•信息工程•

DOI:10.15961/j.jsuese.202201128

本刊网刊

差分编码和块压缩的密文域可逆信息隐藏算法

葛国庆[1], 葛　斌[1], 夏晨星[1,2], 王智盟[1]

(1.安徽理工大学 计算机科学与工程学院, 安徽 淮南 232001; 2.安徽璞华大数据技术有限公司, 安徽 淮南 232001)

摘　要: 随着数字信息与云存储技术的发展与成熟, 密文域可逆信息隐藏算法正逐渐成为通信传输中数据隐私保护的研究热点。如何根据不同载体图像像素的分布特征, 对局部区域内像素进行自适应识别编码, 实现对载体更彻底的压缩以提升嵌入容量仍具有较大挑战。本文针对密文域可逆信息隐藏算法因载体图像冗余空间压缩不充分而导致嵌入容量较低的问题, 提出一种基于差分编码和块压缩的密文域可逆信息隐藏算法。首先, 根据自然图像局部区域内像素强相关性邻位作差, 并基于块内最大差值对差值图像矩阵进行分类和自适应编码, 同时设计分块置乱和块内像素扩散加密机制保证图像信息安全。然后, 将自适应编码结果在对应的密文图像块上进行标记, 压缩冗余空间。最后, 通过位替换嵌入秘密信息。不同于其他算法, 本算法对差分编码后的图像进行比特位重排列, 从密文图像像素最低有效位开始, 标记差值像素的符号位, 其余各位面依次标记最小差值比特位。由于加密操作与自适应编码的可逆性, 合法接收者可实现对原始明文图像的无损重构和秘密信息的无误提取。实验结果表明, 与现有的几类算法相比, 本文提出的算法具有更高的嵌入率和更好的安全性, 在BOSSbase和BOWS–2两个数据集上的平均嵌入率达到3.027 位/像素和2.937 位/像素, 在测试图像上平均嵌入率也均提高了0.57 位/像素以上。

关键词: 可逆信息隐藏; 密文域; 隐私保护; 差分编码; 块压缩

中图分类号: TP309　　**文献标志码:** A　　**文章编号:** 2096-3246(2024)04-0307-09

随着云存储技术的兴起与成熟, 更多用户选择将数据上传至云端储存, 在提供各项便捷的同时, 对其中数据安全[1–2]和用户隐私[3–4]保护提出了更高的要求。基于密文图像的可逆信息隐藏算法(RDHEI)可为云存储过程中的数据传输提供可靠的安全保障[5–7]。不同于传统的明文域信息隐藏算法[8–10], RDHEI将秘密信息嵌入加密后的图像, 不仅能够无损地恢复原始图像与提取秘密信息, 载体图像与秘密信息在信息传输过程中的安全性也能够得到很好的保证, 这对载体图像本身的重要内容信息保护具有很大意义[11–13]。

目前, 许多性能较好的RDHEI算法被相继提出, 可将其大致分为两类[14]: 加密前预留空间(RRBE)[15–22]和加密后腾出空间(VRAE)[23–27]。VRAE方法中, 数据隐藏者通过修改加密像素值以嵌入附加信息。由于加密后图像的信息熵已趋向最大化, 原始明文图像像素间的空间相关性无法保留, 所以在嵌入容量上此类算法上限较低。而为了使RDHEI算法在其应用领域更具现实价值, 对隐藏信息量就提出更高的要求。由此, 在嵌入率上有着更大优势的RRBE算法逐渐成为了研究热点。这类算法通过分析原始图像的特征, 利用图像像素间的相关性来预留空间用作附加信息嵌入。相较于VRAE类算法, RRBE算法能在安全性、可逆性和高嵌入率上达到更好的平衡, 本文主要基于此类框架展开研究。Ma等[15]首次提出基于RRBE框架的算法, 其主要思想是在加密前将原始图

收稿日期:2022 – 10 – 18　　**修回日期:**2022 – 12 – 31　　**网络出版日期:**2023 – 07 – 28

基金项目:安徽理工大学研究生创新基金项目(2022CX2123); 国家自然科学基金项目(62102003); 国家重大专项(2020YFB1314103); 安徽省自然科学基金项目(2108085QF258); 安徽省高等学校自然科学研究项目(KJ2020A0299); 安徽理工大学青年科学研究基金重点项目(QN2019102)

作者简介:葛　斌(1975—), 男, 教授. 研究方向: 信息安全; 信息隐藏. E-mail: ggqx12@163.com

像的部分像素最低有效位(LSB)嵌入另一部分像素来预留空间,而后加密自然图像,并在数据隐藏者一端通过位替换的方式嵌入附加信息。Huang等[16]提出的嵌入思想与Ma等[15]类似,但在对块间像素相关性的利用上有了新进展。在RDHEI早期的发展中,只在LSB上嵌入信息的算法都难以达到一个较好的嵌入容量。Puteaux等[17]提出基于最高有效位(MSB)预测的RDHEI算法,充分利用了图像像素间相关性,较之先前的在LSB上做嵌入的算法,该算法在嵌入率上有了明显提升,但仅在MSB上做比特位替换而无法有效利用其他比特位,因此仍无法达到一个理想的嵌入效果。Yi等[18]在Puteaux算法上进行了改进,提出双MSB预测方法,在嵌入容量上有了一定的突破。Yi等[19]提出基于分块隐藏的方法,在对原始图像加密前,将每一个像素块转换为8个比特平面的二进制块,并在其中的一些平面中嵌入信息。Chen等[20]使用一种扩展的游程编码技术压缩MSB,相较于分块隐藏方法[19],该算法对比特位重新排列,进一步提升了嵌入容量。Qin等[21]使用可逆整数变换的方法移除图像像素的LSBs,为附加信息预留空间。Yi等[22]将原始图像分块,并使用参数二叉树标记预测误差,然后将秘密信息嵌入预测误差较小的像素,相较于先前的算法,该算法在嵌入容量上更具优势。

上述RDHEI算法都实现了较好的嵌入性能,但是没有在安全性上有一个较好的平衡。许多研究者使用生成的伪随机序列对原始图像像素进行异或加密,加密后的像素值会显著变化,但像素相对位置并未改变,此类加密已被证明不能抵抗唯密文攻击[15−18]。Yi等[19]结合动力学公式,构造混沌映射Logistic-sine函数生成伪随机序列,加密效果在之前研究[15−18]的基础上有所提升,但仍然没有置乱原始像素值的位置,无法起到良好的扩散效果。在Yi等[22]研究中,加密过程采取置乱后扩散的方式,加密程度已有了较大的提升,但像素间的相关性遭到破坏,嵌入率难以在RRBE框架下达到最优效果。

为在实现较高嵌入容量的同时兼顾载体图像的安全性,本文提出了一种基于差分编码和块压缩的密文域可逆信息隐藏算法。加密阶段,对原始明文图像进行分块置乱和块内扩散的加密处理,在保证图像信息安全的同时,极大地保留块间像素的相关性。同时,在块间像素差分后进行自适应编码,从而根据不同的块类型最大化地压缩冗余空间,以提升嵌入容量。编码和加密的可逆性使得原始图像和秘密信息能够无损恢复与提取,实现完全可逆。

1 本文算法

本文提出的基于差分编码和块压缩的密文域可逆信息隐藏主要分为4个部分:预处理、块级压缩、信息嵌入、图像恢复与信息提取。提出的RDHEI算法具体框架如图1所示。

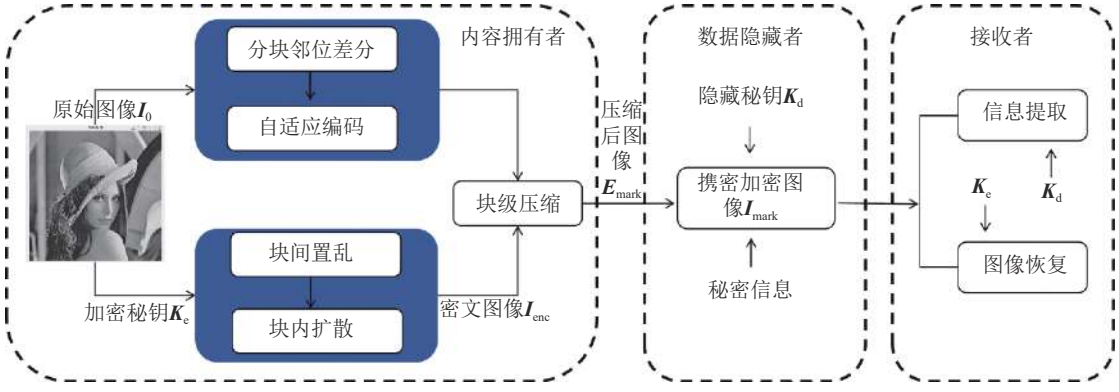


图 1 RDHEI算法框架

Fig. 1 Framework of proposed RDHEI scheme

1.1 预处理

预处理阶段主要执行3部分操作:分块邻位差分、自适应编码和图像加密。

1.1.1 分块邻位差分

大小为$M\times N$的原始图像$\boldsymbol{I}_0$,以块为单位经过相邻像素差分后得到差值像素矩阵$\boldsymbol{I}_{\mathrm{dif}}$。图2为块内作差模型,以块大小$s$=2为例,总分块数$m=(M\times N)/(s\times s)$,像素$x_{i,j}$及其3个相邻像素$x_{i,\,j+1}$、$x_{i+1,\,j}$和$x_{i+1,\,j+1}$构成一个2×2的像素块。经过以$x_{i,\,j}$为参考像素的相邻像素作差后,可以得到相对应的差值像素块,具体步骤为:

$$\begin{cases} x'_{i+1,j} = x_{i+1,j+1} - x_{i+1,j}, \\ x'_{i+1,j+1} = x_{i,j+1} - x_{i+1,j+1}, \\ x'_{i,j+1} = x_{i,j} - x_{i,j+1} \end{cases} \tag{1}$$

式中,$x_{i,j}$为原始像素块中的参考像素,差分过程不改变其像素值。

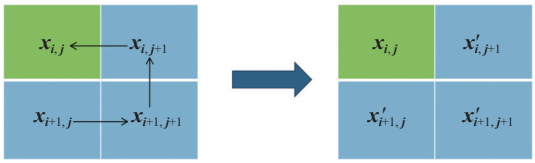


图 2　块内作差的模型

Fig. 2　Model of subtraction in the block

差分处理之后，除各块参考像素外，差值图像的像素值集中在很小的范围内，扩大了块内像素的相似性，并为接下来的自适应编码创造了条件。表1为块编码示例，以丽娜图像（s=2）的块分布为例，最大差值$d_{\max} \le 15$的块占总块数85%以上，由此能有更多的比特位用来嵌入信息。块内差分后，$\boldsymbol{I}_{\mathrm{dif}}$各块内差值像素会出现正负值的情况，为保证算法的完全可逆性，需要记录3个差值像素的符号位，本算法中使用“1”标记正值，“0”标记负值的形式来保留3个差值像素的正负情况，具体将在第1.4节介绍。

表 1　丽娜图像的块编码示例

Tab. 1　Example of block encoding for Lena image

类型编号	最大差值$d_{\max}$区间	数量	频率	码字
1	0或1	2910	0.0444	101110
2	(1,3]	13860	0.2115	100
3	(3,7]	24182	0.3690	0
4	(7,15]	14952	0.2281	11
5	(15,31]	6640	0.1013	1010
6	(31,255]	2992	0.0457	10110

1.1.2　自适应编码

为能够根据不同自然图像差值块的块分布情况动态调整块标签分配，以实现出现频率高的块匹配到较短编码，从而达到高压缩率的目的，本算法利用哈夫曼编码技术[28]，依据字符出现概率构造平均长度最短的码字，完成对所有块的标记。图3为哈夫曼编码示例。

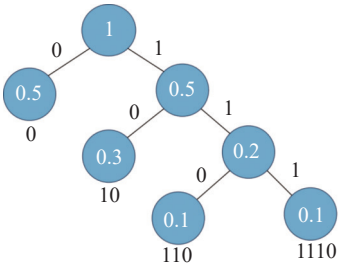


图 3　哈夫曼编码示例

Fig. 3　Example of Huffman coding

原始图像完成邻位差分之后，依次按从左到右、从上到下的顺序遍历各个小块，将块内差值像素取绝对值；但对于最大差值大于31的图像块，需用不少于6个比特位来记录其差值，无多余空间保留参考像素及符号位，所以将这一类定义为不可嵌入块，标记为类型6。按照这一规则，将所有图像块分成6种类型，并根据上述编码思想，预先定义6种不同长度的块标签码字，根据不同纹理图像的各种块出现频率的不同，自适应为各种类型块分配标签码字，从而实现频率更高的块所对应的标签码字长度更短，以达到提升嵌入率的目的。以丽娜图像为例，按照上述差分规则，有24 182个图像块属于类型 3，所占比例最大，因此，对于类型 3的块标签自适应地定义为“0”，所占比特位数最短。随着块类型所占比例的减小，块标签的长度在增加，如此动态分配能留出最大嵌入空间。

对于类型6这一类不可嵌入块，同样需要有相应的标签码字标记，以在嵌入阶段准确识别。为保证完全可逆性，须记录下不可嵌入块中被替换的比特位，记作$\boldsymbol{A}_{\mathrm{U1}}$；为了在后续操作中能直接定位到附加信息的开始嵌入位置，在判断块类型时需记录不可嵌入块数量A_{U2}，以丽娜图像为例，将A_{U2}转换成二进制作为保留信息所占比特位数，计算方式如下：

$$A_{\mathrm{U2}} = \mathrm{lb}\,\frac{M \times N}{s \times s} \tag{2}$$

当s=2时，对于一幅512×512的图像，额外的16个比特位即可记录所有的块数。且经过差值处理后，像素值更为集中，差值像素大于31的分块仅占极少的一部分，所以$\boldsymbol{A}_{\mathrm{U1}}$的长度较短，不会占用过多的预留空间。

1.1.3　图像加密

对$\boldsymbol{I}_0$分块作差生成块编码的同时，内容拥有者可根据加密密钥$\boldsymbol{K}_{\mathrm{e}}$生成$M \times N$的伪随机数矩阵$\boldsymbol{H}$，并将其转换成二进制序列，转换公式如下：

$$h^k_{i,j,p} = \left\lfloor \frac{X^k_{i,j,p}}{2^{k-1}} \right\rfloor \bmod 2,\ k = 1,2,\cdots,8 \tag{3}$$

式中：$h^k_{i,j,p}$为差值像素的二进制形式，$1 \le i \le M, 1 \le j \le N, p \in [1,m]$；$X^k_{i,j,p}$为伪随机值的二进制形式。

根据生成的随机数对分块后的图像进行位置置乱，并以块为单位将像素值的k个有效位与伪随机数矩阵二进制序列对应位置两两异或，其加密后的值$e^k_{i,j,p}$为：

$$e^k_{i,j,p} = X^k_{i,j,p} \oplus h^k_{i,j,p},\ k = 1,2,\cdots,8 \tag{4}$$

式中，$\oplus$为按位异或。

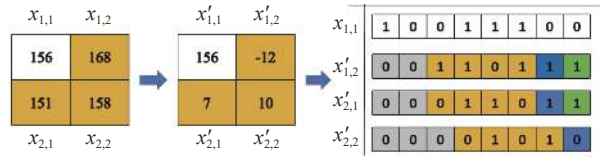
1.2　块级压缩

这一部分有3类信息需要在内容拥有者一端嵌入：块标签、编码规则及辅助信息。块内非参考像素的比特位在以位替换的方式完成重排列后，产生大量的冗余空间以嵌入附加信息。

1.2.1　块标签嵌入

为准确识别每一个块所属类别，块标签编码必

须提前嵌入到每一个块中。图4为所提算法示例。将差值像素块图4(b)通过式(3)转换成二进制序列，然后根据自适应编码过程，将当前块的块标签嵌入到图4(c)中绿色区域。



(a) 原始像素块 (b) 差值像素块 (c) 差值像素块

图 4 所提出算法的示例

Fig. 4 Example of the proposed scheme

嵌入过程如下：

1)若当前块属于类型1～5，作为参考像素$x_{1,1}^k$的8个比特位不做改变。其他3个像素，从最低位开始，依次嵌入已生成的块标签，如原始像素值(图4(a))经邻位差值处理得到差值块类型(4(b))，此时块内最大差值绝对值为12，属于类型 4，对应块标签为“11”，标签嵌入后为图4(c)中的绿色区域。

2)对于属于类型6的不可嵌入块，在对它们的第k个比特位进行块标签替换之前，用$\boldsymbol{A}_{\mathrm{U1}}$记录将要被替换的比特位，其长度$A_{\mathrm{U1_len}}$为：

$$A_{\mathrm{U1\_len}} = B_l \times B_{l\_\mathrm{len}} \tag{5}$$

式中，B_l为各类块数量，B_{l_len}为类型l(l=1,2,⋯,6)对应的编码长度，此处l=6。

1.2.2 差值与符号位嵌入

为了后续操作中能够无损重构图像，需在嵌入标签的密文图像块中，记录非参考像素的差值符号位和有效比特位。图4(c)中，根据差值块非参考像素的正负情况，在块标签后面依次嵌入3个符号位(蓝色区域)及差值像素的最短有效比特位(黄色区域)，高位的灰色区域就是当前块的留出空间。例如：$x_{2,2}$=10，对应的8位二进制00001010，则最短有效位为后4位1010。由此，一个块内的预留空间V_p^k可由下式得出：

$$V_p^k = 32 - C_l - 3 \times (D_l + 1) \tag{6}$$

式中，D_l为3个差值像素中的最大差值有效比特位数，C_l为对应块标记码字。接下来就可求得该图像的总预留空间V为：

$$V = \sum_{p=1}^{m} V_p^k \tag{7}$$

在块标签、差值及相应符号位嵌入完成后，即可得到标记图像。

1.2.3 块标签与辅助信息嵌入

在本文算法下，对于一幅给定大小为$M \times N$的原始图像，块标签映射规则和不可嵌入块的数量是确定的。图5为6种块编码示例，浅色区域是以二进制形式代表的类型1～6块标签的长度，后面浅蓝色区域为对应的块标签码字。最终的自适应编码规则二进制序列Q就可用来表示类型1～6，公式如下：

$$|Q| = \sum_{l=1}^{6} (t_l + n_l) \tag{8}$$

式中，t_l为需要记录的块标签编码长度，n_l为块标签编码长度对应的二进制形式。

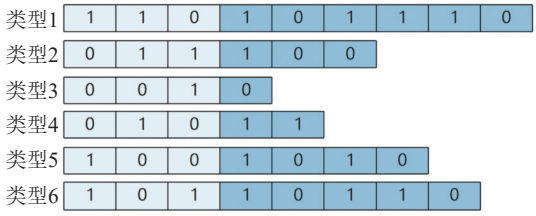


图 5 6种块编码规则的示例

Fig. 5 Example of coding map representation of six block types

以丽娜图像为例，生成的码字长度$|Q|$为39位。在本文算法中，对于不同图像，不同块对应的标签编码可能不同，但映射总长度$|Q|$保持不变。对于已留出空间的加密图像块，按序遍历的前两块，即$p \in \{1,2\}$的块中非参考像素可用来保存块标签映射规则，记作$\boldsymbol{A}_{\mathrm{U3}}$。现将$\boldsymbol{A}_{\mathrm{U1}}$、$A_{\mathrm{U2}}$、$\boldsymbol{A}_{\mathrm{U3}}$统一记作$\boldsymbol{A}_{\mathrm{U}}$，且其各自比特位数都可由已嵌入编码规则得出。从第3个块开始，在预留空间中嵌入$\boldsymbol{A}_{\mathrm{U}}$，详细嵌入过程如下。

输入：标记图像，块大小$s \times s$，辅助信息$\boldsymbol{A}_{\mathrm{U}}$。

输出：嵌入所有辅助信息的标记加密图像$\boldsymbol{E}_{\mathrm{mark}}$。

步骤1：将编码规则嵌入之后的图像矩阵分成$s \times s$的图像块。

步骤2：在前两个块中提取嵌入的块标签映射规则，识别后面的块类型，如果属于类型6，不做$\boldsymbol{A}_{\mathrm{U}}$信息的嵌入。否则，按照块标签类型，利用式(2)将图像块转换成二进制的位矩阵。然后，在块内已腾出空间中，通过位替换嵌入$\boldsymbol{A}_{\mathrm{U}}$信息。

步骤3：重复步骤2，直到$\boldsymbol{A}_{\mathrm{U}}$中所有信息被嵌入加密图像矩阵。

所有辅助信息完成嵌入后，数据隐藏者将二进制图像重新转换成十进制图像，得到最终的标记加密图像$\boldsymbol{E}_{\mathrm{mark}}$。所以，该算法的净腾出空间$T_{\mathrm{room}}$及嵌入率$R$可由式(9)～(10)得出：

$$T_{\mathrm{room}} = V - |\boldsymbol{A}_{\mathrm{U}}| \tag{9}$$

$$R = T_{\mathrm{room}} / (M \times N) \tag{10}$$

式(9)～(10)中，$|\boldsymbol{A}_{\mathrm{U}}|$为$\boldsymbol{A}_{\mathrm{U}}$所占的空间。

1.3　附加信息嵌入

标记编码的图像经重排列后，可腾出连续空间。信息隐藏者在接收到标记加密图像$\boldsymbol{E}_{\text{mark}}$后，首先将其转换成8位二进制图像，并通过提取哈夫曼映射规则编码，得到类型1～6的码字；然后，利用式（2）、（6）计算出$\boldsymbol{A}_{\text{U}}$的长度并识别每块内的符号位与差值像素位，从而得到开始嵌入位置。数据隐藏者可根据拥有的数据隐藏密钥$\boldsymbol{K}_{\text{d}}$加密附加信息，有序地将附加信息通过位替换嵌入每块的预留空间，最终得到携密加密图像$\boldsymbol{I}_{\text{mark}}$。

1.4　信息提取和图像恢复

由于在图像加密和嵌入附加信息阶段，所用的密钥不同，所以根据相应的密钥，合法接收者可以根据自身权限完成以下工作：1）根据数据隐藏密钥$\boldsymbol{K}_{\text{d}}$完成附加信息的提取；2）利用图像加密密钥$\boldsymbol{K}_{\text{e}}$完成原始图像的重构。

1.4.1　附加信息提取

接收者在提取附加信息之前，先将携密密文图像$\boldsymbol{I}_{\text{mark}}$划分成不重叠的大小为$s\times s$的图像块，并在逐块扫描过程中用式（3）转换成二进制矩阵，提取第1块和第2块中的编码信息。通过这些信息，就可得到附加信息的开始嵌入位置。按照编码规则和相应的块标签指示，提取出预留空间中的信息。最后使用密钥$\boldsymbol{K}_{\text{d}}$依次解密，即可获得正确的附加信息。

1.4.2　图像恢复

合法接收者可由$\boldsymbol{K}_{\text{e}}$生成伪随机矩阵$\boldsymbol{H}$，对$\boldsymbol{I}_{\text{mark}}$分块后，进行块间置乱恢复与块内参考像素异或，就可得到位置像素$x_{i,j}$的原始值，再根据块标签编码规则，确定当前块类型、不可嵌入块数量及其码字长度，即可无误提取不可嵌入块中被块编码替换的A_{U2}。而后根据块编码所属的块类型，确定符号位差值有效比特位数，就能够无损重构原始图像。具体步骤如下。

1）若当前块属于类型1～5，在编码之后，依次提取3位表示差值像素正负的符号位与相应长度的差值位，并将差值等分3份，转换成十进制差值。根据符号位指示，块标签后的3个比特分别对应差值块中$x_{i,j+1}$、$x_{i+1,j}$和$x_{i+1,j+1}$像素的正负，若为1，则差值像素为正值；否则，差值像素为负值。最后，将恢复的差值像素填回块中，并在块内用式（1）逆向作差，即可恢复原始像素值。

2）若当前块属于类型6，则按照类型6对应的块标签长度依次提取A_{U2}中的比特位以替换不可嵌入块中的块标签位，转换成十进制像素值后，通过与伪随机矩阵$\boldsymbol{H}$中相应位置的随机数异或，从而恢复原始像素值。

重复步骤1）和2），处理完所有块后，即可得到无损的原始明文图像$\boldsymbol{I}_0$。

2　实验和总结

为验证本文所提算法性能，仿真实验利用图6所示的5幅灰度图像，从安全性、可逆性、嵌入容量3个方面分析本文算法所实现的结果，并在BOSSbase、BOWS–2这两个经典数据集上进行测试，由时间复杂度的分析说明本文算法的实践性。不同的实验在尽可能保证对比算法一致的前提下，考虑到某些算法中没有其他实验的数据，因此选择另外的同类算法进行对比。

(a) 男人　(b) 飞机　(c) 丽娜　(d) 辣椒　(e) 狒狒

图 6　5幅灰度测试图像

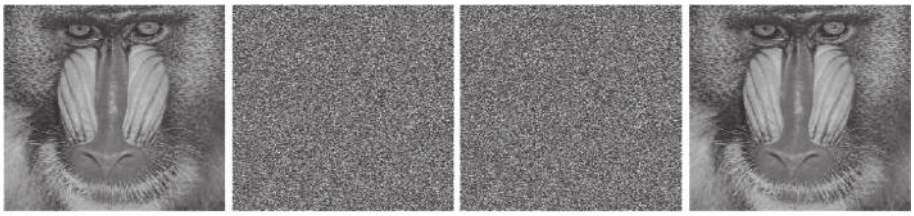
Fig. 6　Five original grayscale test images

2.1　安全性

1）密钥空间。足够大的密钥空间能够有效抵制暴力破解等攻击手段。本文所采用的加密方法中，加密密钥$\boldsymbol{K}_{\text{e}}$用来实现载体图像块间置乱及块内扩散的操作。根据第1.1.3节中的分块规则，首先在m个图像块之间进行置乱操作，块置乱后可能出现的组合结果的数量为$P_{\text{S1}}=m!$。再经过相同的伪随机数$X_{i,j}$（$X_{i,j}\in[0,255]$）进行块内的扩散操作，块内扩散可能出现的组合数量为$P_{\text{S2}}=256^m$。即加密阶段的密文空间为$P_{\text{S}}=P_{\text{S1}}\times P_{\text{S2}}=m!\times 256^m$。对于512×512的载体图像，当分块大小为2时，总块数m=65 536，密钥空间总大小为$65\,536!\times 256^{65\,536}$，由此足以抵抗暴力破解等攻击手段[29]。

2）视觉质量。图7为狒狒图像的测试结果。图7中：图7（a）为原始狒狒图像；图7（b）为原始狒狒图像加密而得的密文图像；图7（c）为嵌入辅助信息的密文图像，即标记密文图像；图7（d）为重构图像。原始图像与密文图像、标记密文图像之间的视觉差异越大，

则算法安全性越高。如图7所示，原始图像（图7（a））与密文图像（图7（b））、标记图像（图7（c））之间几乎不存在视觉相似性，由此可知该算法从视觉角度有较好的安全性。

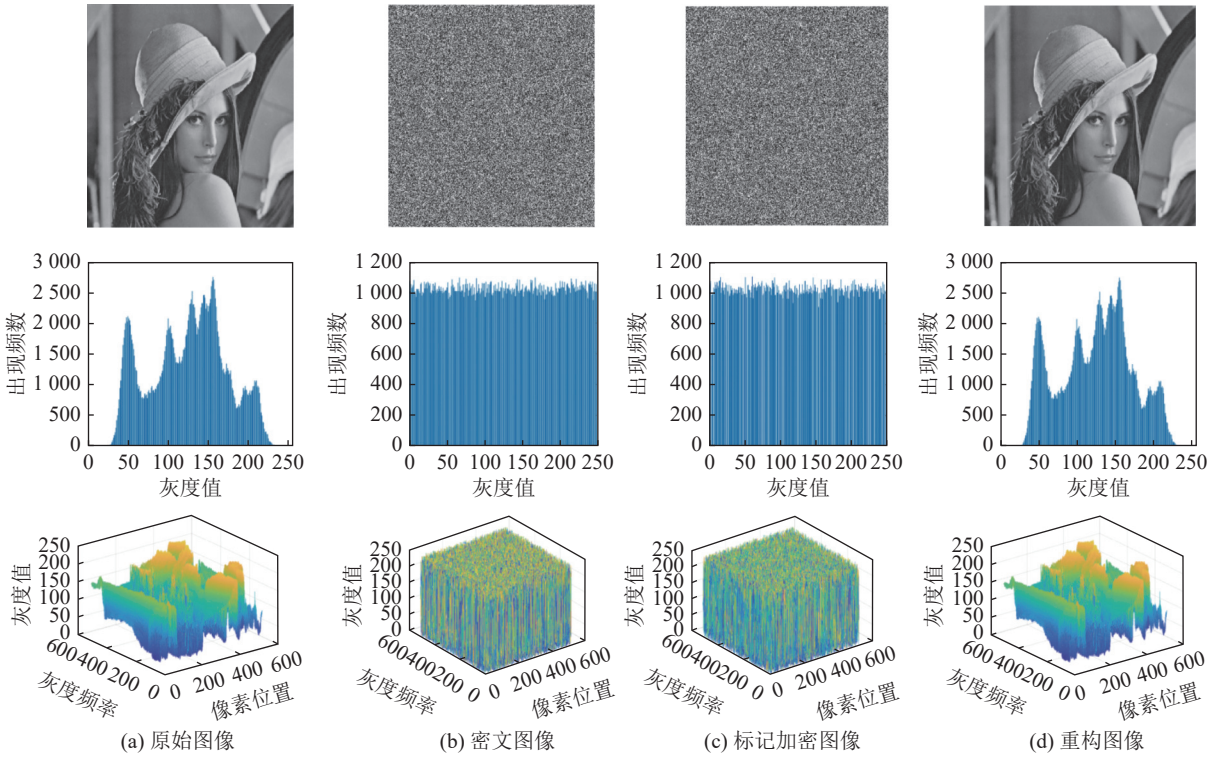


(a) 原始图像 (b) 密文图像 (c) 标记图像 (d) 重构图像

图 7 本文算法对狒狒图像的实验结果

Fig. 7 Results of applying the proposed algorithm to Baboon image

3）直方图分布。图8为丽娜的原始图像（图8（a））、密文图像（图8（b））、标记加密图像（图8（c））和重构图像（图8（d））的图片、直方图和3维图。图8（a）和（d）直方图呈现相同分布，包含了原始图像的特征信息。加密后图像所对应的直方图（图8（b）、（c））及3维图分布均匀而平缓，窃取者难以通过分析像素分布规律得到图像的特征信息，从而实现了本文算法在图像传输过程中具有较强的加密效果，保证了安全性。



(a) 原始图像 (b) 密文图像 (c) 标记加密图像 (d) 重构图像

图 8 丽娜的原始图像、密文图像、标记加密图像、重构图像的直方图及3维视角下的像素分布

Fig. 8 Gray histograms and 3D view of pixel value of original image, encrypted image, marked encrypted image and recovered image

4）相关参数。表2为5幅加密后图像的PSNR和不同阶段的图像信息熵。如表2所示，原始图像与密文图像之间的PSNR不超过10 dB，较低的峰值信噪比值表明加密前后图像之间的差异性大，从而证明本文加密方法具有较优的效果。信息熵是估计加密图像随机性的重要指标，其定义为：

$$H(I)=\frac{1}{N'}\sum_{n=1}^{N'}p(n)\lg\frac{1}{p(n)} \tag{11}$$

式中，$p(n)$为灰度n的概率，N'为灰度的范围值。

表 2 不同图像的PSNR和信息熵

Tab. 2 PSNR and entropy for different images

测试图像	原始图像与加密图像的PSNR/dB	信息熵		
		原始图像	加密图像	标记加密图像
男人	9.1263	7.1926	7.9991	7.9884
飞机	8.0232	6.7025	7.9993	7.9913
丽娜	9.2390	7.4451	7.9993	7.9973
辣椒	8.4598	7.5715	7.9992	7.9929
狒狒	9.5343	7.3579	7.9993	7.9767

由表2可以看出，密文图像和标记加密图像的信息熵都非常接近于8（极限为8）。这说明从统计结果的角度分析，本算法也具有较优的安全性。

2.2 可逆性

为验证本文算法的可逆性，根据均方误差（MSE，记为S_{MSE}）与结构相似度（SSIM，记为S_{SSIM}）的值来判断原始图像$\boldsymbol{G}$和重构图像$\boldsymbol{Z}$之间的差异。MSE与SSIM计算方法由式（12）、（13）给出：

$$S_{\mathrm{SSIM}}(\boldsymbol{G},\boldsymbol{Z})=\frac{2U_GU_Z+C_1}{U_G^2+U_Z^2+C_1}\cdot\frac{2\sigma_G\sigma_Z+C_2}{\sigma_G^2+\sigma_Z^2+C_2}\cdot\frac{\sigma_{G,Z}+C_3}{\sigma_G\sigma_Z+C_3} \tag{12}$$

$$S_{\mathrm{MSE}}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(G_{i,j}-Z_{i,j})^2 \tag{13}$$

式（12）～（13）中，U_G、U_Z为图像$\boldsymbol{G}$和$\boldsymbol{Z}$的均值，σ_G、σ_Z为图像$\boldsymbol{G}$和$\boldsymbol{Z}$的标准差，$\sigma_{G,Z}$为图像$\boldsymbol{G}$和$\boldsymbol{Z}$的协方差，C_1、C_2、C_3为常数，$G_{i,j}$、$Z_{i,j}$分别为图像$\boldsymbol{G}$和$\boldsymbol{Z}$的元素。

具体地，重构图像的MSE越接近于0，SSIM越接近于1，其失真程度就越低。表3为本文算法在两类常用数据集上的MSE和SSIM。由表3可知，两者均是0和1，即重构图像与原始图像之间不存在失真。由此可知本文算法具有完全可逆性。

表 3　MSE和SSIM在两个标准图像数据集上的测试结果

Tab. 3　Test results for MSE and SSIM on two standard image datasets

数据集	S_{MSE}	S_{SSIM}
BOSSbase	0	1
BOWS–2	0	1

2.3 嵌入性能

在保证本文算法的安全性和可逆性后，嵌入容量（ER）就成了判断性能好坏的关键指标。以5幅标准灰度图像为例，将本文与在5幅图像上有较优嵌入性能的同类算法进行对比，结果如表4所示。分析表4数据可知，本文算法嵌入率均高于同类文献。

表 4　不同算法下5幅图像的最大嵌入率对比

Tab. 4　Comparison of the maximum ER of five images under different algorithms

测试图像	Yi等[19]	Gao等[24]	Qin等[21]	Chen等[20]	Celik等[23]	本文算法
男人	1.574	1.564	1.602	1.678	2.216	2.262
飞机	2.163	2.037	2.089	2.337	2.472	2.815
丽娜	1.765	1.711	1.838	1.944	2.513	2.562
辣椒	1.730	1.561	1.821	1.871	2.425	2.430
狒狒	0.402	0.813	0.483	0.535	0.861	0.991

为进一步说明本文算法具有较好的性能，选取在BOSSbase与BOWS–2两个图像数据集上有最优平均嵌入率的3类方法进行定量对比，并同时对最大、最小嵌入率进行对比分析，结果如表5所示。由表5可知，相较于其他3类算法，本文算法在嵌入率上均有显著提升。

表 5　两个数据集上不同算法之间嵌入率的比较

Tab. 5　Comparison of the ER between different algorithms on two datasets

数据集	嵌入情况	嵌入率/(位·像素$^{-1}$)			
		Yi等[19]	Qin等[21]	Liu等[25]	本文算法
BOSSbase	最高	4.427	3.487	2.435	5.146
	最低	0.437	0.187	0.085	0.458
	平均	2.457	2.208	1.791	3.027
BOWS–2	最高	4.315	3.426	2.427	4.962
	最低	0.187	0.134	0.133	0.376
	平均	2.271	2.061	1.682	2.937

2.4 时间复杂度

时间复杂度分析能客观地验证所提算法在实践上的优势，进行图像加密、数据嵌入和数据提取及图像恢复这3个阶段的理论分析和运行时间的测算，将本文算法与3类有相似编码压缩与信息嵌入模块的算法进行对比，如表6所示。

由于在图像加密过程中，运行时间只与载体图像分块的块数m相关，因此，这个部分的时间复杂度为O(m)。信息嵌入阶段包含了基于块间和块内的作差编码及压缩部分，此时，时间复杂度有所增加，平均情况下达5.563 5 s，但相比于文献[20–21,25]，在运行时间上，仍然有较大优势。最后，在信息提取及图像恢复阶段，本文算法运行时间均低于3类经典算法，表明本文所提算法在时间性能上也有着较大优势。

表 6 平均运行时间对比

Tab. 6 Average running times comparison

算法	运行时间/s		
	图像加密	信息嵌入	信息提取与图像恢复
Qin等[21]	1.2352	8.7951	10.0573
Chen等[20]	0.9114	6.2647	7.4725
Liu等[25]	1.3149	8.4583	9.7549
本文算法	0.8221	5.5635	7.1728

3 结 语

针对密文域隐藏算法图像冗余利用率不足的问题，提出了一种基于差分编码和块级压缩的密文域图像可逆信息隐藏算法。在保证安全性的前提下，采用块内邻接像素作差，增大像素间相关性，使像素值分布更为集中。在此基础上，利用哈夫曼技术自适应生成块标签编码，标记差值块并重排列差值比特位实现更高的嵌入容量。最后，仿真实验的结果也表明了本文算法在安全性、可逆性及嵌入容量上的优势。

所提算法在有多种辅助信息需提前嵌入载体图像中，虽然占用的空间有限，但带有图像特征的辅助信息在传输过程中仍存在安全风险。后续工作将设计一定方案，减少辅助信息量，保证安全性的同时提升有效载荷

参考文献：

[1] Yu Mingji,Yao Heng,Qin Chuan.Reversible data hiding in encrypted images without additional information transmission[J].Signal Processing:Image Communication,2022,105:116696.

[2] Wang Xingyuan,Feng Le,Zhao Hongyu.Fast image encryption algorithm based on parallel computing system[J].Information Sciences,2019,486:340–358.

[3] Wang Xingyuan,Yang Jingjing.A privacy image encryption algorithm based on piecewise coupled map lattice with multi dynamic coupling coefficient[J].Information Sciences,2021,569:217–240.

[4] Chang C C,Hsiao J Y,Chan C S.Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy[J].Pattern Recognition,2003,36(7):1583–1595.

[5] Zhang Fan,Pan Zhigeng,Cao Kui,et al.The upper and lower bounds of the information-hiding capacity of digital images [J].Information Sciences,2008,178(14):2950–2959.

[6] Gao Guangyong,Tong Shikun,Xia Zhihua,et al.Reversible data hiding with automatic contrast enhancement for medical images[J].Signal Processing,2021,178:107817.

[7] Zhang Tiancong,Weng Shaowei,Wu Zhijie,et al.Adaptive encoding based lossless data hiding method for VQ compressed images using tabu search[J].Information Sciences,2022,602:128–142.

[8] She Xiaomeng,Du Yang,Ma Wenjing,et al.Reversible data hiding in encrypted images based on pixel prediction and block label[J].Journal of Computer Research and Development,2022,59(9):2089–2100.[余晓萌,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.]

[9] 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.

[10] Ding Wenjia,Zhang Huyin,Reulke R,et al.Reversible image data hiding based on scalable difference expansion[J].Pattern Recognition Letters,2022,159:116–124.

[11] Bai Yongqiang,Jiang Gangyi,Zhu Zhongjie,et al.Reversible data hiding scheme for high dynamic range images based on multiple prediction error expansion[J].Signal Processing:Image Communication,2021,91:116084.

[12] Weng Shaowei,Tan Wenlong,Ou Bo,et al.Reversible data hiding method for multi-histogram point selection based on improved crisscross optimization algorithm[J].Information Sciences,2021,549:13–33.

[13] Xiong Zhiyong,Wang Jiangqing.Reversible information hiding of color images based on shift of difference histogram[J].Journal of Sichuan University(Engineering Science Edition),2011,43(3):81–89.[熊志勇,王江晴.基于差值直方图平移的彩色图像可逆信息隐藏[J].四川大学学报(工程科学版),2011,43(3):81–89.]

[14] Puteaux P,Ong S,Wong K,et al.A survey of reversible data hiding in encrypted images—The first 12 years[J].Journal of Visual Communication and Image Representation,2021,77:103085.

[15] Ma Kede,Zhang Weiming,Zhao Xianfeng,et al.Reversible data hiding in encrypted images by reserving room before encryption[J].IEEE Transactions on Information Forensics and Security,2013,8(3):553–562.

[16] Huang Fangjun,Huang Jiwu,Shi Yunqing.New framework for reversible data hiding in encrypted domain[J].IEEE Transactions on Information Forensics and Security,2016,11(12):2777–2789.

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

[18] Yi Puyang,Yin Zhaoxia,Qian Zhenxing.Reversible data hiding in encrypted images with two-MSB prediction[C]//Proceedings of the 2018 IEEE International Workshop on Information Forensics and Security(WIFS).HongKong:IEEE,2018:1–7.

[19] Yi Shuang,Zhou Yicong.Binary-block embedding for reversible data hiding in encrypted images[J].Signal Pro-

cessing,2017,133:40–51.
[20] Chen Kaimeng,Chang C C.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.
[21] Qin Chuan,Qian Xiaokang,Hong W,et al.An efficient coding scheme for reversible data hiding in encrypted image with redundancy transfer[J].Information Sciences,2019,487:176–192.
[22] 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.
[23] Celik M U,Sharma G,Tekalp A M,et al.Reversible data hiding[C]//Proceedings of the International Conference on Image Processing.Rochester:IEEE,2002,2:157–160.
[24] Gao Kai,Horng Jihwei,Chang Chinchen.High-capacity reversible data hiding in encrypted images based on adaptive block encoding[J].Journal of Visual Communication and Image Representation,2022,84:103481.
[25] Liu Zilong,Pun Chiman.Reversible data-hiding in encrypted images by redundant space transfer[J].Information Sciences,2018,433/434:188–203.
[26] Ren Honglin,Lu Wei,Chen Bing.Reversible data hiding in encrypted binary images by pixel prediction[J].Signal Processing,2019,165:268–277.
[27] Wang Xu,Chang C C,Lin C C.Reversible data hiding in encrypted images with block-based adaptive MSB encoding[J].Information Sciences,2021,567:375–394.
[28] Wu Youqing,Guo Yutang,Tang Jin,et al.Reversible data hiding in encrypted images using adaptive huffman encoding strategy[J].Chinese Journal of Computers,2021,44(4):846–858.[吴友情,郭玉堂,汤进,等.基于自适应哈夫曼编码的密文可逆信息隐藏算法[J].计算机学报,2021,44(4):846–858.]
[29] Tang Zhenjun,Zhang Xianquan,Zhang Shichao.Robust perceptual image hashing based on ring partition and NMF[J].IEEE Transactions on Knowledge and Data Engineering,2014,26(3):711–724.

Reversible Data Hiding Algorithm in Encrypted Images with Difference Encoding and Block Compression

GE Guoqing[1], *GE Bin*[1], *XIA Chenxing*[1,2], *WANG Zhimeng*[1]

(1.School of Computer Sci. and Eng., Anhui Univ. of Sci. and Technol., Huainan 232001, China;
2.Anhui Purvar Bigdata Technol. Co., Ltd., Huainan 232001, China)

Abstract: With the development of digital information and cloud-computing technology toward maturity, reversible hiding of data in encrypted images is gradually becoming an area of intensive research for protection of data privacy in communications. Nonetheless, notable challenges still exist regarding achieving greater compression of carriers to enhance embedding capacity by adaptive-recognition coding of pixels in local areas based on the distribution characteristics of pixels in different cover images. To address the problem of the low embedding capacity of reversible information hiding due to insufficient utilization of redundant space in carrier images, herein, a cipher-text domain-reversible data-hiding algorithm is proposed based on difference coding and block compression. First, the difference-image matrix is classified and adaptively coded according to the maximum difference value within the block based on the differences of strong-correlation neighbors in local areas of the natural image. At the same time, the original image is chunked, disrupting the order between blocks and diffusing pixels within blocks to ensure the security of the image information. Then, according to the result of the adaptive coding of the difference-pixel blocks, the redundant space is compressed on the corresponding encrypted image blocks, and the secret data is finally embedded by bit replacement. In contrast to previous algorithms , this approach rearranges the bits of the differential-encoded image, starting from the least-significant bit of the cipher-text image pixel, marking the sign bit of the differential pixel, and marking the least-significant differential bit in each of the remaining planes in turn. Due to the reversibility of the encryption operation and adaptive coding, a legitimate receiver can achieve lossless reconstruction of the original plain-text image and error-free extraction of the secret data. The experimental results show that the proposed algorithm has a greater embedding rate and better security than several existing algorithms. The average embedding rates were found to be 3.027 and 2.937 bpp for the BOSSbase and BOWS–2 datasets, respectively, and this was also improved by more than 0.57 bpp on classical test images.

Key words: reversible data hiding; encrypted domain; privacy protection; difference encoding; block compression

（编辑　吴芝明）

引用格式：Ge Guoqing,Ge Bin,Xia Chenxing,et al.Reversible data hiding algorithm in encrypted images with difference encoding and block compression[J].Advanced Engineering Sciences,2024,56(4):307–315.[葛国庆,葛斌,夏晨星,等.差分编码和块压缩的密文域可逆信息隐藏算法[J].工程科学与技术,2024,56(4):307–315.]