中图法分类号:TP309　　**文献标识码**:A　　**文章编号**:1006-8961(2025)03-0769-15

论文引用格式:Chen Z Y, Yin Z X, Zhan H J, Lyu S J and Hu M H. 2025. Reversible data hiding in encrypted images based on combined encoding method containing the opposite bit. Journal of Image and Graphics, 30(3):0769-0783(陈振宇, 殷赵霞, 占鸿渐, 吕淑静, 胡孟晗. 2025. 隐含异位联合编码的密文图像可逆信息隐藏. 中国图象图形学报, 30(3):0769-0783)[DOI:10.11834/jig.240287]

隐含异位联合编码的密文图像可逆信息隐藏

陈振宇[1],殷赵霞[1,2*],占鸿渐[1,2],吕淑静[1,2],胡孟晗[1,2]

1. 华东师范大学通信与电子工程学院,上海　200241; 2. 华东师范大学上海市多维度信息处理重点实验室,上海　200241

摘　要:**目的**　密文图像可逆信息隐藏技术旨在将信息嵌入至加密图像,以确保信息和原始图像能够准确提取和无损恢复。针对密文图像可逆信息隐藏嵌入率不高的问题,通过增加编码的信息运载效率与利用相邻像素相关性,提出了一种位平面隐含异位联合编码的密文图像可逆信息隐藏方案。**方法**　首先,图像所有者将原始图像分成大小相等的块,并计算出原始图像像素的预测误差。然后,对预测误差的8个位平面进行重排。在位平面压缩阶段,运用隐含异位的联合编码方法进行压缩。压缩后,各类辅助信息被放置到多个高位平面并加密,在多个低位平面上预留空间,结束后进行图像混洗。信息隐藏者将信息嵌入到混洗图像的预留空间中。最后,图像接收者使用密钥提取嵌入的信息或无损恢复原始图像。**结果**　实验结果表明,所提算法在两个常用数据集BOSSBase(break our steganographic system)和BOWS2(break our watermarking system 2nd)上的平均嵌入率分别为3.818 3 bpp和3.694 3 bpp,在同类算法中表现优异。**结论**　所提算法更好地利用原始图像相邻像素间的相关性解决了实际应用中连续比特流串长度较短、数量较多带来的压缩率损失问题,从而提升了嵌入率。

关键词:密文图像可逆信息隐藏(RDHEI);隐含异位压缩;联合编码;预测误差;位平面;嵌入率(ER)

Reversible data hiding in encrypted images based on combined encoding method containing the opposite bit

Chen Zhenyu[1], Yin Zhaoxia[1,2*], Zhan Hongjian[1,2], Lyu Shujing[1,2], Hu Menghan[1,2]

1. School of Communication & Electronic Engineering, East China Normal University, Shanghai　200241, China;

2. Shanghai Key Laboratory of Multidimensional Information Processing, East China Normal University, Shanghai　200241, China

Abstract: **Objective** The technology of reversible data hiding in encrypted images (RDHEI) aims to embed secret information into encrypted images, ensuring that the secret information and the original image can be extracted and restored without loss. This technology is gaining increasing attention from researchers and is widely applied in cloud services to protect users' privacy. Currently, RDHEI can be mainly divided into two categories: the VRAE (vacating room after encryption) algorithm and the RRBE (reserving room before encryption) algorithm, based on the order of image encryption and room operation. The VRAE algorithm vacates space by compressing the pixels of the encrypted image. This compression yields only a limited amount of space due to the high information entropy of the encrypted image. In contrast, the RRBE algorithm primarily compresses the image using pixel correlation before encrypting it. The original image has lower information entropy; thus, more space can be reserved before encryption. This paper proposes a new RDHEI scheme based on bit-

收稿日期:2024-05-28;**修回日期**:2024-08-13;**预印本日期**:2024-08-20

*通信作者:殷赵霞　zxyin@cee.ecnu.edu.cn

基金项目:国家重点研发计划资助(2023YFF0905000)

Supported by: National Key R&D Program of China(2023YFF0905000)

plane compression containing opposite bits and leverages the correlation between the encoding information delivery efficiency and adjacent pixels to improve the performance of reversible data hiding in encrypted images. **Method** First, bit-plane rearrangement and pixel prediction methods are adopted to ensure the utilization of the correlation between adjacent pixels. The image owner initially divides the original image into several equally sized blocks and calculates the prediction errors of the original image pixels. Afterward, the eight bit-planes of the processed image are rearranged. In the phase of bit-plane compression, a combined encoding method containing the opposite bit is introduced. Specifically, based on the threshold length, the image bitstream is divided into continuous and discontinuous streams for compression. After compressing a continuous bitstream string, the next opposite digit at the end of the string is include; that is, each long compressed bitstream adds an opposite digit. According to this rule, the rearranged images are compressed and sequentially placed in each high-level plane with additional information. Encryption and scrambling operations occur at this point. The room in the low-level plane is then vacated, and the information hider embeds the data into the reserved space of the encrypted image. Finally, the image receiver extracts the original image or secret information without loss based on the different keys used. **Result** Experimental comparisons with six advanced methods on six standard test images and two common datasets, namely BOSSBase and BOWS2, are conducted to evaluate the effectiveness of this algorithm. The embedding rate is used to measure algorithm performance, while peak signal-to-noise ratio (PSNR) and structural similarity (SSIM) indicators serve as quantitative evaluation metrics for lossless reversible recovery. Experimental results show that the average embedding rates of the proposed algorithm on the BOSSBase and BOWS2 datasets are 3.818 3 bpp and 3.694 3 bpp, respectively, demonstrating superior performance compared to similar algorithms. PSNR and SSIM are constant values equal to $+\infty$ and 1, indicating the reversibility of the algorithm. **Conclusion** The proposed algorithm uses the image correlation of the original image and effectively explores the potential of the encoded and compressed information during the encoding and compression processes. This algorithm addresses the issue of compression loss caused by the short and large number of continuous bitstream strings in practical applications, thereby improving compression efficiency and enhancing the embedding rate.

Key words: reversible data hiding in encrypted image (RDHEI); containing opposite bit compression; combined encoding; prediction error; bit-plane; embedding rate (ER)

0 引　言

在当今信息技术快速发展的背景下，个人隐私保护和信息安全成为社会关注的焦点。信息隐藏技术（张新鹏和殷赵霞，2017）作为保护信息不被非法获取和使用的有效手段，在数字通信、军事、医疗和云服务等关键领域扮演着重要角色。在多媒体场景下，信息隐藏技术利用人类视觉系统的不敏感性以及图像（欧博等，2022）、视频（Dalal和Juneja，2021）、音频（Xiang和Li，2017）、3Dmesh（周航等，2022）等多媒体数据编码的冗余性，将额外信息隐藏到多媒体数据中而不破坏其使用价值。而其中，以数字图像为载体的信息隐藏研究最为广泛。可逆信息隐藏（Shi等，2016）在确保所嵌入信息能够准确提取的同时还能无损恢复原始载体信号，在军事、医疗和云服务等方面发挥着重要作用。图像可逆信息隐藏早期研究大多集中在明文域上，核心方法技术包括无损压缩（Fridrich等，2002；Celik等，2005，2006；Zhang等，2013）、差值扩展（Tian，2003；Alattar，2004；Kim等，2008）和直方图修改（Ni等，2006；Zhang等，2013；Zhang，2013；Jia等，2019；Ou和Zhao，2020；Gao等，2020）。移动互联网兴起和智能终端的普及以及云计算技术的成熟使得存储和计算全部由公共云平台提供服务，为了保护数据安全和个人隐私，人们希望将图像等多媒体数据先加密，从而催生了密文压缩、密文检索、外包计算和密文域信息隐藏等密文域信号处理技术。密文图像可逆信息隐藏（reversible data hiding in encrypted image，RDHEI）（Puech等，2008；Zhang，2011；Qian等，2018）又称为图像密文域可逆信息隐藏，是密文域信号处理与信息隐藏的交叉研究。

RDHEI能有效地结合图像加密算法与可逆信息隐藏技术，为云服务安全性等应用场景给出了解决方案：图像所有者拥有加密密钥，并且利用加密算法对原始图像进行加密处理；信息隐藏者拥有信息

隐藏密钥，但其无法获取原始图像的内容，只能在加密图像中嵌入信息，实现信息隐藏；图像接收者是最终的信息接收者，当其拥有加密密钥时可以无损恢复图像，而当其拥有信息隐藏密钥时可以完整提取隐藏的信息。但图像加密后编码冗余大辐降低，因此相较于明文图像可逆信息隐藏，嵌入率（embedding rate，ER）往往不高，是制约实际应用效果的关键问题。

目前，按照图像加密与腾出空间的先后顺序，RDHEI技术主要分为两类：加密后腾出空间（vacating room after encryption，VRAE）算法（Zhang，2011，2012；Hong等，2012；Zhang等，2019；Chen等，2023）以及加密前预留空间（reserving room before encryption，RRBE）算法（Ma等，2013；Cao等，2016；Puteaux和Puech，2018）。VRAE算法通过压缩加密图像的像素来腾出空间，由于图像加密后的信息熵非常大，压缩仅能得到有限的空间；而RRBE算法先压缩图像，再对图像进行加密，由于原始图像的信息熵较小，因此能够预留更多的空间。

在云服务等应用场景下，VRAE的腾出空间步骤由云端的信息隐藏者操作，而RRBE的预留空间操作则由本地的图像所有者执行，信息隐藏者仅需进行信息嵌入操作，避免了对加密后的载体图像进行更多处理，从而提高了安全性。同时，在图像解密操作中，VRAE直接解密图像是有损的，为了实现可逆性，需要进一步进行图像恢复操作，如利用纠错码等；而RRBE框架下，直接解密图像即是无损的。因此，相较于VRAE算法，RRBE算法能够更好地兼顾嵌入容量、保密性以及可逆性。本文的主要研究对象是RRBE算法。

Ma等人（2013）提出的RRBE方法，通过在加密前将部分像素的最低有效位（least significance bit，LSB）嵌入到其他像素中预留空间，提高了嵌入能力并确保了数据提取和图像重建的准确性。Yi和Zhou（2017）提出了一种利用像素最高有效位（most significance bit，MSB）的RDHEI方法，通过二进制块嵌入利用块中的冗余性，但未能在所有情况下实现最佳性能。Puteaux和Puech（2018）提出了一种基于多MSB预测的RDHEI方法，映射不可嵌入像素的误差标签并用1位附加数据替换可嵌入像素的MSB。Puyang等人（2018）利用邻域相关性，通过两个MSB进行数据嵌入，提高了嵌入率，但未考虑像素间的冗余和相关性。Yin等人（2020）通过从MSB到LSB比较原始像素的二进制序列和预测误差，并用Huffman编码标记相同的位数，最终用附加数据替换多个MSB，大幅提高嵌入能力。Mohammadi等人（2020）研究了小块冗余，利用差异预测器计算预测误差后将其嵌入多个MSB。Chen等人（2021）提出了一种基于多MSB压缩的方法，通过迭代MSB反演预测、相邻预测平面异或和块变长编码，有效减小了加密图像的文件大小，提高了嵌入能力。

除了MSB和LSB处理，多种加密前预处理操作也能提升嵌入能力。Cao等人（2016）提出了一种基于位平面压缩的RDHEI方法，通过位平面重排和压缩预留空间以提高嵌入率。Wu等人（2020）根据预测误差绝对值划分MSB进行不同标记操作，划分出可用位。周旭等人（2021）对每个位平面进行分块处理，先进行分情况修正的像素预测，再进行压缩。Yu等人（2022）在像素预测与位平面重排后，对预测误差进行分层分析存储，减少存储位数，提高嵌入率。佘晓萌等人（2022）采用分块像素预测与标记方法，利用MSB保存预测误差符号位，其余位平面保存预测误差，提高嵌入能力。Yao等人（2024）结合连续零值高位平面的压缩、位平面交换及块重排，首次尝试以块为单位压缩全局零值高位平面，并适应性地分配不同的Huffman编码，大幅提高了嵌入率。Gao等人（2024）采用多线性回归预测，使用两层标签图管理预测标签，增强嵌入容量，但处理时间较长。Ankur等人（2024）通过中值边缘检测器和差异预测器将原始图像转换为低幅值差分矩阵，采用四叉树位平面表示策略和位平面冗余缓解策略，对差分矩阵进行编码，显著压缩其大小，为嵌入大量数据创造空间，同时保证完全可逆性。

图像压缩过程中，选择不同编码策略同样显著影响嵌入率。吴友情等人（2021）在压缩阶段采用自适应Huffman编码对相同比特位进行编码。吴友情等人（2022b）采用定长编码和Huffman编码相结合的联合编码方式。Yin等人（2022）提出了一种扩展的游程编码方法，而吴友情等人（2022a）在此基础上对较短编码使用Huffman编码以节约空间。Gao等人（2023）对经过几何变换后的图像标签使用Huffman编码，以压缩标签图所占的空间。Xu等人（2023）提出一种基于分层块可变长度编码的RDHEI方法，通过选择最优可压缩块大小捕获局部稀疏性，

并通过变长编码压缩数据，从而提升嵌入能力。

大多数联合编码算法将比特流分为较长的连续比特流和较短的非连续比特流。然而，在多数情况下，编码非连续比特流的效果并不理想，因此算法的改进主要集中在连续比特流上。目前的编码方法仅保留了压缩前连续比特流的一些信息，但在压缩后仍有机会为其赋予更多的信息。为了更充分地利用连续比特流并提高嵌入率，本文提出了一种基于隐含异位联合编码的RDHEI算法。

本文的主要贡献如下：1）提出一种联合编码方案，能够更有效地压缩经过像素预测与位平面重排的稀疏位平面。通过采用隐含异位的方法，赋予连续比特流更多的信息，从而提升图像压缩效率，并提高嵌入率。2）优化算法流程，确保在图像压缩和重构阶段能够准确地赋予和恢复隐含的异位信息，从而保证载体图像的可逆性和嵌入信息的完整性。

1 相关工作与联合编码

本节阐述图像压缩前的准备工作，包括像素预测以及位平面重排，然后详细介绍使用隐含异位方法的联合编码的编码方案。像素预测能够更好地利用相邻像素间的相关性，使得处理后图像的多个MSB变得更加稀疏；位平面重排则是将不同位平面像素进行重新排列，以找到对后续压缩操作更优的像素序列的方法。以上二者为联合编码实现图像压缩并预留空间提供了必要条件。联合编码采用了连续比特流编码与短编码相结合的方式，并在使用过程中加入隐含异位的处理，从而提升图像的压缩效率。其中连续比特流编码使用隐含异位的编码方法见1.3.3节，短编码使用定长编码的方法见1.3.2节。

1.1 像素预测

像素预测能够更好地利用相邻像素间的相关性。本文采用的是边缘中值预测（median edge detector，MED）方法（Weinberger等，2000），如图1所示。

对于一个长宽分别为m和n的图像，$x(i,j)$为该图像任意位置的像素，其中$0<i\leqslant m$，$0<j\leqslant n$，$x(i,j)$的预测值$px(i,j)$为

$$px(i,j)=\begin{cases}\max(x_2,x_3) & x_1\leqslant\min(x_2,x_3)\\ \min(x_2,x_3) & x_1\geqslant\max(x_2,x_3)\\ x_2+x_3-x_1 & \text{其他}\end{cases}\tag{1}$$

式中，$px(i,j)\in[0,255]$（$0<i\leqslant m$，$0<j\leqslant n$）的预测值应由x_1,x_2,x_3预测得出。x_1位于$px(i,j)$的左上方，x_2位于$px(i,j)$的上方，x_3位于$px(i,j)$的左方。以图1为例：$x_1=144$，$x_2=142$，$x_3=147$。因为$x_1\leqslant\min(x_2,x_3)$且$x_1\geqslant\max(x_2,x_3)$，由式（1）得$px(i,j)=x_2+x_3-x_1=142+147-144=145$。

随后引入预测误差$ex(i,j)$，具体为

$$ex(i,j)=px(i,j)-x(i,j)\tag{2}$$

式中，$x(i,j)$为原始像素值。显然，将$x(i,j)$还原仅需使用预测像素值$px(i,j)$减去预测误差值$ex(i,j)$。为了让预测误差能够放入图像，首先将$ex(i,j)$从十进制转化成8位二进制，具体为

$$ex^k(i,j)=\left\lfloor\frac{ex(i,j)}{2^{k-1}}\right\rfloor\bmod 2,\ k=1,2,\cdots,8\tag{3}$$

式中，$ex^k(i,j)$（$0<i\leqslant m$，$0<j\leqslant n$）表示其二进制，图1中$ex^k(i,j)=px(i,j)-x(i,j)=145-144=1$，用二进制表示为“00000001”。

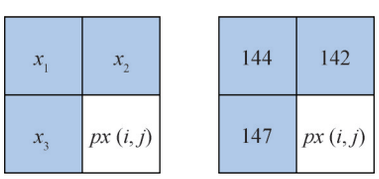


图1 像素预测区域示例

Fig. 1 An example of the pixel prediction area

由于预测误差可能为正也可能为负，因此采用8位二进制的首位表示符号位，其中“1”表示负值，“0”表示正值。由此可确定其表示范围，即$ex(i,j)\in[-127,127]$。当预测误差在该范围内时，称该点为可预测点，不做特殊标记；当预测误差超出该范围，则将该点标记为溢出像素，保留其原始像素值，并将其位置信息存储在附加信息的溢出像素段中。预测误差可以有效包含多个高比特位的像素信息，使得局部相邻像素在高位平面上容易出现多个连续的“0”或“1”，从而有利于提高后续位平面压缩中连续编码的压缩效率；而溢出像素需要保留在原始位置，以确保图像的可逆性。

经过像素预测，原始图像变为由预测像素和溢出像素构成的图像，接着将此图像视为一般的灰度图像，用于位平面重排。

1.2 位平面重排

灰度图像的像素由8位二进制表示，因此图像可以分成8个位平面。通常情况下，通过扫描每个

位平面进行遍历，图像像素间的空间相关性未能得到充分利用。为了提高相邻像素相关性利用率以及图像压缩率，Cao 等人(2016)提出了位平面重排算法。首先，将位平面划分为大小相同的块，然后按照 4 种类型重新排列位平面。位平面重排标志由 2 位二进制表示，其中第 1 位表示块内排列方式，“0”和“1”分别表示块内逐行排列和逐列排列；第 2 位表示块间排列方式，“0”和“1”分别表示块间逐行排列和逐列排列。

以图 2 为例，位平面被分成了 2 × 2 的块，位平面重排标志“00”表示块内的遍历顺序为逐行，块间的遍历顺序也是逐行的，其序列为 $A_1A_2A_3A_4B_1B_2B_3B_4C_1C_2C_3C_4D_1D_2D_3D_4$。由于相邻像素间具有相关性，重排后的比特流往往会存在多个连续相同的比特位，这为提升编码压缩效率提供了条件。

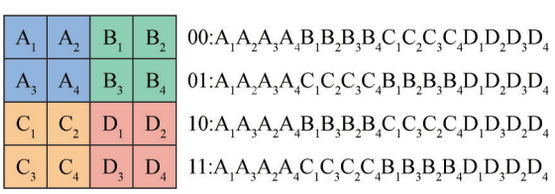


图 2　位平面重排示例

Fig. 2　An example of the bit-plane rearrangement

1.3　编码规则

经过像素预测和位平面重排后，图像的比特流中会出现大量相邻的“0”或“1”。基于这一特性，采用比特流压缩方法进行编码时，可以提取额外的可嵌入空间。本文采用联合编码的方式，并且根据连续比特流的编码特性，提出了隐含异位的联合编码方法，进一步增加了可压缩空间。

编码的长短区分由 l_{thr} 来确定，其中，l_{thr} 为长短编码的临界长度。例如，从重新排列后的比特流中提取一段比特相同的序列 L，L 的长度为 l_L。当 $l_L \geqslant l_{thr}$ 时，称此时的 L 为连续比特序列，并采用隐含异位的连续编码规则；当 $l_L < l_{thr}$ 时，称此时的 L 为短比特序列并采用短编码规则。

1.3.1　连续编码规则

当 $l_L > l_{thr}$ 时，由于连续比特序列的重复位较多，此时可以使用 l_L 的二进制序列来表示“0”或“1”的位数，然后与“0”或“1”组合构成新的序列，以此达到压缩的目的。

假设数字 x 的二进制为 L_x，L_x 的位数为 l_x（$l_x > 0$），x 的值可以拆为两部分，分别为 2^{l_x-1} 和 L_x 的后 $l_x - 1$ 位，也就是说，x 的二进制表示由最高位的值与后 $l_x - 1$ 位的值组成，而此时最高位所表示的值的幂次恰好与其他位的长度相同。例如，数字 13 的二进制为“1101”，即 $13 = 2^{4-1} + (101)_2$，其中 $4 - 1 = 3$，恰好等于其余位的长度。

利用上述特性，对连续比特序列进行编码重构。连续编码可由前缀 L_{pre}、中间部分 L_{mid} 和后缀 L_{tai} 构成。前缀 L_{pre} 表示此段编码为连续编码，其长度也表示中间部分序列 L_{mid} 的长度。L_{pre} 由 $l - 1$ 个“1”与 1 个“0”构成，其中 l 为 L_{pre} 和 L_{mid} 的长度。后缀 L_{tai} 表示此段连续编码由“0”或“1”构成。l 和 L_{mid} 的取值计算式为

$$l = \left\lfloor \log_2^L \right\rfloor \tag{4}$$

$$L_{mid} = (L - 2^l)_2 \tag{5}$$

式中，l 为 L_{pre} 的长度，L_{mid} 为中间部分序列。L_{mid} 即为 L 去掉二进制最高位后的剩余序列。使用这种方法不仅可以有效地压缩重复位比特序列，而且在还原过程中能够准确确定连续编码的长度。

1.3.2　短编码规则

当序列长度 $l_L < l_{thr}$ 时，由于短比特序列的重复位较少，若采用与连续编码相同的规则，则会导致编码序列的长度相较于原始序列更长，压缩效果较差。因此，本文采用定长编码的方法处理短比特序列，此时的编码包含前缀 L_{pre} 和截取比特序列 L_{mid} 两部分，其中 L_{mid} 的长度为 $l_{thr} - 1$。

L_{pre} = “0”标志该段编码为短编码，L_{mid} 为从 L 当前位向后截取长度为 $l_{thr} - 1$ 的比特流序列，因此短编码的长度固定为 l_{thr}。

以截取比特流“11111111110010111111”为例，当 $l_{thr} = 4$ 时，联合编码算法的具体执行过程如下：第 1 轮提取出 11 bits“1”，因为 11 bits > 4 bits，所以此时采用连续编码；通过式(4)计算出 $l = \left\lfloor \log_2 11 \right\rfloor = 3$，因此 L_{pre} = “110”；通过式(5)计算出 $L_{mid} = (11 - 2^3)_2$ = “011”，而 L_{tai} 显然为“1”，最终第 1 轮压缩序列为“1100111”。第 2 轮提取出 2 bits“0”，因为 2 bits < 4 bits，所以此时采用短编码，L_{pre} = “0”，L_{mid} = “001”，因此第 2 轮压缩序列为“0001”。第 3 轮提取出 1 bit “0”，因为 1 bit < 4 bits，所以此时采用短编码，L_{pre} = “0”，L_{mid} = “011”，因此第 3 轮压缩序列为“0011”。第 4 轮提取出 4 bits“1”，因为 4 bits ⩾ 4 bits，所以此时采用连续编码，经计算得出 $l = \left\lfloor \log_2 4 \right\rfloor = 2$，$L_{pre}$ =

“10”，$L_{mid}=(4-2^2)_2$ = “00”，L_{tai} = “1”，因此第4轮压缩序列为“10001”。最终，比特流“111111111110010111111”被压缩成“11001110001001110001”，从21 bits压缩到19 bits。

1.3.3 隐含异位的编码规则

尽管连续编码对于重复位序列有很好的效果，但其仍有提升的空间。在联合编码的程序实现过程中，计算机在截取连续比特序列前，会比较当前位与下一位是否相同。如果不同，则截取当前的连续比特序列；如果相同，则将当前位添加进连续比特序列中，并继续比较下一位。因此，一个必然事件是：在截取连续比特序列后，后一位的数字一定与该连续比特序列的数字不同。

基于此原理，本文提出了隐含异位的编码方法，即在连续编码中隐含后一位的不同数字信息。同样使用$L_{pre}+L_{mid}+L_{tai}$来表示连续比特序列L。使用隐含异位的方法不仅可以表示原本的连续比特序列，还能表示其后的异位数字，即能够表示l_L+1位的原始数据。这意味着，在连续比特序列编码过程中，每个异位数字都被隐含在连续编码中，并在连续比特序列截取时提前移除。在比特流末尾，由于无法进行异位隐含操作，这类特殊情况会在比特流恢复时，根据原始比特流的长度进行判断和处理。

同样，以“11111111110010111111”为例，执行隐含异位的联合编码算法具体过程如下：第1轮提取出11 bits“1”，因为11 bits > 4 bits，所以此时采用隐含异位的连续编码；通过式(4)计算出$l=\lfloor\log_2 11\rfloor=3$，因此$L_{pre}$ = “110”；通过式(5)计算出$L_{mid}=(11-2^3)_2$ = “011”，而L_{tai} = “1”，最终第1轮压缩序列为“1100111”。由于采用隐含异位方法，将剩余比特流的首位“0”剔除，作为压缩比特流的隐含信息。此时剩余比特流为“010111111”。第2轮提取出1 bit“0”，因为1 bit < 4 bits，所以此时采用短编码，L_{pre} = “0”，L_{mid} = “010”，因此第2轮压缩序列为“0010”。第3轮提取出6 bits“1”，因为6 bits > 4 bits，所以此时采用隐含异位的连续编码，经计算得出$l=\lfloor\log_2 11\rfloor=2$，$L_{pre}$ = “10”，$L_{mid}=(6-2^2)_2$ = “10”，L_{tai} = “1”，因此第3轮的压缩序列为“10101”。最终，比特流“11111111110010111111”被压缩成“1100111001010101”，从21 bits压缩到16 bits，相较于1.3.2节示例，压缩效率显著提高。

2 算法设计

基于RRBE框架，本文提出一种隐含异位联合编码的RDHEI算法。本节首先介绍该算法的整体框架，算法的三方参与者分别是图像所有者、信息隐藏者和图像接收者，三者各自承担不同的任务。随后详细介绍算法过程中涉及的空间压缩、图像加密、信息嵌入以及信息提取等步骤。

2.1 算法框架

本文提出的位平面隐含异位联合编码的RDHEI算法框架如图3所示，整个过程分为3个阶段：1)图像所有者先对原始图像进行空间压缩，然后加密；2)信息隐藏者将信息加密并嵌入；3)图像接收者将图像解密还原和提取信息。在第1阶段，为了压缩出更多的空间，预处理会利用原始图像的像素预测误差进行位平面重排。特别地，为确保图像无损压缩的顺利进行，预处理步骤产生的位平面重排块大小、溢出像素数量和位置等辅助信息会被暂存，在无损压缩结束后，这些辅助信息随其他辅助信息一同被存入MSB中。接着，对处理后的比特流使用隐含异位的联合编码进行压缩，其中灰色部分表示比特流压缩后的预留空间，最后对图像进行加密操作。第2阶段，信息隐藏者将加密的信息嵌入到第1阶段压缩生成的预留空间中，从而得到载密图像。最后在第3阶段，图像接收者使用相应密钥进行图像无损还原与信息提取。

2.2 空间压缩

为了增加预留空间的容量，图像所有者会对图像进行压缩后再加密。对8个位平面(从MSB到LSB)的预测误差进行位平面重排和比特流压缩，流程如下。首先，使用第1.2节的4种排序方法重新排列MSB平面。然后，对这4种重新排列的比特流分别进行压缩，并选择压缩结果最短的一种作为该位平面的最终压缩结果。具体步骤为：当$l_L<4$时，采用1.3.2节的短编码压缩方式；当$l_L\geqslant 4$时，则使用1.3.3节的隐含异位连续编码压缩方式。如果4种压缩结果均长于原始比特流，则当前位平面不可被压缩；如果存在某一压缩结果短于原始比特流，则选择此排序类型下的压缩结果作为最终压缩结果。同理，对其他几个位平面也依次进行上述操作。

位平面压缩比特流存储结构如图4所示。首先

会按照位平面重排块的大小、l_{thr}值、溢出像素的数量与具体位置的次序排列存储，从而构成比特流头部的辅助信息。然后根据位平面的可压缩性，将每个位平面的压缩比特流分成两种情况：当位平面可压缩时，$flag = 1$表示位平面可以压缩，重排类型使用2 bits来记录，接着依次存储位平面压缩比特流长度和位平面压缩比特流；当位平面不可压缩时，$flag = 0$表示该位平面不可压缩，直接存储位平面原始比特流。

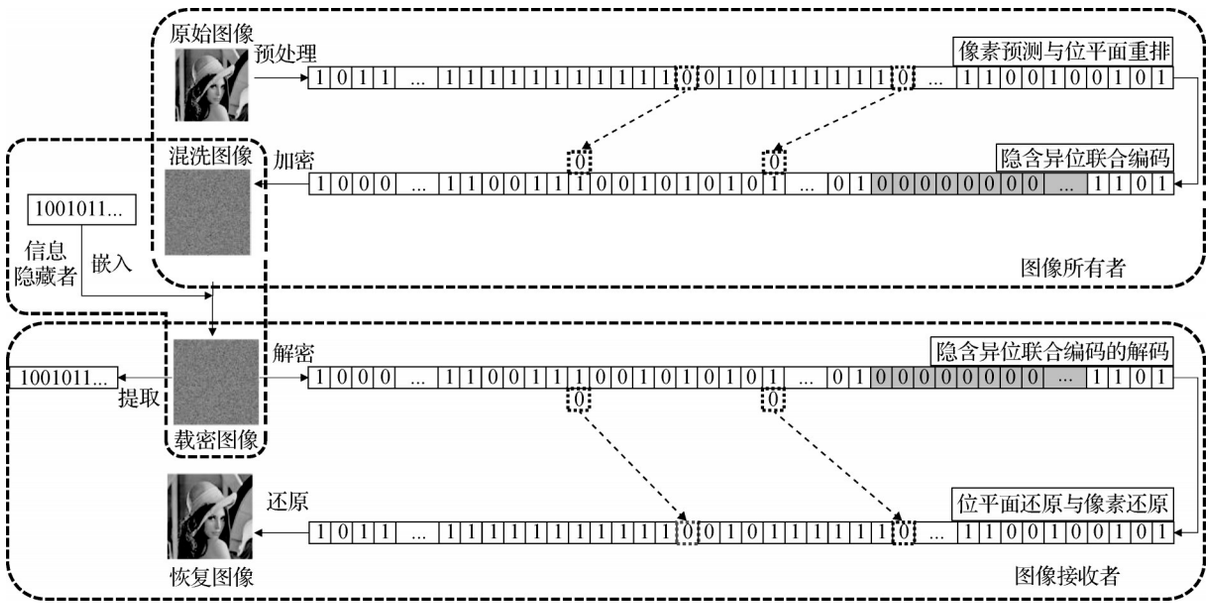


图3　隐含异位联合编码的RDHEI算法框架

Fig. 3　The framework of the RDHEI algorithm based on combined encoding method containing the opposite bit

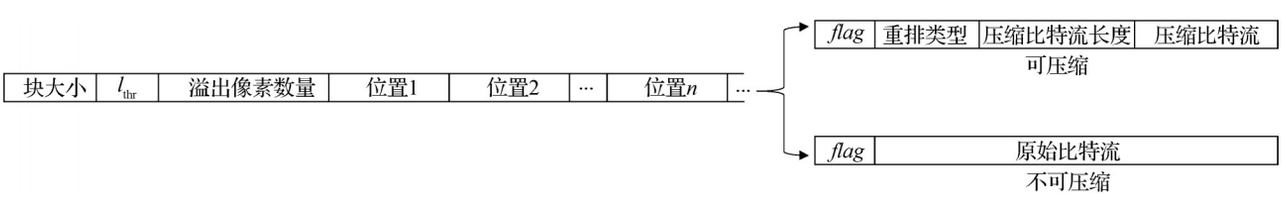


图4　位平面压缩比特流的存储结构

Fig. 4　The storage structure of bit-plane compressed bitstream

压缩图像的存储结构如图5所示。将上述各部分按顺序连接，并依次放入到各个高位平面上，空出的空间和其余低位平面使用0进行填充。辅助信息被放置在MSB平面上，以方便重构图像时获取；预留空间比特流数量被放置在LSB平面上，以方便嵌入或提取隐藏信息时获取。最后，得出包含可嵌入空间的压缩图像$\boldsymbol{I}_c$，具体为

$$x_c(i,j) = \sum_{k=1}^{8} x_c^k(i,j) \times 2^{8-k}, k = 1, 2, \cdots, 8 \quad (6)$$

式中，$1< i \leqslant m$，$1< j \leqslant n$，$x_c(i,j)$为压缩图像$\boldsymbol{I}_c$的像素。

2.3　图像加密

使用流密码加密的方法进行图像加密。首先，图像所有者需要利用密钥K_{en}获取一个伪随机矩阵$\boldsymbol{H}$，其大小为$m \times n$。然后，使用式(3)将$\boldsymbol{H}$的对应值$h(i,j)$与压缩图像$\boldsymbol{I}_c$的像素$x_c(i,j)$转化为8位二进制序列。紧接着，使用式(7)按位执行XOR(异或)加密操作。

$$x_e^k(i,j) = x_c^k(i,j) \oplus h_c^k(i,j), k = 1, 2, \cdots, 8 \quad (7)$$

式中，$x_e^k(i,j)$表示第k个位平面上的通过XOR加密的二进制，“⊕”表示XOR操作。最后，加密像素$x_e(i,j)$通过式(6)计算得出，被加密的图像$\boldsymbol{I}_e$即为所得。

2.4　信息嵌入

为了将信息嵌入预留空间中，信息隐藏者首先提取位于LSB平面的预留空间长度信息，并依据此信息定位预留空间。紧接着，先使用密钥K_d对信息进行XOR加密，然后再将加密的信息嵌入到预留空

间中，最终生成载密图像$\boldsymbol{I}_s$。

2.5 信息提取与图像恢复

图像接收者在此部分进行嵌入信息的提取与图像的恢复。根据所持密钥K_{en}、K_d的不同，图像接收者拥有不同的权限，具体如下：

1）图像接收者只有密钥K_d：此时可以提取嵌入信息。由于密钥K_{en}仅用于图像进行加密，不影响信息嵌入过程，因此提取的嵌入信息可以通过密钥K_d正确解密，从而获取嵌入的信息。解密过程仍采用式(7)。然而，没有密钥K_{en}就无法恢复原始图像的内容。

2）图像接收者只有密钥K_{en}：此时可以恢复原始图像。首先从MSB平面中提取块的大小、l_{thr}和溢出像素的数量和位置，从LSB平面中提取每个位平面的压缩比特流数量。然后根据式(7)，通过密钥K_{en}对图像进行解密，从而获得原始图像。同样，K_d因为不参与图像加密过程，不会对图像还原造成影响，而嵌入信息也无法依靠密钥K_{en}解密提取。

3）图像接收者同时拥有K_{en}和K_d密钥：在此种情况下，图像接收者既可以由K_d正确提取嵌入信息，也可以通过K_{en}解密恢复原始图像。

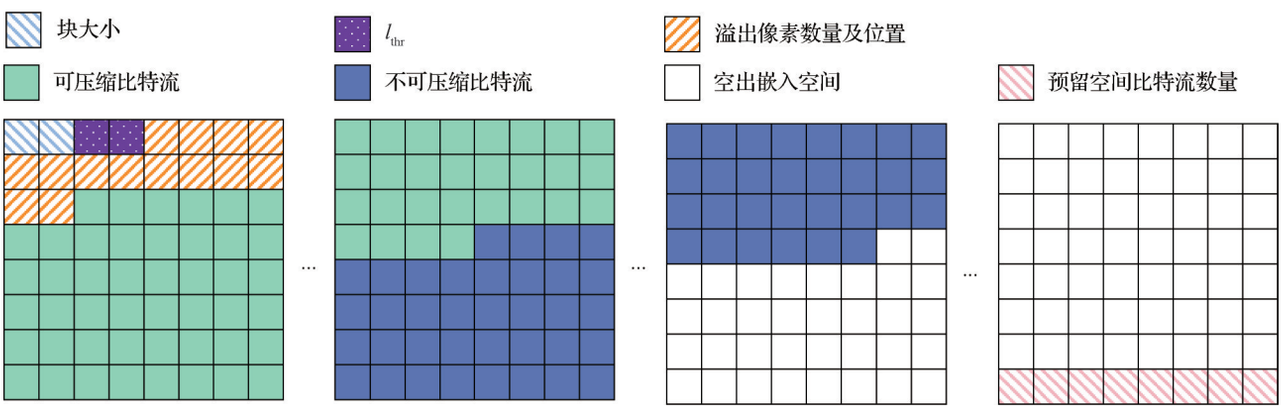


图5 压缩图像的位平面存储结构

Fig. 5 The bit-plane storage structure for compressed images

3 实验结果与分析

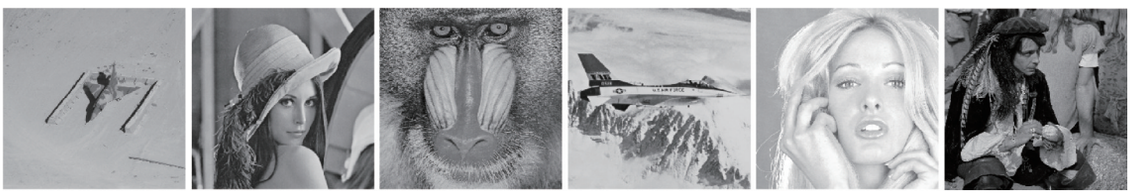
在本节，首先介绍使用的评价指标，然后分别进行可逆性分析、安全性分析、嵌入容量分析、消融实验分析和对比分析。为了验证本方案的优越性，本文将算法与以下研究相比较：Yu等人(2022)、Yin等人(2022)、吴友情等人(2022a)、Gao等人(2023)、Xu等人(2023)和Yao等人(2024)。如图6所示，实验使用了6幅标准灰度图像：Airplane、Lena、Baboon、Jetplane、Tiffany和Man作为测试样例图像。接着使用BOSSbase(break our steganographic system)(Bas等，2011)和BOWS2(break our watermarking system 2nd)(Bas和Furon，2017)两个常用数据集来验证算法的通用性。实验在MATLAB R2021a平台上运行。

3.1 评价指标

本文采用均方差(mean square error，MSE)、峰值信噪比(peak signal-to-noise ratio，PSNR)和结构相似度(structural similarity，SSIM)作为评价方法可逆性的指标，并以嵌入率(ER)评价嵌入能力。MSE是原始图像与处理后图像的均方差，图像失真越少，MSE越小，PSNR取值越大。当MSE = 0时，两幅图像完全相同，PSNR趋近于+∞。SSIM用于比较两图像的相似性，SSIM值范围为0到1，SSIM值越大表示相似性越高。取值为1时，两幅图像完全相同。ER表示每个像素的平均嵌入比特数量，单位为bpp(bit per pixel)，用于衡量隐藏信息的效率。ER值越大，表示嵌入的信息越多。

3.2 可逆性分析

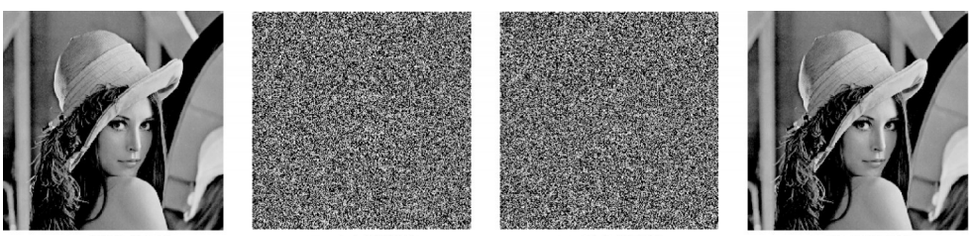
为证明该方法可以无损重建图像，以Lena图像为例，对该图像进行图像压缩、图像加密、信息嵌入以及图像恢复操作。图7(a)为原始图像$\boldsymbol{I}$，图7(b)为经过加密密钥K_{en}加密后的压缩图像$\boldsymbol{I}_e$，图7(c)为载密图像$\boldsymbol{I}_s$，其嵌入率为3.202 3 bpp。由于该方法可以分离提取信息和重建原始图像，因此图像接收者可以使用K_{en}密钥对原始图像进行恢复。图7(d)为重建的图像$\boldsymbol{I}_{re}$。原始图像与恢复图像之间的MSE = 0，SSIM = 1，这说明该方法能无损重建



(a) Airplane (b) Lena (c) Baboon (d) Jetplane (e) Tiffany (f) Man

图6 测试样例图像

Fig. 6 Test images ((a) Airplane; (b) Lena; (c) Baboon; (d) Jetplane; (e) Tiffany; (f) Man)



(a) 原始图像$\boldsymbol{I}$ (b) 加密图像$\boldsymbol{I}_e$ (c) 载密图像$\boldsymbol{I}_s$ (d) 重建图像$\boldsymbol{I}_{re}$

图7 不同操作阶段的Lena图像

Fig. 7 Lena images at different stages of operation

((a) origin image $\boldsymbol{I}$; (b) encrypted image $\boldsymbol{I}_e$; (c) stego image $\boldsymbol{I}_s$; (d) recovered image $\boldsymbol{I}_{re}$)

图像。

为了进一步验证所提方法的可逆性，算法在BOSSbase、BOWS2两个数据集上进行实验验证，表1的结果显示，这两个数据集的原始图像与重建图像间的MSE = 0，并且SSIM = 1。由此可见，该方法对原始图像具有无损重建能力。此外，所提方法在这两个数据集上的信息提取准确率均为1，表明该方法能够无损提取隐藏的信息。

表1 所提算法在BOSSbase和BOWS2的实验结果

Table 1 The experimental results of the proposed algorithm on BOSSBase and BOWS2

测试数据集	最优嵌入率/bpp	最差嵌入率/bpp	平均嵌入率/bpp	MSE	PSNR/dB	SSIM	信息提取准确率
BOSSbase	7.842 8	0.921 95	3.818 3	0	+∞	1	1
BOWS2	7.102 6	0.818 42	3.694 3	0	+∞	1	1

3.3 安全性分析

为了进一步验证安全性，下面将以Lena为例，对其不同阶段的灰度直方图进行详细分析。图7展示了该方法在Lena图像上各阶段的实验结果，而图8展示了Lena图像的3个阶段对应的灰度直方图。图8(a)为包含原始图像特征信息的灰度直方图，其数值分布不均，存在多个峰值点，特征明显。图8(b)为加密图像的灰度直方图，由于图像中像素的分布变得均衡，相关的统计特征难以被轻易获取。从图8(c)可以看出，在嵌入信息后，图像的直方图分布仍保持均衡特征，但载密图像的直方图与原始图像仍有较大差异，也无法从中获得有用的统计信息。

3.4 嵌入容量分析

本节主要通过嵌入率评估该方法在BOSSbase和BOWS2两个数据集以及测试图像上的效果。

表1显示了本文方法在两个数据集BOSSbase和BOWS2上的平均净嵌入率。对于BOSSbase数据集，最佳情况嵌入率为7.842 8 bpp，最差情况嵌入率为0.921 95 bpp，平均嵌入率为3.818 3 bpp。对于BOWS2数据集，最佳情况嵌入率为7.102 6 bpp，最差情况嵌入率为0.818 42 bpp，平均嵌入率为3.694 3 bpp。

表2展示了6幅测试图像和数据集在压缩前后各个位平面的比特流数量，其中，两个数据集展示的是其每个位平面的平均比特流数量。由于使用第8位平面来记录预测误差的符号，因此该位平面上的“0”和“1”数量相似，并且随机分布在该位平面上。这使得被压缩的比特流的长度比原始比特流的长度

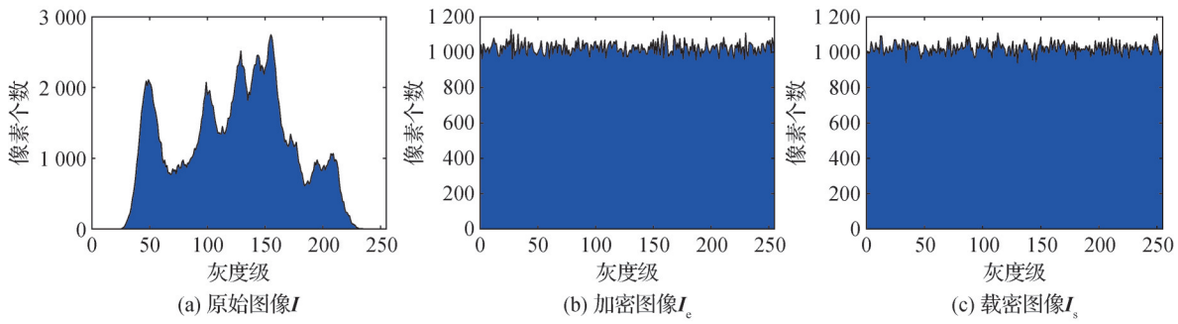


图8　不同操作阶段的Lena图像的灰度直方图

Fig. 8　Histograms of the Lena image at different operational stages ((a) origin image $\boldsymbol{I}$; (b) encrypted image $\boldsymbol{I}_e$; (c) stego image $\boldsymbol{I}_s$)

表2　所提算法在测试样例和测试数据集(平均)各位平面的压缩比特流长度

Table 2　The proposed algorithm's bit-plane compression bitstream length in different test images and test datasets (average)

/bit

测试图像	位平面比特	压缩比特流							
		第8位	第7位	第6位	第5位	第4位	第3位	第2位	第1位
Airplane	262 144	262 144	5 613	13 704	24 830	59 924	154 682	262 144	262 144
Lena	262 144	262 144	3 191	15 241	50 501	140 052	262 144	262 144	262 144
Baboon	262 144	262 144	31 029	124 044	218 806	262 144	262 144	262 144	262 144
Jetplane	262 144	262 144	3 182	17 655	49 903	102 318	199 359	262 144	262 144
Tiffany	262 144	262144	4 227	15 066	51 349	121 422	255 486	262 144	262 144
Man	1 048 576	1 048 576	15 191	76 776	290 663	865 398	1 048 576	1 048 576	1 048 576
BOSSbase (平均)	262 144	232 550.563 8	6 569.852 9	25 379.995 6	58 392.576 0	96 998.522 9	147 117.834 2	189 286.318 1	234 173.235 2
BOWS2 (平均)	262 144	242 050.662 4	6 506.414 1	27 734.835 2	65 462.599 7	108 401.786 9	151 023.779 8	209 995.694 1	235 470.848 0

更长，因此该位平面未被压缩。另一方面，由于MED预测精度高，第7～5位平面的“0”数量远远大于“1”，压缩后比特流的长度小于原始比特流的长度，且压缩效率随着位平面维度的降低而降低。以Airplane为例，第7位平面的压缩比特流的长度为5 613 bits，其压缩程度最大。而第3位平面的压缩比特流的长度为154 682 bits，与其他可压缩位平面相比，其压缩程度最小。

在BOSSbase和BOWS2数据集上也表现同样的规律。一方面，第8位平面和第1位平面的平均压缩比特流长度几乎等于原始比特流长度，这说明绝大多数图像在这些位平面上是不可压缩的；另一方面，第7～2位平面明显可压缩，并且随着位平面维度的降低，位平面的压缩效率逐渐降低。在第7位平面上，平均压缩效率最高，而在第2位平面上，平均压缩效率最低。测试图像和测试数据集的辅助信息长度、净有效载荷和嵌入率如表3所示。假设一幅图像的溢出点数为t，其点数和位置分别使用18 bits和$t\times 18$ bits来记录。块的大小和l_{thr}的值分别用4 bits和3 bits表示，而辅助信息由这些参数构成。从表3可以看出，6幅测试图像上的辅助信息的长度远短于预留空间。以Airplane为例，其辅助信息长度为115 bits，净有效载荷长度为1 051 760 bits，净嵌入率为4.012 1 bpp。在两个数据集中，辅助信息的平均长度也远短于预留空间。因此，存储辅助信息对嵌入率的影响很小。

3.5　消融实验分析

为了验证本文编码方法在提升嵌入容量方面的有效性，本节对图像压缩过程中的隐含异位进行了消融实验。以Lena图像为例，表4展示了使用隐含异位方法前后，长短编码在不同位平面上的数量差距和最长连续比特长度。根据第2节联合编码部分

表 3　所提算法在测试样例和测试数据集（平均）上辅助信息长度、净有效载荷和嵌入率

Table 3　The auxiliary information length, net payload, and ER of the proposed algorithm on test images and test datasets (average)

测试图像	溢出点数	溢出点位置/bit	辅助信息长度/bit	净有效载荷/bit	嵌入率/bpp
Airplane	5	18 × 5	115	1 051 760	4.012 1
Lena	0	18 × 0	25	839 476	3.202 3
Baboon	3	18 × 3	79	412 440	1.573 3
Jetplane	1	18 × 1	43	938 168	3.578 8
Tiffany	5	18 × 5	115	862 963	3.291 9
Man	125	18 × 125	2 527	2 943 911	2.807 5
BOSSbase（平均）	12.828 8	18 × 12.828 8	255.918 4	1 000 951.295 1	3.818 3
BOWS2（平均）	0.681 3	18 × 0.681 3	37.263 4	968 440.568 6	3.694 3

的描述，连续编码数量越多，隐含异位方法的优势越明显；短编码数量越少，压缩效率越高；最长连续比特长度越长，单个连续编码的压缩效率越高。由表 2 可知，Lena 图像可压缩位平面为第 7、6、5、4 位，而从表 4 的相应位平面长短编码数量及最长连续比特长度来看，验证了上述结果：在第 6 和第 4 位平面上，使用隐含异位方法时，尽管最长连续比特长度短于不使用隐含异位方法，但在连续编码数量近乎相同的情况下，短编码数量减少了近 1/3，抵消了最长连续比特长度缩短带来的影响；而在第 7 和第 5 位平面上，连续编码数量近乎相同，使用隐含异位方法后，短编码数量明显减少，因此这几个位平面压缩效率更高，且最长连续比特长度显著增加，效果更优。尽管第 8、第 3、第 2 和第 1 位平面未进行压缩，但从表中可看出，隐含异位方法在各项指标上均具有优势。

3.6　对比分析

相较于其他 RRBE 类型算法，本文提出的隐含异位联合编码方法在嵌入率指标上具有明显的优势。图 9 展示了各算法在 6 幅测试样例图像上的实验结果。除 Airplane 与 Tiffany 外，本文方法的嵌入率均为最优。对于 Airplane 图像，由于其较为平滑，各算法均能取得不错的效果，在这种情况下，Yao 等人（2024）的嵌入率最高，因为其在预测误差后，各位置像素预测误差数量多且分布在同一幂级，因此能够最大限度地利用位平面交换的优势。因此，虽然本文方法在此类图像上稍逊于 Yao 等人（2024）方法，但在纹理更复杂的图像上，本文方法效果更佳。

表 4　隐含异位方法有效性的消融实验

Table 4　Ablation experiment results for the containing the opposite bit method

/bit

位平面	非隐含异位			隐含异位		
	连续编码数量	短编码数量	最长连续比特长度	连续编码数量	短编码数量	最长连续比特长度
8	9 724	68 482	242	9 094	67 940	241
7	215	360	45 090	117	297	53 671
6	1 031	1 728	7 892	959	1 087	7 041
5	3 129	7 648	1 970	3 655	5 024	8 251
4	9 043	24 156	791	9 740	17 457	457
3	13 175	55 064	195	13 732	48 831	162
2	10 586	68 694	31	10 246	65 637	35
1	10 082	69 999	31	9 816	67 125	31

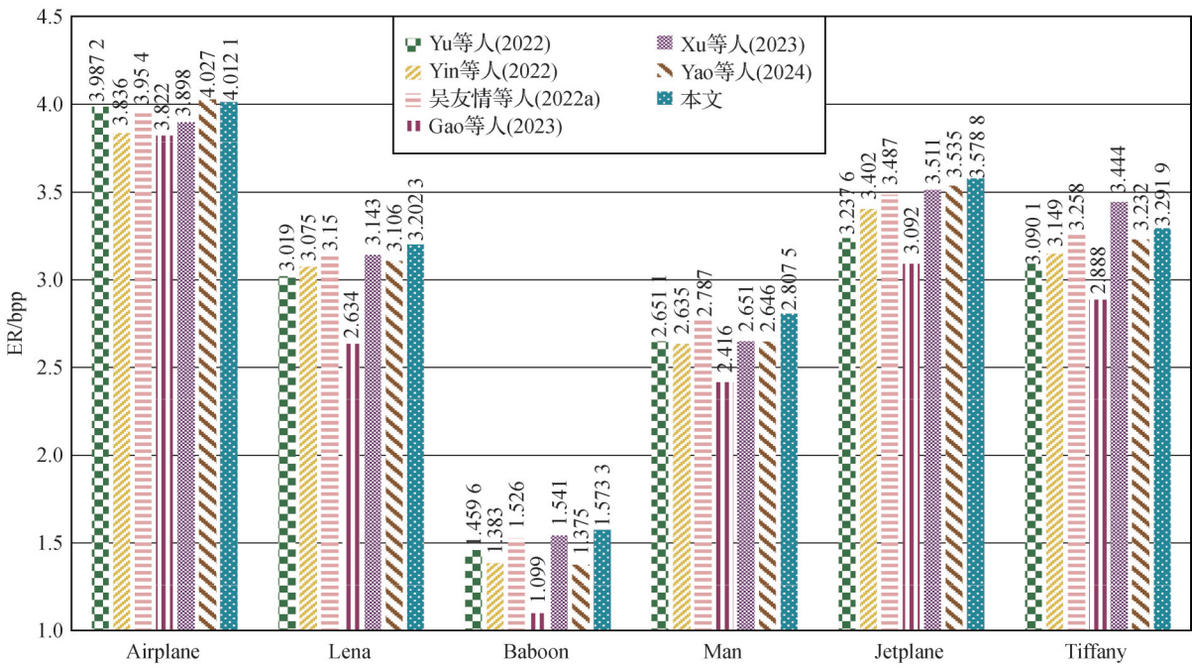


图9　各算法在6幅测试样例上的嵌入率比较

Fig. 9　Comparison of ER among different algorithms on six test images

Tiffany图像由于纹理较为规律，便于Xu等人(2023)根据位平面局部平滑性，自适应地分解不同层级的块，因此在此类图像上的效果最佳。但在局部纹理更为复杂或者全局纹理更为平滑的情况下，Xu等人(2023)的方法效果较差。

图10展示了各算法在BOSSbase和BOWS2数据集上的比较实验结果，表明本文方法具有显著的效果。在BOSSbase数据集中，本文方法的平均嵌入率为3.818 3 bpp，高出第2名(Xu等人(2023)方法)0.025 3 bpp。而在BOWS2数据集中，Xu等人(2023)的方法效果更优，这是因为BOWS2数据集包含超过半数为雪山、河流、海洋等平滑度较高的风景图像，能够更好地发挥其算法优势，因此其嵌入率略高于本文方法。

表5展示了各个算法的时间复杂度。本文算法在像素预测与位平面重排阶段均使用了双循环操作，因此预处理阶段本文方法的时间复杂度为$O(n^2)$。在图像压缩阶段，尽管联合编码设置条件复杂、步骤

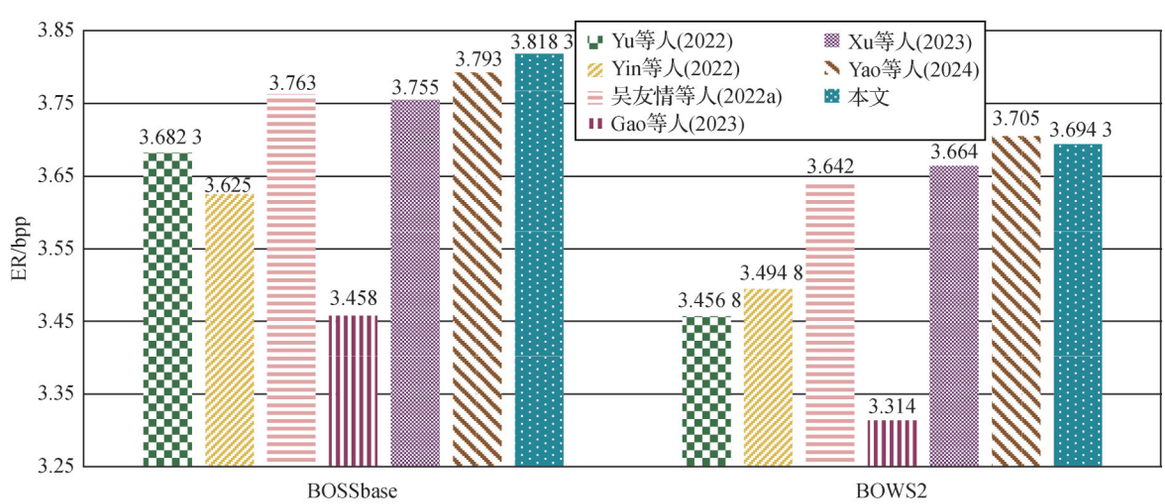


图10　各算法在BOSSbase和BOWS2上的平均嵌入率

Fig. 10　Comparison of average ER among different algorithms on BOSSbase and BOWS2

烦琐，但其仍在双重循环内完成，而隐含异位操作随联合编码同时进行，不会影响时间复杂度。此外，图像加密和信息嵌入步骤较为简单，时间复杂度仅为$O(n)$；图像提取恢复过程是图像压缩和预处理的逆过程，因此其时间复杂度也为$O(n^2)$。综上所述，本算法的整体时间复杂度为$O(n^2)$。

同为RRBE算法，各算法处理流程大致相同，时间复杂度至少应为$O(n^2)$，而算法整体的时间复杂度主要由图像压缩和信息嵌入的复杂程度决定。Yu等人(2022)在计算图像预测误差时，需要对目标图像的各像素生成分层标签，逐层将预测差值绝对值划分为大、中、小3种量级范围，至多会进行3层循环，故其时间复杂度为$O(n^3)$。Yin等人(2022)与吴友情等人(2022a)采用联合编码对图像进行编码压缩，二者将每段截取比特流划分成两种情形，因此压缩编码阶段至多会进行两层循环，二者时间复杂度均为$O(n^2)$。Gao等人(2023)的自适应Huffman编码步骤决定了其时间复杂度为$O(n^2)$。Xu等人(2023)的自适应分块与变长编码的时间复杂度均为$O(n^2)$。由于Yao等人(2024)的位平面交换与块重排是该方法最为复杂的步骤，时间复杂度为$O(n^2)$，因此其总体时间复杂度也应为$O(n^2)$。

表5　时间复杂度比较

Table 5　Comparison of time complexity

方法	时间复杂度
Yu等人(2022)	$O(n^3)$
Yin等人(2022)	$O(n^2)$
吴友情等人(2022a)	$O(n^2)$
Gao等人(2023)	$O(n^2)$
Xu等人(2023)	$O(n^2)$
Yao等人(2024)	$O(n^2)$
本文	$O(n^2)$

4　结　论

为了进一步提高密文图像可逆信息隐藏嵌入率，本文提出了一种基于隐含异位联合编码的RDHEI算法。首先采用像素预测以及位平面像素重排，更好地利用像素间关联性；其次在编码阶段提出隐含异位的联合编码方法对图像比特流进行压缩处理，有效增加了编码信息容量。实验结果表明，所提算法能够在准确提取信息、完整重构原始图像的前提下达到更高的嵌入率。与其他同类型先进算法相比，所提算法嵌入率表现优秀，在BOSSBase和BOWS2上的平均嵌入率分别为3.818 3 bpp和3.694 3 bpp。

然而，本文方法在局部纹理更复杂或者全局纹理更为平滑的情况下，嵌入率表现相对较差。因为局部纹理更复杂会带来更多的短编码降低整体嵌入率效果；全局纹理更平滑会使得连续编码长度更长，数量更少，隐含异位方法效果受限。在未来的工作上，可以针对不同纹理、不同特征的比特流串采用自适应的编码方式，例如采用Huffman编码来进行优化，以解决不同载体信号可能存在的不同问题，如短编码过多带来的效果下降。

参考文献(References)

Alattar A M. 2004. Reversible watermark using the difference expansion of a generalized integer transform. IEEE Transactions on Image Processing, 13(8): 1147-1156 [DOI: 10.1109/tip.2004.828418]

Ankur, Kumar R and Sharma A K. 2024. Bit-plane based reversible data hiding in encrypted images using multi-level blocking with Quad-Tree. IEEE Transactions on Multimedia, 26: 4722-4735 [DOI: 10.1109/TMM.2023.3325993]

Bas P, Filler T and Pevný T. 2011. "Break our steganographic system": the ins and outs of organizing BOSS//Proceedings of the 13th International Comference on Information Hiding. Prague, Czech Republic: Springer: 59-70 [DOI: 10.1007/978-3-642-24178-9_5]

Bas P and Furon T. 2017. Image database of bows-2 [DB/OL]. [2024-04-27]. https://doi.org/10.17632/kb3ngxfmjw.1

Cao X C, Du L, Wei X X, Meng D and Guo X J. 2016. High capacity reversible data hiding in encrypted images by patch-level sparse representation. IEEE Transactions on Cybernetics, 46(5): 1132-1143 [DOI: 10.1109/tcyb.2015.2423678]

Celik M U, Sharma G and Tekalp A M. 2006. Lossless watermarking for image authentication: a new framework and an implementation. IEEE Transactions on Image Processing, 15(4): 1042-1049 [DOI: 10.1109/tip.2005.863053]

Celik M U, Sharma G, Tekalp A M and Saber E. 2005. Lossless generalized-LSB data embedding. IEEE Transactions on Image Processing, 14(2): 253-266 [DOI: 10.1109/tip.2004.840686]

Chen F, Yuan Y, He H J, Tian M and Tai H M. 2021. Multi-MSB compression based reversible data hiding scheme in encrypted images. IEEE Transactions on Circuits and Systems for Video Technology, 31(3): 905-916 [DOI: 10.1109/tcsvt.2020.2992817]

Chen K M, Guan Q X, Zhang W M and Yu N H. 2023. Reversible data hiding in encrypted images based on binary symmetric channel model and polar code. IEEE Transactions on Dependable and Secure Computing, 20(6): 4519-4535 [DOI: 10.1109/TDSC.2022.3228385]

Dalal M and Juneja M. 2021. A survey on information hiding using video steganography. Artificial Intelligence Review, 54(8): 5831-5895 [DOI: 10.1007/s10462-021-09968-0]

Fridrich J, Goljan M and Du R. 2002. Lossless data embedding—new paradigm in digital watermarking. EURASIP Journal on Advances in Signal Processing, 2002: #986842 [DOI: 10.1155/s1110865702000537]

Gao G Y, Zhang L P, Lin Y, Tong S K and Yuan C S. 2023. High-performance reversible data hiding in encrypted images with adaptive Huffman code. Digital Signal Processing, 133: #103870 [DOI: 10.1016/j.dsp.2022.103870]

Gao H, Zhang X P and Gao T G. 2024. Hierarchical reversible data hiding in encrypted images based on multiple linear regressions and multiple bits prediction. Multimedia Tools and Applications, 83(3): 8757-8783 [DOI: 10.1007/s11042-023-15939-0]

Gao X Y, Pan Z B, Gao E D and Fan G J. 2020. Reversible data hiding for high dynamic range images using two-dimensional prediction-error histogram of the second time prediction. Signal Processing, 173: #107579 [DOI: 10.1016/j.sigpro.2020.107579]

Hong W, Chen T S and Wu H Y. 2012. An improved reversible data hiding in encrypted images using side match. IEEE Signal Processing Letters, 19(4): 199-202 [DOI: 10.1109/lsp.2012.2187334]

Jia Y J, Yin Z X, Zhang X P and Luo Y L. 2019. Reversible data hiding based on reducing invalid shifting of pixels in histogram shifting. Signal Processing, 163: 238-246 [DOI: 10.1016/j.sigpro.2019.05.020]

Kim H J, Sachnev V, Shi Y Q, Nam J and Choo H G. 2008. A novel difference expansion transform for reversible data embedding. IEEE Transactions on Information Forensics and Security, 3(3): 456-465 [DOI: 10.1109/TIFS.2008.924600]

Ma K D, Zhang W M, Zhao X F, Yu N H and Li F H. 2013. Reversible data hiding in encrypted images by reserving room before encryption. IEEE Transactions on Information Forensics and Security, 8(3): 553-562 [DOI: 10.1109/tifs.2013.2248725]

Mohammadi A, Nakhkash M and Akhaee M A. 2020. A high-capacity reversible data hiding in encrypted images employing local difference predictor. IEEE Transactions on Circuits and Systems for Video Technology, 30(8): 2366-2376 [DOI: 10.1109/tcsvt.2020]

Ni Z C, Shi Y Q, Ansari N and Su W. 2006. Reversible data hiding. IEEE Transactions on Circuits and Systems for Video Technology, 16(3): 354-362 [DOI: 10.1109/tcsvt.2006.869964]

Ou B, Yin Z X and Xiang S J. 2022. Overview of reversible data hiding in plaintext image. Journal of Image and Graphics, 27(1): 111-124 (欧博, 殷赵霞, 项世军. 2022. 明文图像可逆信息隐藏综述. 中国图象图形学报, 27(1): 111-124) [DOI: 10.11834/jig.210384]

Ou B and Zhao Y. 2020. High capacity reversible data hiding based on multiple histograms modification. IEEE Transactions on Circuits and Systems for Video Technology, 30(8): 2329-2342 [DOI: 10.1109/tcsvt.2019.2921812]

Puech W, Chaumont M and Strauss O. 2008. A reversible data hiding method for encrypted images//Proceedings Volume 6819, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X. San Jose, USA: SPIE: 534-542 [DOI: 10.1117/12.766754]

Puteaux P and Puech W. 2018. An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images. IEEE Transactions on Information Forensics and Security, 13(7): 1670-1681 [DOI: 10.1109/tifs.2018.2799381]

Puyang Y, Yin Z X and Qian Z X. 2018. Reversible data hiding in encrypted images with two-MSB prediction//Proceedings of 2018 IEEE International Workshop on Information Forensics and Security. Hong Kong, China: IEEE: 1-7 [DOI: 10.1109/wifs.2018.8630785]

Qian Z X, Zhou H, Zhang X P and Zhang W M. 2018. Separable reversible data hiding in encrypted JPEG bitstreams. IEEE Transactions on Dependable and Secure Computing, 15(6): 1055-1067 [DOI: 10.1109/tdsc.2016.2634161]

She X M, Du Y, Ma W J and Yin Z X. 2022. Reversible data hiding in encrypted images based on pixel prediction and block labeling. Journal of Computer Research and Development, 59(9): 2089-2100 (佘晓萌, 杜洋, 马文静, 殷赵霞. 2022. 基于像素预测和块标记的图像密文可逆信息隐藏. 计算机研究与发展, 59(9): 2089-2100) [DOI: 10.7544/issn1000-1239.20210495]

Shi Y Q, Li X L, Zhang X P, Wu H T and Ma B. 2016. Reversible data hiding: advances in the past two decades. IEEE Access, 4: 3210-3237 [DOI: 10.1109/access.2016.2573308]

Tian J. 2003. Reversible data embedding using a difference expansion. IEEE Transactions on Circuits and Systems for Video Technology, 13(8): 890-896 [DOI: 10.1109/tcsvt.2003.815962]

Weinberger M J, Seroussi G and Sapiro G. 2000. The LOCO-I lossless image compression algorithm: principles and standardization into JPEG-LS. IEEE Transactions on Image Processing, 9(8): 1309-1324 [DOI: 10.1109/83.855427]

Wu Y Q, Guo Y T, Tang J, Luo B and Yin Z X. 2021. Reversible data hiding in encrypted images using adaptive Huffman encoding strategy. Chinese Journal of Computers, 44(4): 846-858 (吴友情, 郭玉堂, 汤进, 罗斌, 殷赵霞. 2021. 基于自适应哈夫曼编码的密文可逆信息隐藏算法. 计算机学报, 44(4): 846-858) [DOI: 10.11897/SP.J.1016.2021.00846]

Wu Y Q, Ma W J, Yin Z X, Peng Y Y and Zhang X P. 2022a. Reversible data hiding in encrypted image based on bit-plane compression of prediction error. Journal on Communications, 43(8): 219-230

（吴友情，马文静，殷赵霞，彭银银，张新鹏. 2022a. 基于预测误差位平面压缩的密文图像可逆信息隐藏. 通信学报，43(8)：219-230）[DOI：10.11959/j.issn.1000-436x.2022149]

Wu Y Q，Xiang Y Z，Guo Y T，Tang J and Yin Z X. 2020. An improved reversible data hiding in encrypted images using parametric binary tree labeling. IEEE Transactions on Multimedia，22(8)：1929-1938 [DOI：10.1109/tmm.2019.2952979]

Wu Y Q，Zhang R L，Tang J and Yin Z X. 2022b. Reversible data hiding in encrypted images based on joint fixed-length coding and Huffman coding. Journal of Image and Graphics，27(1)：277-288（吴友情，张睿灵，汤进，殷赵霞. 2022b. 定长编码和哈夫曼编码的密文域可逆信息隐藏. 中国图象图形学报，27(1)：277-288）[DOI：10.11834/jig.200363]

Xiang S J and Li Z H. 2017. Reversible audio data hiding algorithm using noncausal prediction of alterable orders. EURASIP Journal on Audio，Speech，and Music Processing，2017(1)：#4 [DOI：10.1186/s13636-017-0101-9]

Xu S Y，Horng J H，Chang C C and Chang C C. 2023. Reversible data hiding with hierarchical block variable length coding for cloud security. IEEE Transactions on Dependable and Secure Computing，20(5)：4199-4213 [DOI：10.1109/tdsc.2022.3219843]

Yao Y，Wang K，Chang Q and Weng S W. 2024. Reversible data hiding in encrypted images using global compression of zero-valued high bit-planes and block rearrangement. IEEE Transactions on Multimedia，26：3701-3714 [DOI：10.1109/tmm.2023.3314975]

Yi S and Zhou Y C. 2017. Binary-block embedding for reversible data hiding in encrypted images. Signal Processing，133：40-51 [DOI：10.1016/j.sigpro.2016.10.017]

Yin Z X，Peng Y Y and Xiang Y Z. 2022. Reversible data hiding in encrypted images based on pixel prediction and bit-plane compression. IEEE Transactions on Dependable and Secure Computing，19(2)：992-1002 [DOI：10.1109/tdsc.2020.3019490]

Yin Z X，Xiang Y Z and Zhang X P. 2020. Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding. IEEE Transactions on Multimedia，22(4)：874-884 [DOI：10.1109/tmm.2019.2936314]

Yu C Q，Zhang X Q，Zhang X P，Li G X and Tang Z J. 2022. Reversible data hiding with hierarchical embedding for encrypted images. IEEE Transactions on Circuits and Systems for Video Technology，32(2)：451-466 [DOI：10.1109/tcsvt.2021.3062947]

Zhang R，Lu C J and Liu J Y. 2019. A high capacity reversible data hiding scheme for encrypted covers based on histogram shifting. Journal of Information Security and Applications，47：199-207 [DOI：10.1016/j.jisa.2019.05.005]

Zhang W M，Hu X C，Li X L and Yu N H. 2013. Recursive histogram modification：establishing equivalency between reversible data hiding and lossless data compression. IEEE Transactions on Image Processing，22(7)：2775-2785 [DOI：10.1109/tip.2013.2257814]

Zhang X P. 2011. Reversible data hiding in encrypted image. IEEE Signal Processing Letters，18(4)：255-258 [DOI：10.1109/lsp.2011.2114651]

Zhang X P. 2012. Separable reversible data hiding in encrypted image. IEEE Transactions on Information Forensics and Security，7(2)：826-832 [DOI：10.1109/tifs.2011.2176120]

Zhang X P. 2013. Reversible data hiding with optimal value transfer. IEEE Transactions on Multimedia，15(2)：316-325 [DOI：10.1109/tmm.2012.2229262]

Zhang X P and Yin Z X. 2017. Data hiding in multimedia. Chinese Journal of Nature，39(2)：87-95（张新鹏，殷赵霞. 2017. 多媒体信息隐藏技术. 自然杂志，39(2)：87-95）[DOI：10.3969/j.issn.0253-9608.2017.02.002]

Zhou H，Chen K J，Zhang W M and Yu N H. 2022. 3D mesh steganography and steganalysis：review and prospect. Journal of Image and Graphics，27(1)：150-162（周航，陈可江，张卫明，俞能海. 2022. 3D 网格隐写与隐写分析回顾与展望. 中国图象图形学报，27(1)：150-162）[DOI：10.11834/jig.210371]

Zhou X，Wu F H，Chen Z L and Ren S. 2021. All bit planes reversible data hiding for images with high-embedding-rate in ciphertext field. Journal of Image and Graphics，26(5)：1147-1156（周旭，吴福虎，陈志立，任帅. 2021. 密文域高嵌入率图像全位面可逆数据隐藏. 中国图象图形学报，26(5)：1147-1156）[DOI：10.11834/jig.200365]

作者简介

陈振宇，男，硕士研究生，主要研究方向为信息隐藏。E-mail：71255904035@stu.ecnu.edu.cn

殷赵霞，通信作者，女，教授，博士生导师，主要研究方向为信息隐藏、多媒体与AI安全。E-mail：zxyin@cee.ecnu.edu.cn

占鸿渐，男，专任副研究员，主要研究方向为图像处理与模式识别。E-mail：hjzhan@cee.ecnu.edu.cn

吕淑静，女，专任研究员，主要研究方向为文本图像检测与识别、机器视觉和机器学习。E-mail：sjlv@cs.ecnu.edu.cn

胡孟晗，男，副教授，博士生导师，主要研究方向为面向康复医疗的智能信息处理。E-mail：mhhu@ce.ecnu.edu.cn