间的相关性来扩展嵌入空间，从而进一步提高嵌入率和安全性.

信息隐藏者将秘密信息嵌入到加密载体图像上，完成可逆信息隐藏步骤. 然后，对载密图像进行置乱处理以抵抗唯密文攻击. 最终，置乱图像被传输给接收者，接收者可以根据手中持有密钥的不同来对加密后的载体图像或是秘密信息进行分别或是同时提取. 实验结果表明，RDHEI-CE 算法与最先进的 RDHEI 算法[37-40]相比也拥有出色的性能.

2.1 预测误差的生成

由于图像像素具有空间相关性，因此当前像素值可通过其相邻像素值的预测结果得出. 预测误差是数据压缩中广泛使用的技术，其主要目的是通过降低比特长度来代表原始像素. 此技术通常用于 RDHEI 方法中，利用空间冗余来产生嵌入的空间，从而实现更高效的数据压缩. 对于大小为 $M\times N\times 3$ 的原始彩色图像I_c，将I_c的 R, G, B 通道分开并把它们分别视为 3 个灰度图像I_r, I_g, I_b. 将每个通道的第 1 行第 1 列

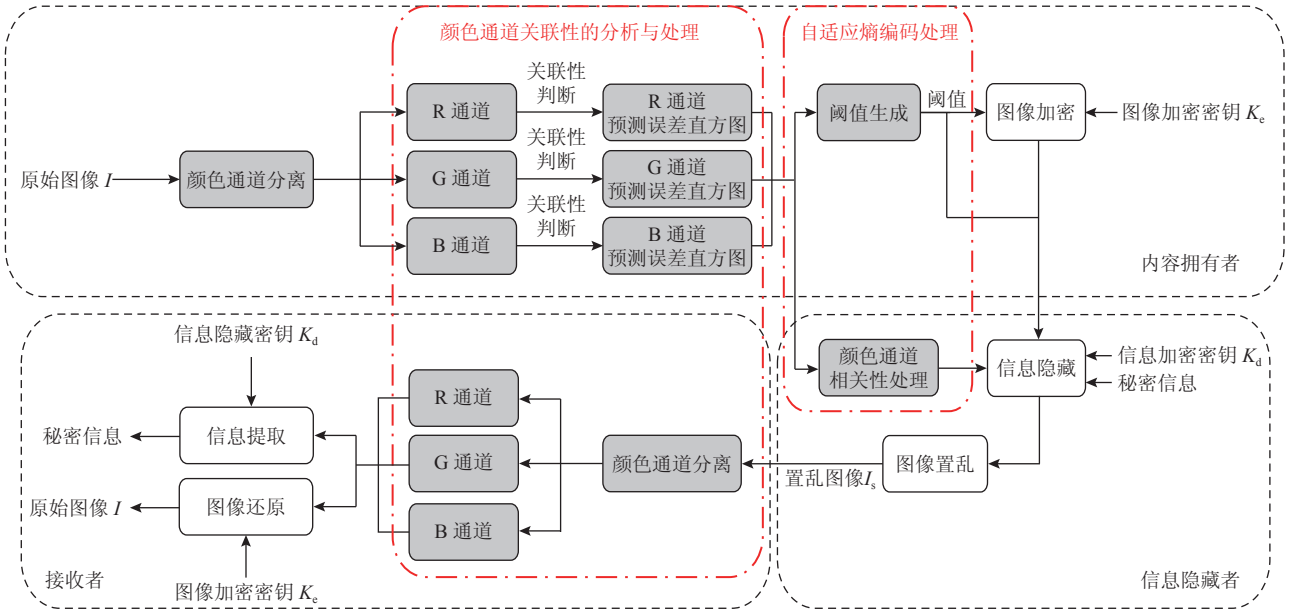


Fig. 2 RDHEI-CE algorithm framework

图 2 RDHEI-CE 算法框架

作为参考像素. 以 I_r 为例来计算预测误差, I_g 和 I_b 的预测误差以此类推. I_r 中每个像素 γ_r 的预测值 $p\gamma_r$ 可以由中值边缘检测器(median-edge detector, MED)预测得到. 从图 3 中可以看出, MED 预测器是基于当前像素 $\gamma_r(i,j)$ 周围的 3 个像素的像素值, 相应的预测值由式(2)计算得出.

$$p\gamma_r=\begin{cases}\max(b,c), & a<\min(b,c),\\ \min(b,c), & a\geqslant\max(b,c),\\ b+c-a, & \text{其他},\end{cases} \tag{2}$$

其中 $2\leqslant i\leqslant M$, $2\leqslant j\leqslant N$. 每个像素的预测误差 r_r 由式(3)计算得出:

$$\eta_r=p\gamma_r-\gamma_r. \tag{3}$$

之后再利用相同的方法得出 I_g, I_b 的预测误差并记录在预测误差矩阵中, 即获得 $\boldsymbol{e}_r$, $\boldsymbol{e}_g$, $\boldsymbol{e}_b$.

a	b
c	η_r

Fig. 3 Relationship between related pixels in MED predictor

图 3 MED 预测器中相关像素之间的关系

2.2 通过颜色通道相关性和熵编码生成嵌入空间

在获得 $\boldsymbol{e}_r$, $\boldsymbol{e}_g$, $\boldsymbol{e}_b$ 后, 可以得出 3 个颜色通道的预测误差直方图(prediction error histogram, PEH). 如图 4 所示, 对于明文图像, PEH 通常服从以 0 为中心的拉普拉斯分布. 对 PEH 图像, 横轴表示预测误差值 e 的绝对值, 纵轴表示对应的像素数量. 像素值的数量随着 e 的绝对值的增加而减少.

PEH 的像素被分成 2 类: 可嵌入像素(PE)和不可嵌入像素(PU). 熵代表系统内在的无序程度, 即熵值越小, 系统内部越有序. 为了将熵引入 RDHEI, RDHEI-CE 方法改进了熵的计算公式(见式(1)). T 是不同 PEH 的改进熵, 即不同的载体图像使用不同的 T 来获得最大嵌入容量. 因为根据熵的定义, 当熵最小的时候, 意味着系统内部是最稳定的. 如果系统是图像, 那就代表此时图像像素之间的关联性最强, 表明此时的预测误差最小, 保存预测误差所需空间越少, 那就代

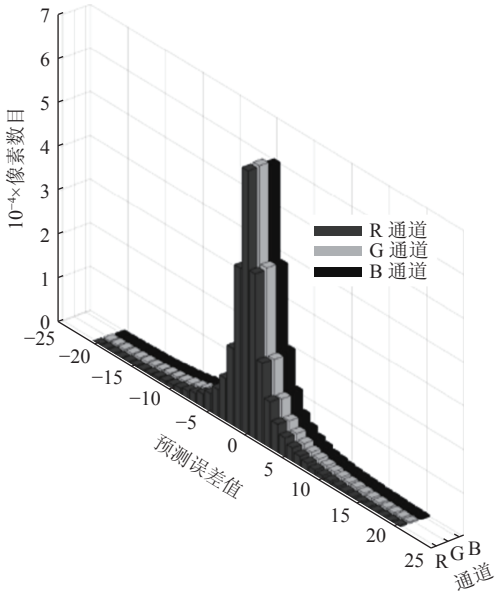


Fig. 4 PEH of image Lena

图 4 图像 Lena 的预测误差直方图

表此时纯嵌入量大. 图 4 显示了以彩色明文图像 Lena 为例的 PEH, 可见服从拉普拉斯分布.

因此, 用传统的熵编码方法将所有预测误差分为$(2k+1)$类, 其中$k\in\mathbb{N}$, 代表前$2k$类属于 PE, 第$(2k+1)$类属于 PU. 因此, T_k表示$(2k+1)$个分类的熵值. 由于 PU 像素不可嵌入, 它们的位置图被压缩并保留为D_{LM}用于图像恢复, $\boldsymbol{e}_{\mathrm{r}}$, $\boldsymbol{e}_{\mathrm{g}}$, $\boldsymbol{e}_{\mathrm{b}}$通过算术编码压缩并被记为$D_{\mathrm{CD}}$, 它们的长度分别记作$L_{\mathrm{LM}}$和$L_{\mathrm{CD}}$. T_k的计算过程如式(4)所示.

$$T_k=-\sum_{x=1}^{2k+1}P(x)\mathrm{lb}P(x)+\delta, \tag{4}$$

$$\delta=\frac{8+H(2k+1)+(2k+1)\times\alpha+8\times\beta}{M\times N},$$

其中$P(x)$表示第x类的像素数占总像素数的百分比. δ是熵计算公式的改进部分, 相当于 RDHEI 中的冗余项. $H(2k+1)$表示第$(2k+1)$类的像素数. α表示最大的$H(x)$被转换为一个α位的二进制序列, β表示L_{CD}被存储为一个β位的二进制序列. 表 1 是以 Lena 的 PEH 为例, 并说明如何将其分为$(2k+1)$类. 例如当$k=1$时, $2k+1=3$, 因此 PEH 被分为 3 类, 前 2 类分别是$e=0$和$e=-1$. 第 3 类也就是第$(2k+1)$类, 是$\{e=-255, e=-2\}\cup\{e=1, e=255\}$, 即剩下的没有被分类的预测误差被归为第$(2k+1)$类. 当$x$等于其他值时也以此类推.

Table 1 An Example for How to Classify with PEH of Image Lena

表 1 以图 Lena 的 PEH 举例说明如何进行分类

k	第 1 类	第 2 类	第 3 类	第 4 类	第 5 类	第 6 类	…	第$(2k+1)$类
1	$e=0$	$e=-1$			$\{e=-255, e=-2\}\cup\{e=1, e=255\}$			
2	$e=0$	$e=-1$	$e=1$	$e=-2$		$\{e=-255, e=-3\}\cup\{e=2, e=255\}$		
255	$e=0$	$e=-1$	$e=1$	$e=-2$	$e=2$	$e=-3$	…	$e=255$

最后, 对T_k进行逐一比较, 选择最小的T_k并记作T_O, 其目的是通过最小的熵T_O找到嵌入空间最大的最佳阈值$O\in[1, 255]$, 然后将信息嵌入符合$e\in[-O, O-1]$的像素中. 当T最小时, 意味着此时 PE 的数量最大, 也意味着像素之间的相关性最大. 所以此时, $e\in[-O, O-1]$的像素中嵌入的信息量是最大的. 算法 1 详细说明了如何通过熵编码来求取阈值O.

算法 1. 利用熵编码计算阈值.

输入: 预测误差直方图G_{PEH};

输出: 阈值O.

① for (i←1 to 255) do

② $His_group(i)\leftarrow G_{\mathrm{PEH}}(i)$;

/*计算各类预测误差的占比*/

③ $P_group(i)=His_group(i)$ / $sum(His_group)$;

④ end for

⑤ for (k←1 to 255) do

⑥ for (x←1 to 2k+1) do

/*参考熵值计算*/

⑦ $T(k)=T(k)-P_group(x)\times$lb ($P_group(x)$);

⑧ end for

/*自适应熵编码值计算*/

⑨ $T(k)=T(k)+\delta$;

⑩ end for

/* 求最小熵及其对应的 k */

⑪ $[k_{\min}, T_{\min}]\leftarrow find(\min(T(1:255)))$;

⑫ $O\leftarrow k_{\min}$.

首先分别计算出I_{r}, I_{g}, I_{b}的T_O值, 并记为T_{r}, T_{g}, T_{b}. 之后是通过关联 R, G, B 通道来扩大秘密信息的嵌入容量. 如图 5 所示, 以图 Lena 为例, 通过逐一比较$\boldsymbol{e}_{\mathrm{r}}$, $\boldsymbol{e}_{\mathrm{g}}$, $\boldsymbol{e}_{\mathrm{b}}$中各坐标的值, 相同位置以及相同数值的记为 1, 相同位置以及不同数值的记为 0, 最后生成的 2 张位置图分别记为$\boldsymbol{M}_{\mathrm{rg}}$, $\boldsymbol{M}_{\mathrm{bg}}$. 因为在 R 或 B 通道与 G 通道中相同位置处的值相等, 所以它们的原始值或预测误差只需被存储 1 次. 故而可以通过$\boldsymbol{M}_{\mathrm{rg}}$, $\boldsymbol{M}_{\mathrm{bg}}$缩短$D_{\mathrm{CD}}$和$D_{\mathrm{LM}}$. 也就意味着, 如果$e_{\mathrm{r}}(i, j)=e_{\mathrm{g}}(i, j)$, 那么只需存储$e_{\mathrm{g}}(i, j)$的值, 故而可以压缩$L_{\mathrm{CD}}$和$L_{\mathrm{LM}}$. 并且不论$e_{\mathrm{r}}(i, j)$是否属于$[-O, O-1]$, $\gamma_{\mathrm{r}}(i, j)$都可以嵌入信息, 这进一步提高了秘密信息的嵌入容量. 最后将$\boldsymbol{M}_{\mathrm{rg}}$, $\boldsymbol{M}_{\mathrm{bg}}$用压缩函数压缩以节约嵌入空间.

2.3 图像加密

为保护图像和信息不被泄露, 在进行图像标记之前需要对图像进行加密操作. 流密码是当今最流行和最方便的加密算法之一, 因为它只需要 1 个密钥来生成相应的伪随机序列, 并且计算复杂度低、开销小, 因此 RDHEI-CE 使用流密码对原始图像进行加密. I_{r}, I_{g}, I_{b}分别使用流密码进行加密, 下面以I_{r}为例. 首先, 用K_e生成一个大小为$M\times N$的伪随机矩阵$\boldsymbol{R}$, $\boldsymbol{R}$中的数值在 [0, 255] 之间. 然后依照式(5), 将像素值$\gamma_{\mathrm{r}}(i, j)$和相应的$R(i, j)$转换成 8b 二进制序列, 并分别记作$\gamma_{\mathrm{r}}^{b}(i, j)$, $R^{b}(i, j)$.

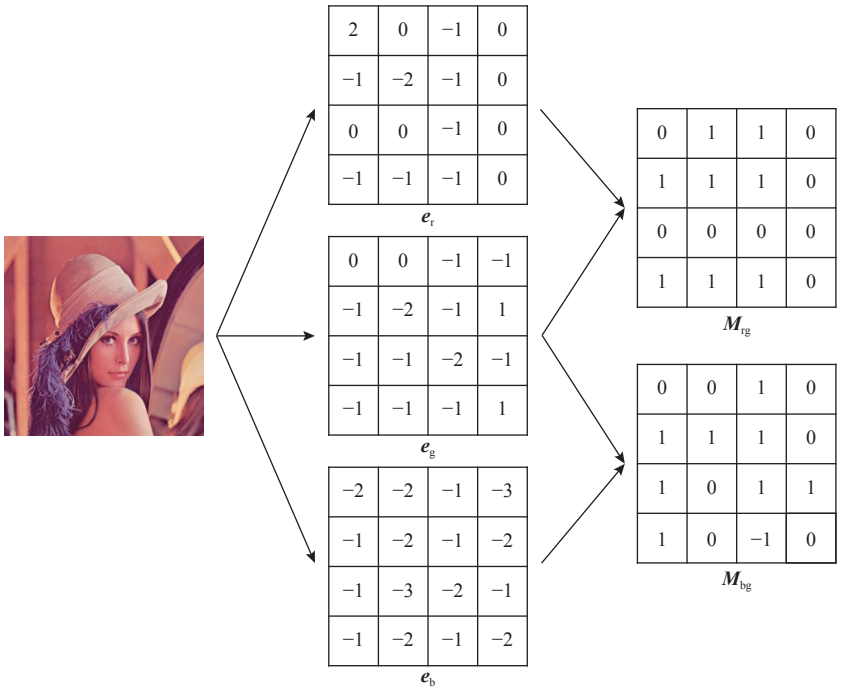


Fig. 5 $\boldsymbol{M}_{rg}$, $\boldsymbol{M}_{bg}$ generated by $\boldsymbol{e}_r$, $\boldsymbol{e}_g$, $\boldsymbol{e}_b$

图 5 通过$\boldsymbol{e}_r$，$\boldsymbol{e}_g$，$\boldsymbol{e}_b$生成$\boldsymbol{M}_{rg}$，$\boldsymbol{M}_{bg}$

$$\gamma_r^b(i,j)=\left\lfloor\frac{\gamma_r(i,j)\bmod 2^{9-b}}{2^{8-b}}\right\rfloor,b=1,2,\cdots,8, \tag{5}$$

其中“⌊⌋”表示向下取整. 然后，通过式(6)对图像的每个像素值进行加密.

$$E_r^b(i,j)=\gamma_r^b(i,j)\oplus R^b(i,j),b=1,2,\cdots,8, \tag{6}$$

其中“⊕”表示异或运算，$E_r^b(i,j)$是加密的 8b 二进制序列. 最后，加密的像素值$E_r(i,j)$由式(7)产生，以生成加密的图像I_{er}. 同样的方法可用于获得I_{eg}，I_{eb}. 组合上述 3 颜色通道图像生成彩色加密图像I_e.

$$E_r(i,j)=-\sum_{b=1}^{8}E_r^b(i,j)\times 2^{8-b},b=1,2,\cdots,8. \tag{7}$$

2.4 信息隐藏

在生成加密图像I_{er}，I_{eg}，I_{eb}后，为了能在图像加密后辅助提取嵌入的秘密信息，需要在秘密信息隐藏之前先行嵌入辅助信息. 缩短的D_{CD}，D_{LM}，以及压缩的$\boldsymbol{M}_{rg}$，$\boldsymbol{M}_{bg}$和它们的长度被记为辅助信息. 辅助信息和秘密信息将嵌入到 3 个通道中符合$e\in[-O,O-1]$的像素中. 首先，为方便图像恢复. 辅助信息通过式(8)被嵌入到 G 通道的低位平面. 一旦辅助信息被嵌入完毕，秘密信息通过式(6)被信息隐藏密钥K_d加密后，通过式(8)嵌入到剩余空间中：

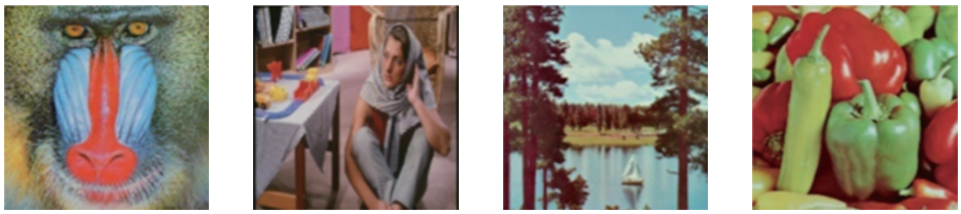
$$I_{mg}(i,j)=\sum_{b=1}^{8}W^b(i,j)\times 2^{b-1},b=1,2,\cdots,8, \tag{8}$$

其中I_{mg}代表被嵌入秘密信息后的加密图像，W^b代表需要嵌入的二进制信息. 在I_{eg}中信息嵌入完成后，其余信息被嵌入到I_{er}，I_{eb}中. 一旦辅助信息和秘密信息被嵌入完毕，就会得到载密图像I_{mr}，I_{mg}，I_{mb}，并通过组合I_{mr}，I_{mg}，I_{mb}得到彩色载密图像I_m.

2.5 图像置乱

虽然流密码是目前 RDH 领域常用的加密方法，但使用流密码加密存在许多风险，会影响嵌入秘密数据的安全性. Khelifi[42] 提出唯密文攻击(ciphertext-only attack, COA)算法可以用来破解只用流密码加密的秘密信息. 如果仅使用流密码加密秘密信息，由于利用像素间的冗余是这类图像嵌入方法的特点，内容所有者通常通过空间冗余来无损恢复图像，所以攻击者也可以利用空间冗余估算加密密钥. Khelifi[42] 使用相同的密钥对大量的图像进行流密码加密，然后根据 COA 算法，通过加密图像来获得估计密钥用于破解加密图像并恢复原始图像轮廓，从而揭示原始图像的大致内容. 图 6 是用 Khelifi[42] 提出的方法攻击只用流密码加密的彩色图像的对比图.

要提高现有 RDHEI 技术的安全性，可行的解决方案之一是在加密前对像素进行伪随机排列. RDHEI-CE 算法使用猫映射置乱算法. 如果在应用流密码之前，用密钥对像素进行伪随机洗码，系统就会变得更加安全，对 COA 攻击的防御能力也会更强，从而在不影响数据隐藏过程的情况下对抗 COA 攻击. 基于



(a) 使用正确密钥解密的图像



(b) 使用COA算法估计密钥解密的图像

Fig. 6 Experimental comparison diagram of color images attacked by COA

图 6 COA 攻击彩色图像的实验对比图

上述原因，RDHEI-CE 算法对彩色载密图像I_m进行猫映射置乱操作，猫映射置乱算法可以打乱图像中各彩色通道内各像素的比特位置以及所有像素之间的相对位置，攻击者无法通过空间冗余估计图像破解密钥，因此可以有效地防止 COA 攻击，是保证图像安全的重要部分. 置乱后的彩色图像I_m被记作I_s.

2.6 信息提取和图像重构

信息提取和图像重构阶段是数据加密与隐藏的逆向工程，描述了接收者如何恢复加密的彩色载密图像I_m并从中提取秘密信息. 首先，合法的接收者将置乱图像I_s还原，得到载密图像I_m，通过对I_m进行通道分离得到I_{mr}，I_{mg}，I_{mb}. 然后，由于在信息隐藏过程中，辅助信息被优先嵌入到I_{mg}的 LSB 平面，因此接收者可以从I_{mg}中提取辅助信息 D_{CD}，D_{LM}，$\boldsymbol{M}_{rg}$，$\boldsymbol{M}_{bg}$. 这些信息可以帮助接收者正确地提取秘密信息或恢复载体图像. 最后，对于接收者来说，其所拥有的密钥的不同会导致其能够从I_m中提取的信息不同.

如果接收者只拥有信息隐藏密钥K_d，那么接收者将只能通过其提取嵌入图像的秘密信息，而不能将载体图像恢复到原始状态. 在提取秘密信息的过程中，接收者通过从I_m中得到的辅助信息检索和解码其中加密的秘密信息并将其复原. 然而，由于接收者没有图像加密密钥K_e，故而其无法复原载体图像.

如果接收者只拥有图像加密密钥K_e，那么接收者将只能通过其恢复原始的载体图像信息，而不能从中提取到嵌入的秘密信息. 在恢复载体图像的过程中，接收者通过从I_m中得到的辅助信息，从对应的I_{mr}，I_{mg}，I_{mb}的高位平面中提取嵌入的加密图像特征信息，并最终利用提取的 D_{CD} 以及计算其对应的像素预测值来恢复 PE 的原始像素值，再利用 D_{LM} 找出 PU 的位置，从而覆盖计算出的 PE 的原始像素值，最终恢复完整的载体图像. 然而，由于接收者没有信息隐藏密钥K_d，故而其无法提取秘密信息.

只有当接收者同时拥有信息隐藏密钥K_d和图像加密密钥K_e时，才可以同时正确提取秘密信息且无损恢复原始图像. 上述过程使得接收者通过手中持有密钥的不同来分别或同时进行载体图像恢复和秘密信息提取操作，以确保秘密信息和载体图像的安全性和保密性.

3 实验结果与分析

为了验证本文所提出的 RDHEI-CE 算法的可行性和优越性，采用图 7 所示的大小为 512×512×3 的 5 张常规彩色图像进行实验对比和性能测试. 同时，利用 3 个公开的数据库，即 UCID 数据库[43]、Kodak 数据库[44] 以及 SIPI 数据库[45]，来测试不同方法的嵌入率. 其中作为衡量标准的嵌入率以 bpp 表示. 同时由于 RDHEI 算法追求更高的嵌入性能，为了定量说明算法的性能，使用嵌入率作为客观评判算法有效载荷的关键指标，此处提到的嵌入率是指不含辅助信息的纯内容的净嵌入率，能更好反映各算法的实际嵌入效果.

3.1 安全性分析与对比

原始图像I_C的特征信息可以通过流密码加密来隐藏，这种加密方式能够保护载密图像的机密性，但是如果没有置乱算法，仍然会存在唯密文攻击的风险. 然后通过置乱算法，图像I_S的特征信息被混淆，这



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

Fig. 7 Five public color test images

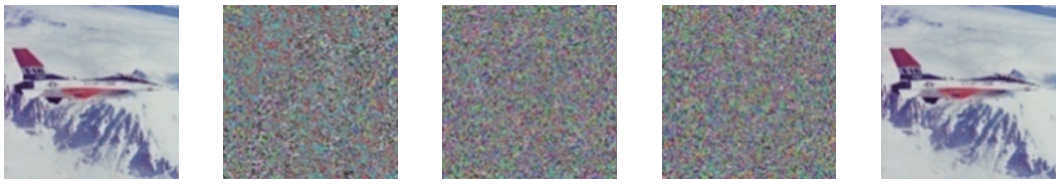
图 7 5 张公开的彩色测试图像

有效防止了唯密文攻击. 为了证明 RDHEI-CE 算法的安全性, 将通过其统计特性进行详细分析.

以图像 Airplane 为例, 图 8 显示了 RDHEI-CE 每个阶段的实验结果, 图 9 展示了图像 Airplane 的 4 个阶段所对应的直方图. 图 9(a)是包含原始图像重要特征信息的直方图. 图 9(b)是加密图像的直方图, 该图像是由流密码加密的, 由于此处像素的分布变得一致, 无法在图 9(b)中得到相关的统计特征信息. 从图 9(c)可以看出, 在嵌入秘密信息后, 由于通过彩色图像的 R, G, B 通道嵌入秘密信息, 很难产生明显的直方图特征, 加密图像中也并未产生明显的统计特征信息. 图 9(d)是置乱图像的直方图, 由于进行了猫映射操作, 图像的像素分布与图 9(c)相同, 攻击者同样无法从中获得有用的统计特征信息, 且增强了图像抵抗 COA 攻击的能力.

正如 Khelifi[42] 的方法中提到的, 仅使用流密码的加密图像仍存在许多风险, 并不完全保证安全. 为进一步说明 RDHEI-CE 算法的安全性, 假设嵌入的秘密信息是图像 Lena, 采用一个相同的密钥对 100 张图像进行加密并通过 Khelifi[42] 的方法生成一个估计密钥, 之后使用不同数量的加密图像得到的估计密钥用以实施解密操作, 最终生成不同精度的破解图像. 算法处理图像各阶段的实验结果如图 10 和图 11 所示. 图 10 所示的图像能够很容易用肉眼观察到破解图像的大致内容, 因为仅使用流密码加密的 RDHEI 方法没有采用任何抵抗 COA 攻击的预防措施. 相反, 从图 11 可以明显发现, 通过 RDHEI-CE 方法嵌入的秘密图像并不能通过估计密钥进行破解.

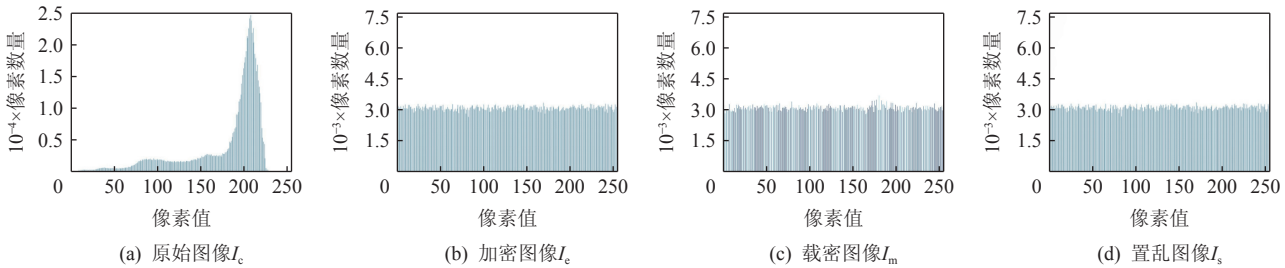
同时, 由于 RDHEI-CE 使用了猫映射过程进行图像置乱以加强图像的安全性, 此时会对图像使用可以设置为仅针对此图像的此次处理流程的密钥. 由于猫映射算法是存在置乱密钥的可逆置乱算法, 所以 RDHEI-CE 算法能够确保提取和重构阶段的可逆性. 同时, COA 攻击的实质是唯密文攻击, 攻击者在攻击时仅能获得经过算法处理和加密置乱后的图像, 并不能获取到对应的置乱密钥. 如果攻击者并未拥有置乱密钥, 则无法实现逆置乱过程, 进而无法解密并得到用于获得图像轮廓的估计密钥.



(a) 原始图像I_c (b) 加密图像I_e (c) 载密图像I_m (d) 置乱图像I_s (e) 重建图像I_c

Fig. 8 Results of five phases of images Airplane generated by RDHEI-CE algorithm

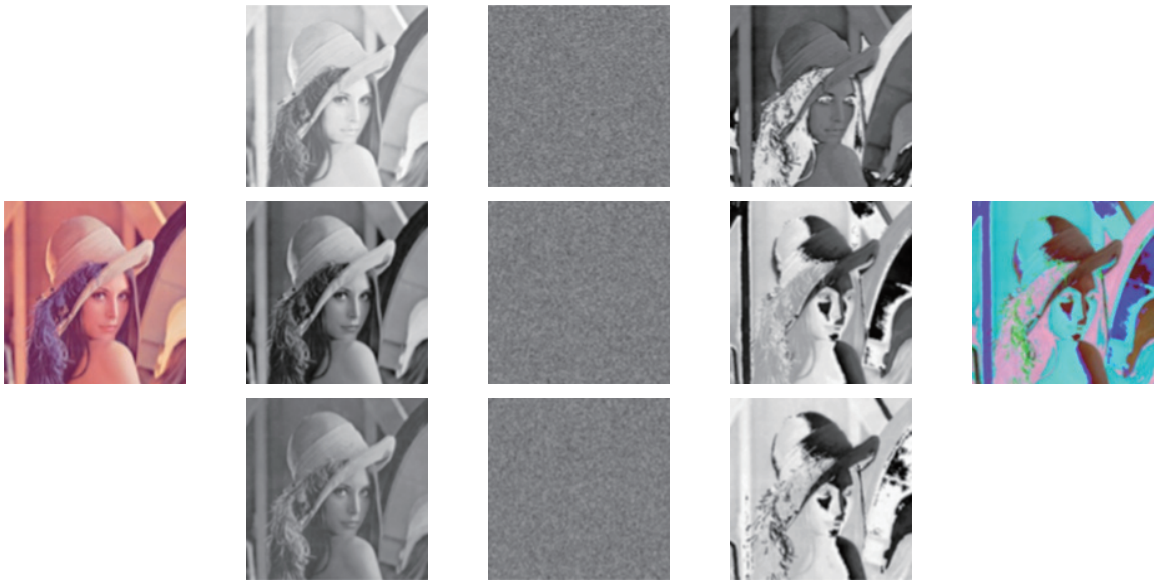
图 8 图像 Airplane 经 RDHEI-CE 算法生成的 5 个阶段的结果



(a) 原始图像I_c (b) 加密图像I_e (c) 载密图像I_m (d) 置乱图像I_s

Fig. 9 Histograms of four phases of image Airplane generated by RDHEI-CE algorithm

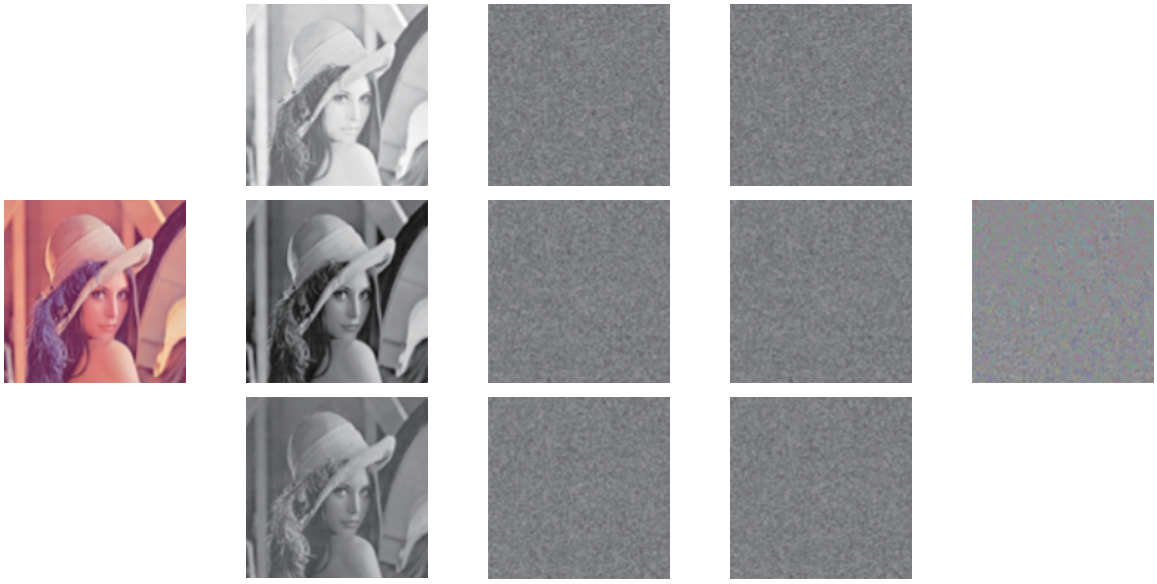
图 9 图像 Airplane 经 RDHEI-CE 算法生成的 4 个阶段的直方图



(a) 原始图像 (b) 分离的彩色通道 (c) 加密后的彩色通道 (d) 解密后的颜色通道 (e) 解密图像

Fig. 10 Experimental results of the conventional RDHEI algorithms are extracted by cracking program for image processing in each stage

图 10 通过破解程序提取常规 RDHEI 算法处理图像各阶段的实验结果



(a) 原始图像 (b) 分离的彩色通道 (c) 加密后的彩色通道 (d) 解密后的颜色通道 (e) 解密图像

Fig. 11 Experimental results of RDHEI-CE algorithm extracted by cracking program for image processing in each stage

图 11 通过破解程序提取 RDHEI-CE 算法处理图像各阶段的实验结果

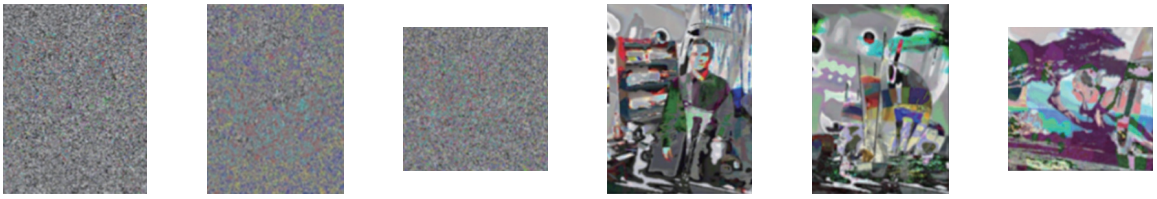
为了进一步说明 RDHEI-CE 方法在保护秘密信息安全方面的优越性，分别从 3 个数据库中选择了一些有代表性的图像进行对比实验，以随机验证 COA 攻击后泄露图像大致内容的风险，实验过程如图 12 所示，实验图像分别属于人物、物体和风景类型，所选图像分别是 UCID 中的 127 号、Kodak 中的 9 号和 SIPI 中的 6 号. 通过图 10~12 的实验结果可以直观得到，大部分测试图像在仅通过流密码处理后都出现了安全性问题，但通过置乱操作的 RDHEI-CE 方法在实际应用中确实可以很好地解决该问题，从而增强图像安全性.

3.2 性能分析与对比

为了在彩色图像中嵌入更多秘密信息，我们采用了改进的 MED 预测和熵编码计算出最适合嵌入秘密信息的阈值，此外还充分利用了彩色图像的整体特征，分析了彩色图像 R, G, B 通道之间的相关性，以进一步提高算法的嵌入能力. 表 2 和表 3 展示了使用 RDHEI-CE 方法对上述 5 张公开测试彩色图像和



(a) 原始图像



(b) 使用1张估计图像破解RDHEI-CE算法的测试结果 (c) 使用1张估计图像破解其他RDHEI算法的测试结果



(d) 使用60张估计图像破解RDHEI-CE算法的测试结果 (e) 使用60张估计图像破解其他RDHEI算法的测试结果



(f) 使用100张估计图像破解RDHEI-CE算法的测试结果 (g) 使用100张估计图像破解其他RDHEI算法的测试结果

Fig. 12 Results of RDHEI-CE and the conventional RDHEI methods are attacked by COA to test some representative images

图 12 对 RDHEI-CE 算法和常规 RDHEI 算法进行 COA 攻击测试一些代表性图像的结果

Table 2 Experimental Results of RDHEI-CE in Five Test Images

表 2 RDHEI-CE 在 5 张测试图像中的实验结果

测试图像	嵌入率/bpp	PSNR/dB	SSIM
Lena	4.730 7	+∞	1
Baboon	1.543 5	+∞	1
Airplane	3.631 7	+∞	1
Lake	2.335 4	+∞	1
Peppers	2.758 9	+∞	1

Table 3 Experimental Results of RDHEI-CE in Three Databases

表 3 RDHEI-CE 在 3 个数据库中的实验结果

测试数据库	嵌入率/bpp	PSNR/dB	SSIM
UCID	3.127 7（平均）	+∞	1
Kodak	3.224 3（平均）	+∞	1
SIPI	3.405 7（平均）	+∞	1

3 个数据库进行实验的结果.

从表 2 和表 3 可以看出，RDHEI-CE 方法实现了相对更高的嵌入率，尤其是在 SIPI 数据库中的平均嵌入率达到了 3.405 7 bpp. 此外，通过 RDHEI-CE 算法进行图像恢复操作后得到的图像的 PSNR 值为+∞，SSIM 值为 1，说明 RDHEI-CE 方法在进行图像恢复操作后得到的图像与原始明文图像相同，可以无损恢复原始图像，进一步证明了 RDHEI-CE 方法在彩色密文图像可逆信息隐藏方面的优异性能.

由于目前已有的彩色图像 RDHEI 算法[41]是将彩色图像的单一通道进行分别处理，且在嵌入算法上较为基础，相比目前最先进的灰度图像 RDHEI 方案而言嵌入效果[37-40]并不理想. 例如以彩色图像 Lena 为实验对象，文献 [41] 中所展示算法的嵌入率最高仅约为 1.2 bpp，而将文献 [37−40] 中所展示的方案运用于彩色图像，实验结果为 2.686 4~3.820 2 bpp，领先文献 [41] 中所展示的方案. 所以为了更好地展示 RDHEI-CE 方法的优越性，本文选用了目前最先进的灰度图像 RDHEI 方案[37-40]进行实验数据的比较. 在图 13 和图 14 中给出了 RDHEI-CE 方案与 4 种方案在 5 张公

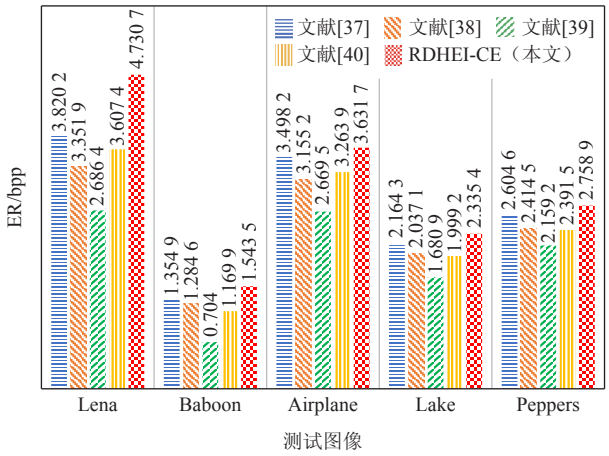


Fig. 13 Comparison of ER on five public color images

图 13 在 5 张公开彩色图像的嵌入率比较

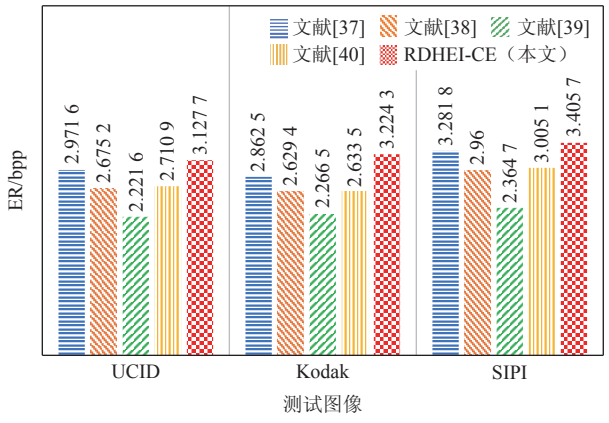


Fig. 14 Comparison of ER on three public color databases

图 14 在 3 个公开彩色数据库中的嵌入率比较

开测试彩色图像和 3 个数据库进行实验的结果.

上述灰度密文图像可逆信息隐藏算法通过 2.2 节所述的彩色图像通道应用方法进行分析, 类似文献 [41] 中算法所展示的步骤, 对彩色目标图像的 3 个颜色通道分别应用灰度图像可逆信息隐藏算法的操作, 得到图像各通道中像素嵌入秘密信息的嵌入率, 之后计算各通道嵌入率的平均值, 作为衡量此灰度密文图像算法应用于彩色密文图像可逆信息隐藏的结果. 可以看出, 与上述灰度图像方法相比, RDHEI-CE 方法的实验结果仍旧在所有测试图像上都表现出色, 并且在 UCID 数据库和 Kodak 数据库中, 文献 [37−40] 提出的方法的平均嵌入率不超过 3 bpp. 虽然文献 [37] 方法的嵌入率可以达到最大的值(2.971 6 bpp), 但是该方法仍未充分利用所有可用的嵌入空间. 这是因为在分离彩色图像的颜色通道后, RDHEI-CE 算法通过自适应熵编码技术关联颜色通道相关性, 对嵌入空间进行了扩展, 从而能够更高效地进行数据嵌入. 根据这些结果, 可以得出 RDHEI-CE 方法的嵌入率达到了最佳性能, 这也进一步验证了该方法的可靠性和有效性. 此外, 5 张彩色测试图像和 3 个数据库中嵌入容量和增量的数据在表 4 中列出, 5 张彩色图像中的最高增量为 0.910 5 bpp, 3 个数据库中的最高增量为 0.368 1 bpp.

为了凸显 RDHEI-CE 方法的优越性, 表 5 展示了 RDHEI-CE 算法的计算复杂度和空间复杂度上与现有的 RDHEI 方法的比较. 由于时间复杂度只能作为相应性能的上界估计, 实际的实现可能受到常数等因素的影响, 表 6 展示了文献 [37−40] 提出的方法与 RDHEI-CE 算法实际执行时间的比较. 此处展示的实际执行时间会由于测试设备的性能不同存在一定程度的差异, 但是依旧可以作为算法在相应性能上的参考. 最终的实验结果仍表明, 即使考虑 RDHEI-CE 算法需要进行彩色图像相关性的处理, 导致相比灰度密文图像算法需要耗费更多时间的情形下, 仍旧

Table 4 Net Payloads and Increments in Five Public Color Images and Three Databases

表 4 在 5 张公开彩色图像和 3 个数据库中的净有效载荷及增量

测试图像及数据库	平均净有效载荷										增量	
	文献 [37]		文献 [38]		文献 [39]		文献 [40]		RDHEI-CE（本文）			
	单载荷/bpp	总载荷/b	单载荷/bpp	总载荷/b	单载荷/bpp	总载荷/b	单载荷/bpp	总载荷/b	单载荷/bpp	总载荷/b	单载荷/bpp	总载荷/b
Lena	**3.820 2**	**3 004 328**	3.351 9	2 636 040	2.686 4	2 112 672	3.607 4	2 836 947	**4.730 7**	**3 720 373**	0.910 5	716 046
Baboon	**1.354 9**	**1 065 537**	1.284 6	1 010 250	0.704 0	553 647	1.169 9	920 046	**1.543 5**	**1 213 857**	0.188 6	148 321
Airplane	**3.498 2**	**2 751 096**	3.155 2	2 481 351	2.669 5	2 099 379	3.263 9	2 566 836	**3.631 7**	**2 856 084**	0.133 5	104 989
Lake	**2.164 3**	**1 702 075**	2.037 1	1 602 042	1.680 9	1 321 914	1.999 2	1 572 234	**2.335 4**	**1 836 633**	0.171 1	134 559
Peppers	**2.604 6**	**2 048 340**	2.414 5	1 898 841	2.159 2	1 698 063	2.391 5	1 880 751	**2.758 9**	**2 169 867**	0.154 3	121 346
UCID	**2.971 6**	**2 336 961**	2.675 2	2 103 864	2.221 6	1 747 137	2.710 9	2 131 938	**3.127 7**	**2 459 724**	0.156 1	122 762
Kodak	**2.862 5**	**2 251 162**	2.629 4	2 067 844	2.266 5	1 782 448	2.633 5	2 071 069	**3.224 3**	**2 535 693**	0.368 1	289 486
SIPI	**3.281 8**	**2 580 913**	2.960 0	2 327 839	2.364 7	1 859 676	3.005 1	2 363 307	**3.405 7**	**2 678 351**	0.123 9	97 439

注：黑体数值表示最优值.

得到相近的实际计算时间,同时实现了更高的嵌入率.综合上述理论中对于计算复杂度和空间复杂度的对比以及实验中实际处理时间的对比,表明RDHEI-CE方案能够保持高嵌入率和安全性的同时保证较低的复杂度.

Table 5 Data of Computational Complexity and Space Complexity

表 5 计算复杂度和空间复杂度的数据

方法	计算复杂度	空间复杂度
文献 [37]	$O(n^2)$	$O(n^2)$
文献 [38]	$O(n^3)$	$O(n^2)$
文献 [39]	$O(n^2)$	$O(n^2)$
文献 [40]	$O(n^2)$	$O(n^2)$
RDHEI-CE (本文)	$O(n^2)$	$O(n^2)$

Table 6 Comparison of Actual Implementation Time

表 6 实际执行时间的比较 s

测试图像	文献 [37]	文献 [38]	文献 [39]	文献 [40]	RDHEI-CE (本文)
Lena	18.230 8	45.778 7	16.498 3	20.054 2	16.102 0
Baboon	19.921 8	38.691 5	16.130 3	19.953 5	18.806 4
Airplane	18.314 8	46.329 5	17.319 6	18.983 1	15.684 3
Lake	18.662 5	39.515 2	15.977 9	19.832 0	19.183 5
Peppers	19.021 8	40.224 2	16.465 5	19.913 7	18.238 7

4 总 结

本文提出了基于颜色通道相关性和熵编码的彩色密文图像可逆信息隐藏方法(RDHEI-CE),首次将彩色图像的整体特征引入彩色密文图像可逆信息隐藏算法,充分利用了彩色图像中颜色通道间的关联性和单通道中像素间的相关性,以提高彩色密文图像的信息嵌入容量.通过熵编码技术和置乱算法,RDHEI-CE能够在保证信息嵌入容量的同时保证信息的安全性.实验结果表明,RDHEI-CE的嵌入容量比其他方法更高,并且其充分保障了彩色载密图像的安全性能.彩色密文图像可逆信息隐藏的应用场景不仅可以应用于云端,还可以在各种领域中发挥作用,如医疗影像处理、数字水印、视频加密等.因此,RDHEI-CE的提出为可逆信息隐藏技术的研究和应用提供了新的思路.尽管本文通过颜色通道的相关性和自适应熵编码充分利用了彩色图像中不同颜色通道中的像素相关性,然而基于较为传统的方法进行彩色图像整体特征的应用探索毕竟效果有限.因此在未来的工作中,还可以通过深度神经网络学习R, G, B通道在彩色图像间的关联特征,进一步提高算法性能.

作者贡献声明: 高光勇提出了算法思路和实验方案;季驰负责完成实验并撰写论文;夏志华提出指导意见并修改论文.

参 考 文 献

[1] Tang Zhenjun, Zhang Xianquan, Li Xianxian, et al. Robust image hashing with ring partition and invariant vector distance[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(1): 200−214

[2] Qin Chuan, Ji Ping, Zhang Xinpeng, et al. Fragile image watermarking with pixel-wise recovery based on overlapping embedding strategy[J]. Signal Processing, 2017, 138: 280−293

[3] Tao Jinyuan, Li Sheng, Zhang Xinpeng, et al. Towards robust image steganography[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2019, 29(2): 594−600

[4] Li Sheng, Zhang Xinpeng. Toward construction-based data hiding: From secrets to fingerprint images[J]. IEEE Transactions on Image Processing, 2019, 28(3): 1482−1497

[5] Tang Zhenjun, Chen Lv, Zhang Xianquan, et al. Robust image hashing with tensor decomposition[J]. IEEE Transactions on Knowledge and Data Engineering, 2019, 31(3): 549−560

[6] Celik M U, Sharma G, Tekalp A M, et al. Lossless generalized-LSB data embedding[J]. IEEE Transactions on Image Processing, 2005, 14(2): 253−266

[7] Tian Jun. Reversible data embedding using a difference expansion[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(8): 890−896

[8] Alattar A M. Reversible watermark using the difference expansion of a generalized integer transform[J]. IEEE Transactions on Image Processing, 2004, 13(8): 1147−1156

[9] Ou Bo, Li Xiaolong, Zhao Yao, et al. Pairwise prediction-error expansion for efficient reversible data hiding[J]. IEEE Transaction Image Processing, 2013, 22(12): 5010−5021

[10] Chen Xianyi, Sun Xingming, Sun Huiyu, et al. Reversible watermarking method based on asymmetric-histogram shifting of prediction errors[J]. Journal of Systems and Software, 2013, 86(10): 2620−2626

[11] Ou Bo, Li Xiaolong, Zhao Yao, et al. Reversible data hiding using invariant pixel-value-ordering and prediction-error expansion[J]. Signal Processing: Image Communication, 2014, 29(7): 760−772

[12] Peng Fei, Li Xiaolong, Yang Bin. Improved PVO-based reversible data hiding[J]. Digital Signal Processing, 2014, 25: 255−265

[13] Wang Dewang, Zhang Xianquan, Yu Chunqiang, et al. Reversible data hiding by using adaptive pixel value prediction and adaptive embedding bin selection[J]. IEEE Signal Processing Letters, 2019, 26(11): 1713−1717

[14] Qin Jianqiang, Huang Fangjun. Reversible data hiding based on

multiple two-dimensional histograms modification[J]. IEEE Signal Processing Letters, 2019, 26(6): 843−847

[15] Qi Wenfa, Li Xiaolong, Zhang Tong, et al. Optimal reversible data hiding scheme based on multiple histograms modification[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2020, 30(8): 2300−2312

[16] Ni Zhicheng, Shi Yunqing, Ansari N, et al. Reversible data hiding[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2006, 16(3): 354−362

[17] Qin Chuan, Chang Chin-Chen, Huang Ying-Hsuan, et al. An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2013, 23(7): 1109−1118

[18] Jia Yujie, Yin Zhaoxia, Zhang Xinpeng, et al. Reversible data hiding based on reducing invalid shifting of pixels in histogram shifting[J]. Signal Processing, 2019, 163: 238−246

[19] Puech W, Chaumont M, Strauss O. A reversible data hiding method for encrypted images[G]//SPIE 6819: Proc of the Int Society for Optical Engineering (SPIE). Bellingham, WA: SPIE, 2008: 11−19

[20] Qian Zhenxing, Zhang Xinpeng. Reversible data hiding in encrypted images with distributed source encoding[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2016, 26(4): 636−646

[21] Chen Kaimeng, Guan Qingxiao, Zhang Weiming, et al. Reversible data hiding in encrypted images based on binary symmetric channel model and polar code[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(6): 4519−4535

[22] Huang Delu, Wang Jianjun. High-capacity reversible data hiding in encrypted image based on specific encryption process[J]. Signal Processing: Image Communication, 2020, 80: 115632

[23] Qiu Yingqiang, Ying Qichao, Yang Yuyan, et al. High-capacity framework for reversible data hiding in encrypted image using pixel prediction and entropy encoding[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 32(9): 5874−5887

[24] She Xiaomeng, Du Yang, Ma Wenjing, et al. Reversible data hiding in encrypted images based on pixel prediction and block labeling[J]. Journal of Computer Research and Development, 2022, 59(9): 2089−2100 (in Chinese)
(佘晓萌, 杜洋, 马文静, 等. 基于像素预测和块标记的图像密文可逆信息隐藏[J]. 计算机研究与发展, 2022, 59(9): 2089−2100)

[25] Yi Shuang, Zhou Yicong. Separable and reversible data hiding in encrypted images using parametric binary tree labeling[J]. IEEE Transactions on Multimedia, 2019, 21(1): 51−64

[26] Puteaux P, Puech W. EPE-based huge-capacity reversible data hiding in encrypted images[C/OL]//Proc of 2018 IEEE Int Workshop on Information Forensics and Security. Piscataway, NJ: IEEE, 2019[2023-05-19]. https://ieeexplore.ieee.org/document/8630788/

[27] Yi Puyang, Yin Zhaoxia, Qian Zhenxing. Reversible data hiding in encrypted images with two-MSB prediction[C/OL]//Proc of 2018 IEEE Int Workshop on Information Forensics and Security. Piscataway, NJ: IEEE, 2019[2023-05-19]. https://ieeexplore.ieee.org/document/8630785/

[28] Chen Kaimeng, Chang Chin-Chen. High-capacity reversible data hiding in encrypted images based on extended run-length coding and block-based MSB plane rearrangement[J]. Journal of Visual Communication and Image Representation, 2019, 58: 334−344

[29] Yin Zhaoxia, Xiang Youzhi, Zhang Xinpeng. Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding[J]. IEEE Transactions on Multimedia, 2020, 22(4): 874−884

[30] Qian Zhenxing, Zhang Xinpeng, Wang Shuozhong. Reversible data hiding in encrypted JPEG bitstream[J]. IEEE Transactions on Multimedia, 2014, 16(5): 1486−1491

[31] Zhou Jiantao, Sun Weiwei, Dong Li, et al. Secure reversible image data hiding over encrypted domain via key modulation[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2016, 26(3): 441−452

[32] Liao Xin, Li Kaide, Yin Jiaojiao. Separable data hiding in encrypted image based on compressive sensing and discrete Fourier transform[J]. Multimedia Tools Application, 2017, 76(3): 20739−20753

[33] Xu Meng, Li Jian. 3D PEE mapping based reversible data hiding for color images[J]. Multimedia Tools Application, 2019, 78(2): 8003−8016

[34] Zhou Siyan, Zhang Weiming, Shen Chaomin. Rate-distortion model for grayscale-invariance reversible data hiding[J]. Signal Processing, 2020, 172: 1−11

[35] Chan Y H, Xu Zixin, Lun P K. A framework of reversible color-to-grayscale conversion with watermarking feature[J]. IEEE Transactions Image Processing, 2020, 29: 859−870

[36] Yang Yang, Zou Tianrui, Huang Genyang, et al. A high visual quality color image reversible data hiding scheme based on B-R-G embedding principle and CIEDE2000 assessment metric[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 32(4): 1860−1874

[37] Ma Wenjing, Wu Youqing, Yin Zhaoxia. High-capacity reversible data hiding in encrypted images using adaptive encoding[J]. Journal of Software, 2022, 33(12): 4746−4757 (in Chinese)
(马文静, 吴友情, 殷赵霞. 自适应编码的高容量密文可逆信息隐藏算法[J]. 软件学报, 2022, 33(12): 4746−4757)

[38] Yu Chunqiang, Zhang Xianquan, Zhang Xinpeng, et al. Reversible data hiding with hierarchical embedding for encrypted images[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 32(2): 451−466

[39] Wu Youqing, Xiang Youzhi, Guo Yutang. et al. An improved reversible data hiding in encrypted images using parametric binary tree labeling[J]. IEEE Transactions on Multimedia, 2020, 22(8): 1929−1938

[40] Yin Zhaoxia, Peng Yinyin, Xiang Youzhi. Reversible data hiding in encrypted images based on pixel prediction and bit-plane compression[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(2): 992−1002

[41] Zhang Qiuyu, Feng Yuchun. Adaptive reversible data hiding algorithm of ciphertext color image[J]. Computer Applications and Software, 2020, 37(2): 313−321 (in Chinese)
(张秋余, 冯玉春. 自适应的密文彩色图像可逆数据隐藏算法[J]. 计算机应用与软件, 2020, 37(2): 313−321)

[42] Khelifi F. On the security of a stream cipher in reversible data hiding schemes operating in the encrypted domain[J]. Signal Processing, 2018, 143: 336−345

[43] Schaefer G, Stich M. UCID: An uncompressed color image database[G]//SPIE 5307: Proc of the Int Society for Optical

Engineering (SPIE). Bellingham, WA: SPIE, 2004: 472−480
[44] Franzen R. The Kodak lossless true color image suite[EB/OL]. [2023-05-19]. http://r0k.us/graphics/kodak/
[45] Weber A. The USC-SIPI image database[EB/OL]. [2023-05-19]. https://sipi.usc.edu/database/



Gao Guangyong, born in 1973. PhD, professor, PhD supervisor. Senior member of CCF. His main research interests include reversible data hiding, computer networks security, multimedia information security, and digital image processing.

高光勇, 1973 年生. 博士，教授，博士生导师. CCF 高级会员. 主要研究方向为可逆数据隐藏、计算机网络安全、多媒体信息安全、数字图像处理.



Ji Chi, born in 2002. Undergraduate. His main research interests include reversible data hiding and multimedia information security.

季　驰, 2002 年生. 本科生. 主要研究方向为可逆数据隐藏、多媒体信息安全.



Xia Zhihua, born in 1983. PhD, professor, PhD supervisor. Winner of the National Science Fund for Excellent Young Scholars. His main research interests include digital forensic and encrypted image processing.

夏志华, 1983 年生. 博士，教授，博士生导师，国家优秀青年科学基金获得者. 主要研究方向为数字取证、加密图像处理.