基于分组密码的加密域图像可逆信息隐藏算法研究与实现

王星垚[1] 丁海洋[1]
WANG Xingyao DING Haiyang

摘 要 提出一种基于 SM4 分组密码和直方图平移的信息隐藏算法的加密域可逆信息隐藏算法，首先使用 SM4 分组密码对载体图像进行预处理，然后使用基于分块和密钥的直方图平移算法在加密后的载体图像中嵌入秘密信息；提取时先将图像进行分块处理，接收密钥后提取秘密信息，进行直方图逆向平移，最后进行解密操作。经过实验验证，算法符合实际应用中对嵌入秘密信息后图像的要求，并且能够正确提取秘密信息、解密恢复原始载体图像，在数据的隐蔽传输和个人信息保护领域具有较好的应用前景。

关键词 分组密码；信息隐藏；直方图平移；SM4；加密域信息隐藏

doi：10.3969/j.issn.1672-9528.2024.09.044

0 引言

随着计算机和网络技术的发展，数字化媒体信息已成为人们生活中的重要组成部分，并在网络上迅速传播。因此，在互联网带来进步的同时，如何在开放的网络环境下确保数字化媒体信息的安全传输和保管，以及防止敏感信息被篡改和窃取，成为数据信息安全领域的热点研究问题。

基于密码学的加密技术是保护数据安全的常用手段，通过将明文加密成密文再进行传输，使非法拦截者无法获取机密信息[1]。信息隐藏技术则利用人类感觉器官对数字信号的感觉冗余，将消息隐藏在普通消息中，不影响普通消息的特征和使用价值，同时提高数据安全性[2]。早期的信息隐藏技术主要是不可逆的，载体图像在提取后不可恢复，影响了信息隐藏在部分领域的应用[3]，因此可逆信息隐藏的算法和应用成为信息安全领域的研究热点。

随着科技的发展，人们将加密技术和可逆信息隐藏技术进行结合，将秘密信息嵌入加密图像中。加密域图像的可逆信息隐藏（reversible data hiding in encrypted image，RDHEI）技术使秘密信息得到了充分保护，实现了信息的隐蔽传输和隐藏。

肖文乾等人[4]提出一种基于加法同态以及 MSB 的密文域信息隐藏方法，对载体图像和秘密信息图像同样采用同态加密，并在自嵌入和秘密信息嵌入阶段都采用了高位嵌入，实现信息隐藏。王紫琪[5]提出结合压缩感知技术和混沌理念的可分离算法，利用离散小波变换和 Logistic 置乱进行预处理，再采用混沌压缩感知进行加密和信息嵌入，预处理的置乱大幅提升了安全性。邓光纬[6]通过对图像像素值分类在加密前预留空间，生成较多用于隐藏信息的空间，之后采用像素差分扩展算法实现信息隐藏。随着同态密码的应用，张敏情等人[7]利用同态密码和公钥信息隐藏技术，直接在密文上进行部分操作，保护数据安全。

传统的基于直方图的信息隐藏算法在图像处理过程中只修改了图像的像素值，不会改变图像的结构，因此对于许多图像处理攻击具有较强的抗打击性。但是当直方图平移信息隐藏应用于加密后的图像时，往往会产生溢出，导致隐藏后的图像质量受到较大的影响，并且加密后图像零点提取也有一定难度。

基于以上情况，本文提出了一种基于分组密码的加密域图像可逆信息隐藏（reversible data hiding in encrypted image based on block cipher，RDHEI -BC）算法。在加密前预处理时，引入分块与信息隐藏密钥的思想。为了防止加密后直方图平移像素溢出，导致图像质量受损，利用信息隐藏密钥生成像素统计数组。使用 SM4 分组密码对载体图像进行加密，然后使用基于分块和密钥的直方图平移算法，在加密后的载体图像中嵌入秘密信息。其在数据的隐蔽传输和个人信息保护领域具有较好的应用前景。

1. 北京印刷学院信息工程学院 北京 102600
[基金项目] 北京市教委科研计划（KM202010015009、KM202110015004、KM202310015002）；北京市高等教育学会项目（MS2022093、20240014）；北京市数字教育研究课题（20240022）；北京印刷学院思政重点项目（20240053）；北京印刷学院博士启动金项目（27170120003/020、27170122006）；北京印刷学院科研创新团队项目（Eb202101）；北京印刷学院科研基础研究一般项目（Ec202201）；北京印刷学院青年卓越项目（Ea202411）

1 已有工作

1.1 SM4 分组密码算法

SM4 分组密码是采用 32 轮非线性迭代结构的分组密码算法，非平衡 Feistel 网络结构，分组长度为 128 bit。SM4 算法由两部分组成：初始变量算法和密钥扩展算法，并且加密和解密的算法结构相同，只是轮密钥的使用顺序相反。

（1）初始变量算法：SM4 分组密码算法的加密算法包含 32 次迭代运算以及 1 次反序变换，首先将输入的明文分组，每组 128 bit，将每组明文输入记为 X_0,X_1,X_2,X_3，之后将明文分组进行轮密钥参与下的轮函数运算，轮函数主要由合成置换 T 构成，也就是 X_0 与合成置换所得到的结果进行异或。合成置换主要由线性变换 L 和非线性变换 τ 组成，非线性变换 τ 由四个并行的 S 盒构成，SM4 分组密码算法的 S 盒是一个八进八出的布尔函数，作为唯一的非线性结构，主要起到混淆的作用。线性变换 L 是将四个 S 盒的输出作为输入，将分别进行循环左移 0、2、10、18、24 之后的数据进行异或运算，起到了扩散的作用，最终得到的结果作为 T 运算的输出 [8]。

（2）密钥扩展算法：上述加密算法中的轮密钥是加密密钥经过密钥扩展算法得到的。参与密钥扩展算法的主要有两个常数，分别为系统参数 FK 和固定参数 CK。首先，将加密密钥分为四个字，并分别与系统参数进行异或，得到的结果进行 T 变换，也就是对合成置换 T 中的 L 函数的循环移位的位数进行修改 [9]。

SM4 分组密码算法经过密码工作者的测试，能够抵抗所有的密码攻击，易于在软硬件上实现，并且运行速度相对较快，因此本次实验采用了 SM4 分组密码进行具体实现。

1.2 直方图平移可逆信息隐藏算法

基于直方图的信息隐藏算法主要通过修改原始图像峰点和零点之间的直方图来进行信息嵌入。

在嵌入数据之前，首先选取出图像的峰点 P 和最低点 Zero，进行直方图平移。若峰点大于最低点，则将像素值大于 Zero 且小于 P 的点的像素减 1，空出 P-1 的位置；若峰点小于最低点，则将峰点和最低点之间的直方图向右平移 1 位，空出的位置用于秘密信息的嵌入。之后进行信息嵌入，当秘密信息为 0 时，嵌入到像素值为 P 的点；当秘密信息为 1 时，嵌入到像素值为 P+1(P-1) 的点。

提取时，首先先寻找灰度值为 P 和 P+1（或 P-1）的点，当灰度值为 P 时，提取秘密信息 0，当灰度值为 P+1（或 P-1）时，提取秘密信息为 1。最后恢复图像，若峰点 P 大于最低点，则将峰点和最低点之间的直方图向右平移 1 位；若峰点 P 小于最低点，则将峰点和最低点之间的直方图向左平移 1 位。至此，直方图恢复到与原图完全一致，实现了可逆的信息隐藏 [10]。

2 基于分组密码的加密域可逆信息隐藏算法

2.1 基于直方图平移的可逆信息隐藏算法

本文提出了一种基于分块和密钥的直方图平移可逆信息隐藏（reversible data hiding of histogram translation based on block and key，RDHHT -BK）算法。该算法首先将图像划分成多个大小相等的块，并将每个块的直方图进行平移，从而留出嵌入秘密信息的位置。这样做的好处是，嵌入的信息不会对图像的像素值直接进行修改，因此可以避免因为改变像素值而导致的视觉质量损失。相对于传统的基于 LSB（最低有效位）的信息隐藏算法，具有更高的隐藏容量和更好的安全性。同时，采用密钥进行信息隐藏和提取，使得只有持有密钥的人才能成功提取嵌入的秘密信息，提高了算法的安全性。

在算法实现中，需要根据秘密信息的大小和图像分块的大小来确定嵌入容量，并根据密钥生成每个分块的直方图平移值，从而进行信息嵌入。而在信息提取时，则需要根据像素值来提取嵌入的秘密信息。RDHHT -BK 算法的流程图如图 1 所示。

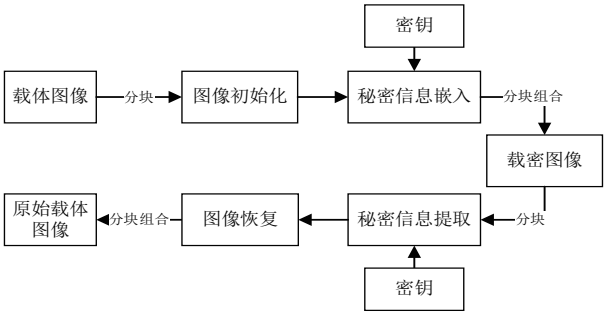


图 1 RDHHT -BK 算法流程图

本文中 RDHHT -BK 算法具体实现流程如下。

（1）图像的初始化：首先对原始图像进行分块，对每个分块分别进行像素扫描，选取出直方图的峰点 p 和最低点 z。

（2）秘密信息嵌入：首先根据密钥，进行直方图平移。平移规则如下。引入密钥 k，计算平移点。当密钥输入正确时，进行信息嵌入操作。如果峰点 p 大于最低点 z，则将像素值大于最低点且小于峰点的点的像素减 k，空出像素值为 p-k 的位置，也就是将峰点和最低点之间的直方图向左平移 k 位；若峰点 p 小于最低点，则将像素值大于峰点且小于零点的点的像素值加 k，空出像素值为 p+k 的位置，也就是将峰点和最低点之间的直方图向右平移 k 位，空出的像素值为 p+k 或 p-k 的位置用于秘密信息的嵌入。

之后将秘密信息的值转化为信息位，由秘密信息的值决定嵌入位置，嵌入规则如下。

当秘密信息为 0 时，在像素值为 p 的点中嵌入秘密信息；当秘密信息为 1 时，在像素值为 p+k（p-k）的点嵌入信息，

当秘密信息嵌入后，原始图像灰度值为 p 的点由于嵌入秘密信息为 0，还在峰点的位置，另一部分由于嵌入的秘密信息为 1，位置改变到了 p-k（或 p+k）的位置。

嵌入秘密信息后的分块进行组合，得到信息隐藏后的图像。

（3）秘密信息提取：将图像按照相同规则进行分块。对于每一分块寻找灰度值为 p 和 p+k（或 p-k）的点，根据像素值判断嵌入的秘密信息位。当灰度值为 p 时，提取秘密信息 0；当灰度值为 p+k（或 p-k）时，提取秘密信息为 1。同时，验证提取出的秘密信息是否与原始秘密信息相等。

（4）恢复原始图像，若峰点大于最低点，则将像素值大于最低点且小于峰点的点的像素加 k，也就是将峰点和最低点之间的直方图向右平移 k 位；若峰点小于最低点，则将像素值大于峰点且小于最低点的点的像素减 k，将峰点和最低点之间的直方图向左平移 k 位。将分块组合，得到原始载体图像。恢复图像后通过计算峰值信噪比和归一化系数值，来确定是否准确提取秘密信息、成功恢复图像。

2.2 基于分组密码的加密域可逆信息隐藏算法

本文提出的 RDHEI -BC 算法在实现信息隐藏之前，对载体图像进行预处理，使用 SM4 分组密码对原始载体图像进行加密。接着，使用基于直方图平移的信息隐藏算法对加密的载体图像进行隐藏操作。

算法包括四个部分：分组密码加密过程、信息隐藏过程、信息提取过程、分组密码解密过程。加密算法和信息隐藏算法的主要实现步骤如下。

（1）将载体图像读入程序中，并将其转化为一维数组。这样做的主要目的是方便对图像进行后续处理。一维数组可以更容易进行分组、加密等操作，同时也节省了储存空间。

（2）将数组的十进制数据转换成十六进制数据，并进行打包。SM4 算法的输入数据长度必须为 16 个字节，而一般的图像数据长度往往不符合这个要求，因此需要将其转换为符合 SM4 算法要求的数据。这里本文选择将十进制数据转换为十六进制数据，使其长度符合 SM4 算法的要求输入维度。

（3）对上述数据进行 SM4 分组密码加密，得到的一维数组的十六进制数据转换为十进制数据，最后将数组转化为图像文件格式，得到加密后的图像。

（4）对加密后的载体图像分成固定大小的块，同时输入密钥 k。

每个分块依次进行直方图平移算法，根据输入的密钥 k 计算平移点，之后按照 RDHHT-BK 算法设定的平移规则进行直方图的平移，空出部分像素空间，根据秘密信息的不同，选取不同的嵌入位置。秘密信息嵌入后，将每个分块进行组合，得到信息隐藏后的图像。图 2 为 RDHEI-BC 算法的加密和信息隐藏过程。

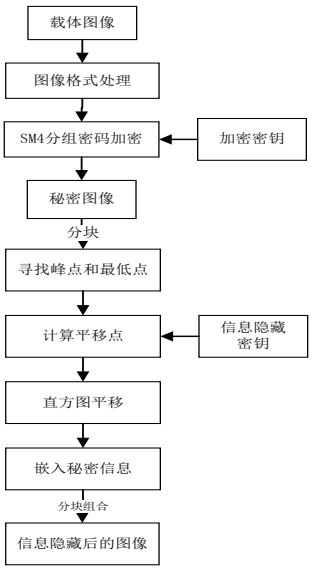


图 2 RDHEI -BC 算法—加密和隐藏

解密算法和信息提取算法的主要步骤如下。

（1）对嵌入秘密信息后的图像分成固定大小的块，同时输入密钥 k。

（2） 对每个分块依次进行直方图平移算法，由输入的密钥计算平移点，图像嵌入秘密信息后，一部分峰点由于嵌入秘密信息为 0，像素保持不变，一部分由于嵌入的秘密信息为 1，变成了平移点的像素值，因此根据图像像素值的不同可以提取不同的秘密信息。之后进行直方图的逆向平移，恢复图像的原始直方图，将每个分块进行组合，得到信息提取后的图像。

（3）将信息提取后的图像转化为一维数组，并将数组的十进制数据转换成十六进制数据，进行打包，使其长度符合 SM4 解密算法的维度要求。

（4）对上述数据进行 SM4 分组密码解密，得到的一维数组的十六进制数据转换为十进制数据，最后将数组转化为图像文件格式，得到解密后的图像。图 3 为 RDHEI -BC 算法的解密和信息提取过程。

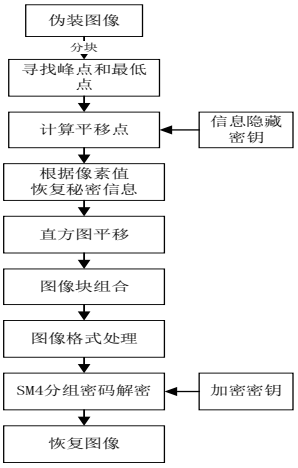


图 3 RDHEI -BC 算法—解密和提取

2.3 本文创新点

现有的基于直方图平移的加密域信息隐藏算法在实现信息隐藏时存在一些问题。

首先是像素溢出问题。由于加密后的图像直方图分布较为分散，平移后在平移点附近可能会出现溢出。为了实现图像的无损恢复并正确提取秘密信息，本文在预处理时首先根据信息隐藏密钥，确定直方图平移的位数及秘密信息的隐藏位置，并记录平移点附近的像素值。

其次是零点的读取难度。为了解决这个问题，本文采用了图像分块的方法。如果原始图像中存在零点，那么每个分块中一定也会包含零点；如果原始图像中不存在零点，那么当其被分割成足够多的部分时，每个分块中都会出现零点，从而确保了算法的可行性。

另外，基于直方图平移的信息隐藏算法并没有密钥的参与，为了提升算法的安全性，本文引入了密钥 k，使用密钥 k 计算直方图平移时的平移点位置，保证信息的安全性。只有在接收方采用相同的密钥 k 进行平移时，才能成功提取秘密信息。

3 实验分析

3.1 算法仿真

本文采用了 256×256 的灰度图像作为载体图像，经过多幅图像的实验，均可以得到良好的效果。本章主要运用图 4 的 Lena、Boat、Couple、Plane 进行实验说明，根据加密后的载体图像的峰点的值而产生的伪随机数作为秘密信息嵌入。实验在 Matlab R2018 系统平台上仿真实现。

首先，利用 SM4 加密算法对图 4 中的四幅图片进行加密，得到加密后的载体图像，如图 5 所示。随后，对这些加密后的载体图像应用 RDHHT-BK 算法，嵌入秘密信息，得到如图 6 所示的图像。接着，从图 6 中提取秘密信息，得到提取信息后的图像，如图 7 所示。最后，对提取秘密信息后的图像使用 SM4 分组密码进行解密，得到如图 8 所示的图像。至此，基于 SM4 分组密码的图像加密域可逆信息隐藏算法基本实现。

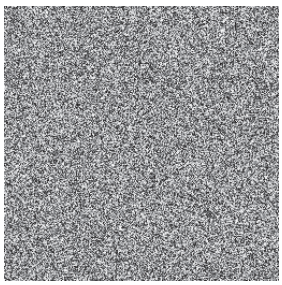
（a）Lena

（b）Boat

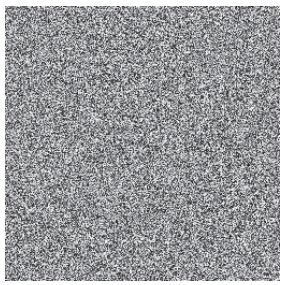
（c）Couple

（d）Plane

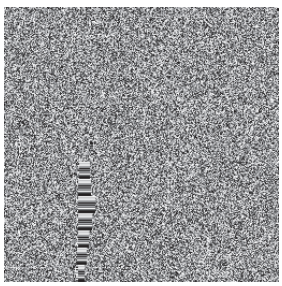
图 4 原始载体图像



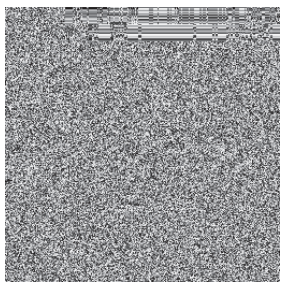
（a）sm4-lena



（b）sm4-Boat

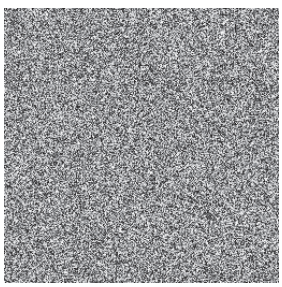


（c）sm4-Couple

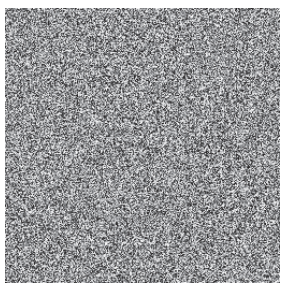


（d）sm4-Plane

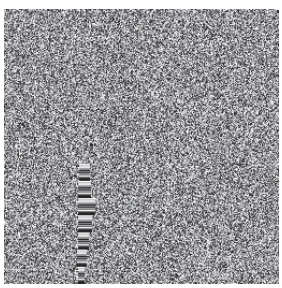
图 5 SM4 分组密码加密后的图像



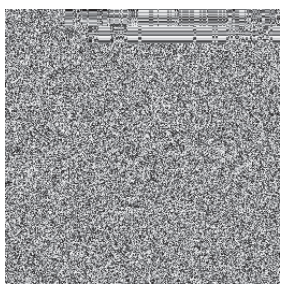
（a）shift-Lena



（b）shift-Boat

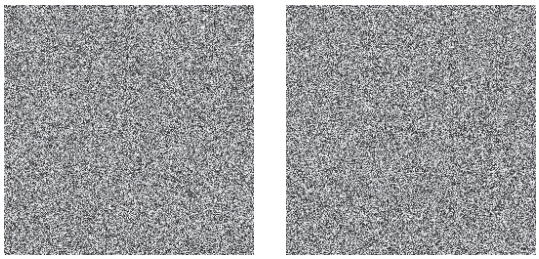


（c）shift-Couple



（d）shift-Plane

图 6 信息隐藏后的图像

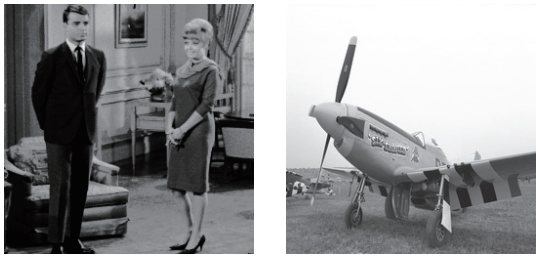


（a）shift_Lena （b）shift_Boat

（c）shift_Couple （d）shift_Plane

图 7 信息提取后的图像

（a）decrypt-Lena （b）decrypt-Boat



（c）decrypt-Couple （d）decrypt-Plane

图 8 SM4 分组密码解密后的图像

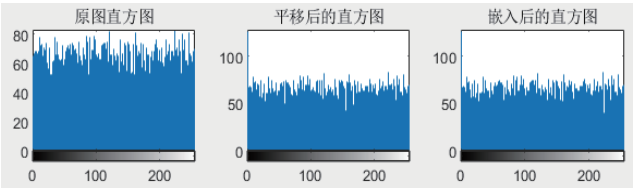
3.2 具体实现

在信息隐藏和提取过程中，需要对每个分块都分别进行处理，以保证秘密信息在整张图像中的均匀分布，避免信息在某些局部区域过于密集，影响图像整体的质量。步骤如下。

（1）在 Lena 加密后的第一分块直方图中，峰点值为 224，最低点值为 0，密钥选择为 1。

（2）因为峰点值大于最低点，所以将像素值在 0 和 224 之间的点向左平移 1 位，空出像素值为 223 的点用于秘密信息的嵌入。

（3）秘密信息嵌入：当秘密信息为 0 时，在像素值为 224 的点中嵌入秘密信息；当秘密信息为 1 时，在像素值为 223 的点嵌入信息。图 9 为分块一信息隐藏直方图变换过程。

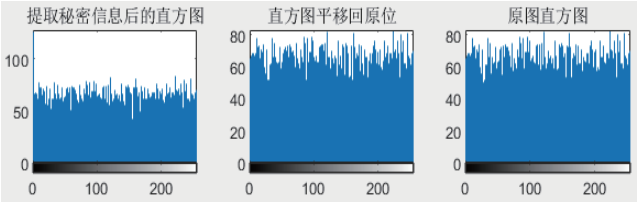


（a）原直方图 （b）平移后直方图 （c）隐藏后直方图

图 9 分块一信息隐藏直方图变换过程

（4）秘密信息提取：灰度值为 224 时，提取秘密信息 0；灰度值为 223 时，提取秘密信息 1。

（5）验证提取出的秘密信息是否与原始秘密信息相等，并恢复原始图像。图 10 为分块一提取秘密信息后、平移后以及原图的直方图，可见本文算法可以正确提取秘密信息，并且恢复图像直方图。



（a）提取后直方图（b）平移恢复原始直方图（c）原直方图

图 10 分块一信息提取直方图变换过程

4 性能分析

本节通过对比原图与加密图像的熵值分析算法的安全性。在算法性能分析模块，先引入归一化系数（NC）分析信息提取算法的正确性以及图像解密的正确性，之后引入峰值信噪比（PSNR）与结构相似性（SSIM）判断算法的可逆性，最后在不可感知性方面与优秀算法进行了对比。

4.1 安全性分析

香农熵是指体系的混乱程度，越乱越大。图像熵则是图像特征的一种统计形式，它反映了图像中平均信息量的多少，从而能够反映图像各像素点的分布复杂程度 [11]。图像的香农熵计算公式为：

$$H(X)=-\sum_{i=1}^{n}p_i\log_2 p_i \tag{1}$$

式中：p_i 为某一事件发生的概率，对数一般取 2 为底，单位为 bit。

表 1 图像的熵值

测试图像	原始图像熵值	加密后图像熵值
Lena	7.568 3	7.989 2
Boat	7.161 2	7.990 5
Couple	6.168 9	7.985 5
Plane	6.390 8	7.976 4

由表1可以看出，加密后图像的熵值相比原图像更接近8。这表明加密后的图像更加复杂，像素值分布更加均匀，因此嵌入秘密信息后，攻击者更难以从中分析出具体数据，从而提高了安全性。

4.2 算法性能分析

4.2.1 正确性

正确性是衡量一个算法性能好坏的重要标准，在加密域信息隐藏算法中，主要是确保秘密信息提取的正确性以及解密后图像是否与原图完全一致（秘密信息提取后图像恢复的正确性）。本文使用归一化系数（NC）验证以上正确性。

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W_{i,j} \bullet W'_{i,j}}{\sum_{i=1}^{M}\sum_{j=1}^{N} (W_{i,j})^2} \quad (2)$$

式中：$W_{i,j}$ 代表原始图像，$W'_{i,j}$ 代表信息提取后的图像，若两者越相似，则NC系数值越接近1。

首先，本文利用NC系数验证秘密信息提取的正确性以及秘密信息提取后图像恢复的正确性。

通过计算信息提取后图像与信息隐藏前图像的归一化系数，NC系数等于1，说明该算法能够做到秘密信息正确提取，并且提取后成功恢复未嵌入信息前的图像，做到了可逆的信息隐藏，如表2所示。

表2 信息提取后的归一化系数

信息隐藏后的图像	NC值
shift_Lena	1
shift_Boat	1
shift_Couple	1
shift_Plane	1

通过计算解密后图像与原始载体图像的归一化系数，NC系数等于1，说明该算法能够在加密图像的基础上，实现可逆信息隐藏，并且成功解密恢复原始载体图像，如表3所示。

表3 解密后的归一化系数

解密后的图像	NC值
decrypt-Lena	1
decrypt-Boat	1
decrypt-Couple	1
decrypt-Plane	1

4.2.2 可逆性

（1）峰值信噪比（PSNR）

对于 $M \bullet N$ 的灰度图像，PSNR的计算公式为：

$$PSNR = 10\log_{10}\frac{255^2}{\frac{1}{M \bullet N}\sum_{i=1}^{M}\sum_{j=1}^{N}(I(i,j)-I'(i,j))^2} \quad (3)$$

式中：M 为灰度图像的长度，N 为灰度图像的宽度，I 为原始灰度图像，I' 为嵌入秘密信息后的载密图像。

（2）结构相似性（SSIM）

SSIM是一种基于感知的模型，用于评估图像质量。它将图像退化视为结构信息的感知变化，同时结合了亮度掩蔽和对比度掩蔽等重要的感知现象，能够更准确地反映人类对图像质量的感知。相比之下，PSNR等方法主要关注图像间的绝对误差，未能充分考虑人类视觉系统对图像质量的实际感知。SSIM的计算公式为：

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (4)$$

式中：x 表示恢复图像，y 表示原始图像，μ_x 为 x 的平均值，μ_y 为 y 的平均值，μ_x^2 为 x 的方差，μ_y^2 为 y 的方差，σ_{xy} 为 x 和 y 的协方差。

本文计算了测试的原始图像与最终解密后的图像之间的PSNR值与SSIM值，如表4所示。四幅图像的PSNR值均为∞，SSIM值均为1，可以得出，当接收方拥有信息提取密钥和解密密钥时，能够恢复原始图像，即本文提出的算法完全可逆。

表4 测试图像的PSNR与SSIM

测试图像	PSNR	SSIM
Lena	∞	1
Boat	∞	1
Couple	∞	1
Plane	∞	1

4.3 算法对比

本文与Zhang等人[12]和Xu等人[13]的方法进行对比。Zhang等人在加密前首先生成一个随机密钥，调用加密算法将原图像与随机密钥进行异或操作，完成加密。之后根据要嵌入的秘密信息修改图像分块内的加密LSB像素，也就是将秘密信息嵌入到图像的最低有效位。该算法的嵌入容量取决于分块大小，分块越小，嵌入容量越高，然而失败的位提取和图像恢复的风险也随着分块变小而上升。并且该算法的单纯异或加密无法抵抗唯密文攻击，算法安全性较低。Xu等人将预测误差技术应用于加密域中，加密前首先对图像进行预测，并用预测误差替代原始像素得到预处理图像。之后对采样像素进行异或加密，对阈值之内非采样像素不加密，阈值之外的非采样像素采用Mod加密。信息嵌入时，采用的是直方图平移和差值扩展技术。该算法能够使加密后的像素值仍保持在规定的范围内，但是一个像素仅能嵌入1 bit信息，嵌入容量较低，并且采样像素仅异或加密会导致信息泄露。

本节主要将三个算法的不可感知性进行对比。不可感知性是指嵌入秘密信息后，秘密信息是否会被观察到也就是图像是否会产生明显变化，是评价信息隐藏算法好坏的最基本属性。

PSNR 不仅可以验证算法的可逆性，由于其可以计算图像的失真情况，还被更多地应用于评价秘密信息嵌入后的不可感知性。在信息隐藏算法中，一般计算原始灰度图和信息隐藏得到的图像的 PSNR 值，用于反映嵌入秘密信息后图像的质量以及秘密信息的不可感知性 [14]。PSNR 的值越大，MSE 的值越小，说明解密后图像越接近原始图像。

表 5 对比了文献 [12] 和文献 [13] 以及本文算法（RDHEI -BC）信息隐藏前后图像的峰值信噪比和均方差。

表 5 信息隐藏后的 PSNR 对比

图像	Lena	Boat	Couple	Plane
文献 [12]	37.971 8	37.911 2	38.104 3	38.022 2
文献 [13]	26.067 7	32.569 0	32.565 6	19.762 6
本文算法	51.832 9	51.914 6	51.631 1	53.397 3

可以看出本文算法的 PSNR 值与文献 [12]、文献 [13] 相比有着显著提升，秘密信息嵌入后不可感知性较高，算法性能得到较大的提升。

综上，本文提出的 RDHEI -BC 算法在不影响载体图像质量的情况下，能够正确地提取秘密信息，并且解密后成功得到原始载体图像。加密算法有效混淆了载体图像的直方图，相邻像素相关性降低，并且信息隐藏算法引入了密钥运算，因此该算法具有较高的安全性，做到了安全性和实用性的平衡。

5 总结

本文研究了加密域信息隐藏算法，将分组密码应用于信息隐藏中。在信息隐藏前，使用 SM4 分组密码加密算法对载体图像进行预处理，提高算法的安全性。接着对图像进行分块，并使用密钥对使用者身份进行验证，对每一分块分别采用基于直方图平移的方法实现信息的隐藏。之后将信息隐藏后的分块利用原分块规则进行组合，得到信息隐藏后的图像。提取时将图像分块，输入密钥计算平移点，采用基于直方图平移的方法实现信息的提取，得到提取后图像，并进行 SM4 解密操作，恢复原始载体图像。实验结果通过峰值信噪比、归一化系数等客观数值的评价，表明该算法可成功嵌入并提取秘密信息，在解密后亦可恢复原始图像，成功实现了图像加密域的可逆信息隐藏。

对于本文的不足之处，在使用加密域信息隐藏技术时，需要注意信息泄露和攻击的问题。在之后的研究中，会加强密码和算法实现的复杂性，避免同一密钥被用于多个信息嵌入过程中，引用相应的加密算法加强对嵌入的秘密信息的保护，并且进行信息检测和提取工作，以防止信息提取不及时或秘密信息提取不完整而导致的信息泄露问题。

参考文献：

[1] 易开祥 . 数字图像加密与数字水印技术研究 [D]. 杭州 : 浙江大学 , 2001.

[2] 陈波 , 谭运猛 , 吴世忠 . 信息隐藏技术综述 [J]. 计算机与数字工程 , 2005(2):21-23+27.

[3] 向娇 . 基于直方图平移的 JPEG 图像加密域可逆信息隐藏算法研究 [D]. 成都 : 西南交通大学 ,2021.

[4] 肖文乾 , 杨高波 , 王德望 , 等 . 基于加法同态加密与多高位嵌入的加密域图像可逆信息隐藏 [J]. 网络与信息安全学报 , 2023, 9(4):121-133.

[5] 王紫琪 . 基于混沌压缩感知的多图像信息隐藏与加密算法 [D]. 北京 : 北京邮电大学 ,2020.

[6] 邓光纬 . 加密前预留空间的加密图像可逆信息隐藏算法研究 [D]. 成都 : 西南交通大学 ,2019.

[7] 张敏情 , 周能 , 刘蒙蒙 , 等 . 同态加密域可逆信息隐藏技术研究 [J]. 信息网络安全 ,2020,20(8):25-36.

[8] 李建立 , 莫燕南 , 粟涛 , 等 . 基于国密算法 SM2、SM3、SM4 的高速混合加密系统硬件设计 [J]. 计算机应用研究 , 2022, 39(9):2818-2825+2831.

[9] 胡禹佳 , 代政一 , 孙兵 .SIMON 算法的差分—线性密码分析 [J]. 信息网络安全 ,2022,22(9):63-75.

[10] 崔炳德 , 辛晨 , 裴祥喜 . 基于直方图平移的安全可逆信息隐藏算法 [J]. 科学技术与工程 ,2019,19(22):215-222.

[11] 肖文乾 , 杨高波 , 王德望 , 等 . 基于加法同态加密与多高位嵌入的加密域图像可逆信息隐藏 [J]. 网络与信息安全学报 , 2023, 9(4):121-133.

[12]ZHANG X.Reversible data hiding in encrypted image[J]. IEEE signal processing letters,2011,18:255-258.

[13]XU D, WANG R.Separable and error-free reversible data hiding in encrypted images[J].Signal processing, 2016,123: 9-21.

[14] 宋畅 . 基于图像加密域的可逆信息隐藏算法研究 [D]. 南京 : 东南大学 ,2020.

【作者简介】

王星垚（2001—），女，河北张家口人，硕士研究生，研究方向：加密域信息隐藏、图像加密。

丁海洋（1979—），通信作者（email: 13810284215@163.com），男，北京人，博士，副教授，研究方向：信息隐藏、数字图像处理等。

（收稿日期：2024-06-20）