

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

肖文乾, 杨高波, 王德望, 夏明

(湖南大学信息科学与工程学院, 湖南 长沙 410082)

摘要: 密文域图像可逆信息隐藏将图像加密和可逆信息隐藏相结合, 可提升图像网络传输的安全性和信息传输效率。然而, 对于密文图像可逆信息隐藏, 常规的逐位流加密会破坏图像的空间相关性, 影响预留嵌入空间。提出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方法, 通过加密预留空间。将原始图像划分为无重叠的块, 同一个块采用相同的密钥进行加法同态加密, 尽可能地将原始图像子块内像素相关性转移到加密后图像对应的子块中。为了提升安全性, 加密后的图像再逐块进行 Arnold 置乱。依据块内像素与预测值之间的差值, 确定该块是否嵌入信息及嵌入容量。对于可嵌入的块, 利用少量的像素低位保存预测差值以保证图像可逆, 冗余的多高位则以位替换的方式嵌入秘密信息。针对多高位预测可能错误的问题, 设计一个依据预测差值大小腾出高位的嵌入位置选择策略, 使得越接近的像素值能预留越多的高位空间。在解密阶段, 秘密信息能够无误地从子块内像素的多高位提取, 图像内容也能根据嵌入的多高位的数量、预测值以及预测差值实现无损恢复。实验结果表明, 所提方法对广泛使用的 BOWS-2 数据集的图像平均嵌入容量可达 2.58 bit/pixel, 优于其他的同类方法。

关键词: 加法同态; 可逆信息隐藏; 加密域; 多高位嵌入

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023058

Reversible data hiding in encrypted images based on additive homomorphic encryption and multi-MSB embedding

XIAO Wenqian, YANG Gaobo, WANG Dewang, XIA Ming

School of Information Science and Engineering, Hunan University, Changsha 410082, China

Abstract: Reversible Data Hiding in Encrypted Images (RDHEI) combines image encryption and reversible data hiding to improve the security and information transmission efficiency for the network transmission of images. In RDHEI, the conventional bit-by-bit encryption destroys the spatial correlation in an original image and has side effects on the preservation of embedding spaces. An approach for RHDEI was proposed, which utilized additive

收稿日期: 2022-04-11; 修回日期: 2023-02-16

通信作者: 杨高波, gbyang-hunu@hotmail.com

基金项目: 国家自然科学基金 (61972143, 61972142)

Foundation Item: The National Natural Science Foundation of China (61972143, 61972142)

引用格式: 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密文域可逆信息隐藏[J]. 网络与信息安全学报, 2023, 9(4): 121-133.

Citation Format: XIAO W Q, YANG G B, WANG D W, et al. Reversible data hiding in encrypted images based on additive homomorphic encryption and Multi-MSB embedding[J]. Chinese Journal of Network and Information Security, 2023, 9(4): 121-133.

homomorphic encryption and a multi-MSB (Most Significant Bit) embedding strategy to create room within the encryption process. The original image was divided into non-overlapped blocks, and each block was subjected to the same key for additive homomorphic encryption. This helped transfer the pixel correlation within an original block to the encrypted image block as much as possible. To enhance security, the encrypted image was further subjected to an Arnold transformation on a block-by-block basis. The decision of whether data will be embedded in a block and the embedding capacity were determined by the pixel differences within the block and the predicted values. When a block was selected for embedding, a small number of LSBs (Least Significant Bits) were used to store the prediction differences, ensuring reversibility. The redundant multi-MSBs were embedded with secret information by bit replacement. For the possible errors caused by multi-MSBs prediction, an embedding position selection strategy was designed by vacating MSBs in terms of the values of prediction errors, then more MSBs were reserved for those pixels with less prediction errors. During decryption, the secret information can be accurately extracted from the multiple MSBs of the pixels in a block, and the image content can be losslessly recovered using the number of embedded multi-MSBs, predicted values, and prediction differences. Experimental results on the BOWS-2 image dataset demonstrate that the average embedding capacity is improved to 2.58 bit/pixel, surpassing existing methods.

Keywords: additive homomorphism, reversible data hiding, encrypted domain, multi-MSB embedding

0 引言

传统的信息隐藏在嵌入秘密信息的过程中通常会对载体造成不可逆的修改,也被称为有损信息隐藏。可逆信息隐藏(RDH, reversible data hiding)是指将秘密信息嵌入文本、图像和视频等载体,能够无误地提取嵌入的信息并且无损地恢复载体内容^[1]。可逆信息隐藏具有突出的优势,适用于加密信息管理与认证、隐蔽通信和其他的安全保护,在医疗、金融和军事等领域有巨大的应用前景。依据实现原理的不同,可逆信息隐藏可分为无损压缩(LC, lossless compression)^[2-4]、差值扩展(DE, difference expansion)^[5-7]、直方图平移(HS, histogram shifting)^[8-10]和像素值排序(PVO, pixel value ordering)^[11-13]等类型。

随着云计算等应用的发展,图像经常会加密后存储到云服务器再进行数据访问和处理。这样,加密域图像可逆信息隐藏(RDHEI, reversible data hiding in encrypted image)应运而生,即对加密后的图像以可逆的方式嵌入秘密信息,而不需要解密或者提供对于加密图像的特定内容的感知。由于图像加密通常会破坏图像的空域冗余, RDHEI 不同于传统的基于明文图像的 RDH 技术,而是结合密文信号处理与信息隐藏技术。通常, RDHEI 包括图像加密和数据隐藏两个步骤。依据数据隐藏/提取是否独立于图像加密,现有的 RDHEI 方

法可以分为联合 RDHEI 和可分离的 RDHEI; 依据数据隐藏空间的创造方式, RDHEI 方法可以分为三类: 加密后预留空间(VRAE, vacating room after encryption)^[14-16]、通过加密预留空间(VRBE, vacating room by encryption)^[23-26]和加密前预留空间(RRBE, reserving room before encryption)^[17-22]。其中, RRBE 方法是在原始图像中创造嵌入空间,并且在加密后保留。因为原始图像像素之间的相关性高,这类方法的嵌入容量通常较高。对于 VRBE 方法,隐藏空间的预留取决于图像加密的方式,这类方法通常与空载的可逆信息隐藏方式结合起来。

VRAE 方法是直接在加密后的图像中寻找数据隐藏的空间。VRAE 方法通常利用传统的加密方法(如逐位流式加密)进行图像加密。这类方法通过轻微修改加密图像像素值嵌入秘密信息,嵌入容量较低,其可逆性也需要借助图像的空间相关性判别一个像素是否修改,并且在图像解密后无法做到可逆的恢复原始像素值。Zhang 等^[14]提出将加密后的图像划分成无重叠的子块,通过翻转子块内一半像素的最低 3 bit,以嵌入 1 bit 秘密信息。在接收方,利用子块内像素之间的空间相关性,进行平滑估计判别像素是否被修改,并提取秘密信息和恢复像素值。此后, Hong 等^[15]采用边缘匹配的策略提升平滑估计的准确性,减少信息提取与图像恢复时产生的误差,从而进一步提高可逆性。此外,为了进一步提升平滑估计的精确性,

Liao 等^[16]提出在恢复原始图像像素子块时, 将已经恢复的像素子块也作为评估当前子块平滑程度的重要依据。尽管如此, 上述算法还是无法保证完全可逆地提取秘密信息和恢复原始图像内容。

RRBE 方法是利用原始图像空域相关性, 在加密前预留足够的嵌入空间。信息嵌入者能够直接得到并利用加密后图像上预留的空间进行秘密信息嵌入。Ma 等^[17]首次提出采用 RRBE 方法实现可逆信息隐藏。在加密前, 利用 RDH 技术将一部分像素的 LSB (least significant bit) 存在图像的其他位置, 腾出该部分像素 LSB 位置保留到图像加密后用于秘密信息嵌入。相对低位, 加密前图像像素的高位相关性更强。为此, Puteaux 等^[18]提出了一个基于最高位 (MSB, most significant bit) 预测的 RDHEI 方法, 通过预测的方式在 MSB 平面腾出空间。此后, Yi 等^[20]改进 Puteaux 方法^[18], 同时预测像素最高两位并预留嵌入空间, 增加了嵌入容量。受到上述方法的启发, Yin 等^[21]提出了自适应多高位预测的方案, 进一步提升了嵌入容量。Mohammadi 等^[22]提出局部差分预测器, 利用相邻的像素进行预测并分析预测差值以腾出空间嵌入秘密信息。

VRBE 方法是指利用特殊的加密方案, 将原始图像的部分空间相关性保留或者转移到加密图像, 这类方法通常能够与空域的可逆信息隐藏方法结合起来。在文献[23-26]中, 图像被分成无重叠的像素块, 每块采用相同的密钥进行流加密, 使得加密后的块内像素一定程度上保留原始图像块像素的相关性。Ge 等^[23]将图像分成无重叠子块后, 计算每个子块内相邻像素差值, 并生成差值直方图, 再结合 HS 进行秘密信息嵌入。为提升嵌入容量, Huang 等^[24]使用了两种不同的 HS 方案分别进行信息嵌入: 一个是子块内相邻像素的差值 HS; 另一个是子块内预测差值 HS。Yi 等^[25]提出一个基于预测 DE 的方案, 在 2×2 子块嵌入秘密信息。Wang 等^[26]则提出了自适应的多高位预测算法, 利用子块内像素高位相关的特性, 在预测值满足嵌入条件的像素的高位通过位替换进行信息嵌入, 显著提升嵌入容量。

上述采用 VRBE 的 RDHEI 算法都是通过分块进行流同态加密保留子块内像素相关性。但是,

由于流加密随机性较强, 子块内的像素相关保留有限。此外, 在 Wang 等^[26]算法中, 多高位预测嵌入方式对于像素值相当接近的情况, 存在预测错误的现象。这两个问题会直接导致图像可预留的嵌入容量降低。

针对上述问题, 本文提出一个基于加法同态加密与多高位嵌入的 RDHEI 方法。鉴于流加密的随机性会破坏子块内像素的相关性, 本文提出对相同子块的像素采用相同的密钥进行加法同态加密, 尽可能地将原始图像子块内像素相关性转移到加密后图像对应的子块中。针对多高位预测可能错误的问题, 本文设计一个依据预测差值大小腾出高位的策略, 使得越接近的像素值能预留越多的高位空间。实验证明, 所提方法嵌入容量远超出 Wang 等^[26]提出的方法。具体地, 本文工作的创新点如下。

1) 提出一个基于 VRBE 且可分离的 RDHEI 方法。它采用加法同态加密的方式, 相对流加密^[26]有助于保留子块内像素值相关性。

2) 提出通过分析每个子块内预测差值大小, 将较小的预测差值保存到子块内像素的低位, 腾出的高位则作为秘密信息的嵌入空间, 显著提升了嵌入容量。

3) 在解密阶段, 该方法能够无误地提取秘密信息并且无损地恢复原始图像内容。

1 基于加法同态加密与多高位嵌入策略

在基于 VRBE^[26-28]的 RDHEI 方法中, 常规的加密手段会使得图像或图像块的熵值较高, 可腾出的嵌入空间较小。为此, 本文提出一个基于加法同态加密与多高位嵌入的 RDHEI 方法。首先, 如图 1(a)所示, 内容拥有者将图像分为无重叠子块, 同一个子块像素采用相同的密钥进行加法同态加密以保留子块内像素相关性。为了保证加密安全性, 对同态加密后的图像进行迭代的 Arnold 置乱。接着, 图 1(b)中的信息嵌入者按照内容拥有者的分块方式对加密后图像进行分块, 然后利用子块内保留的像素相关性, 在每个子块中预留足够的空间进行信息嵌入。在图 1(c)中, 当接收者收到含密的加密图像后, 可根据拥有的密钥不同得到不同的信息。当只拥有解密密钥时, 可解密出高质量的图像; 当只拥有嵌入密钥时, 可无

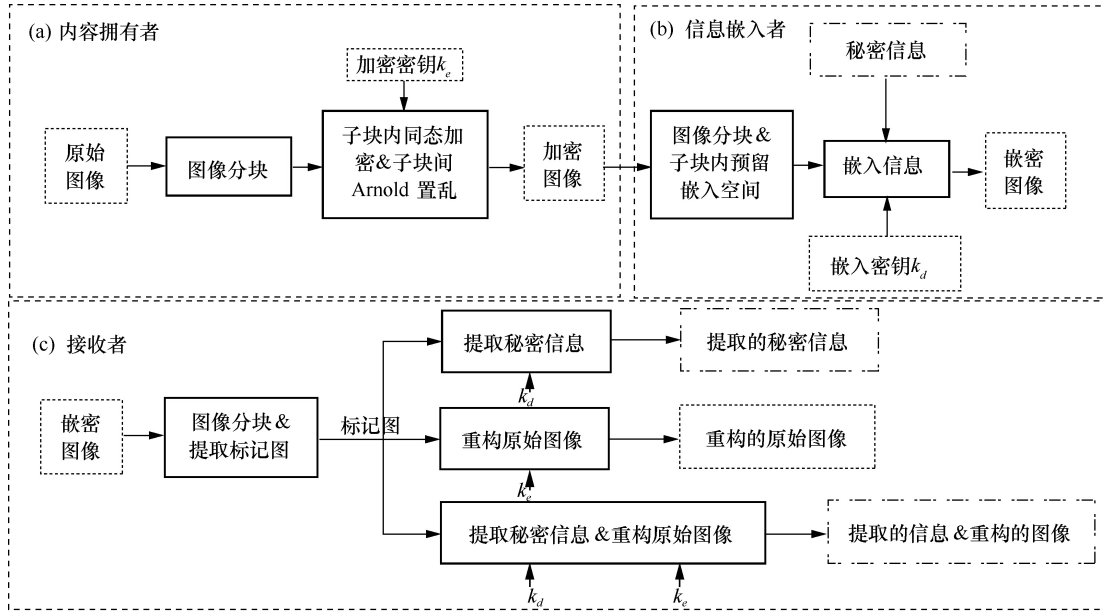


图1 本文算法框架

Figure 1 Framework of the proposed approach

误地提取秘密信息；当同时拥有解密和嵌入密钥时，可无误地提取秘密信息和无损地恢复图像。

1.1 加法同态加密机制

同态加密的概念由 Rivest 等^[29]首次提出。同态加密允许在没有解密密钥的情况下对加密数据做相应变化。常用的同态加密包括乘法同态和加法同态两种。乘法同态加密算法通常会产生数据扩展的问题，无法保证安全性。本文对原始图像使用模 N 的加法同态算法进行加密，假设 M 和 C 分别代表明文和密文信息， K 表示由 RC4 算法^[30]得到的秘密种子随机产生的密钥流。对数据进行加密 E 和解密 D 可以分别由式(1)和式(2)得到。

$$C = E(M, K) = (M + K) \bmod N \quad (1)$$

$$M = D(C, K) = (C - K) \bmod N \quad (2)$$

假设 m_1 和 m_2 是两个不同的明文数据， k_1 和 k_2 是两个随机加密密钥，那么

$$\begin{aligned} E(m_1, k_1) \oplus E(m_2, k_2) &= \\ E(m_1 + m_2, k_1 + k_2) \bmod N &= \\ (m_1 + m_2 + k_1 + k_2) \bmod N \end{aligned} \quad (3)$$

$$\begin{aligned} D(E(m_1, k_1) \oplus E(m_2, k_2), k_1 + k_2) &= \\ (E(m_1, k_1) \oplus E(m_2, k_2) - (k_1 + k_2)) \bmod N &= \\ (m_1 + m_2) \bmod N \end{aligned} \quad (4)$$

其中， $\oplus$ 是模 N 加法运算。特别地，当 $k_2 = 0$ 时，由式(3)和式(4)可以得到

$$\begin{aligned} E(m_1, k_1) \oplus m_2 &= \\ E(m_1, k_1) \oplus E(m_2, k_2) &= E(m_1 + m_2, k_1) \end{aligned} \quad (5)$$

$$\begin{aligned} D(E(m_1, k_1) \oplus E(m_2, k_2), k_1 + k_2) &= \\ (E(m_1, k_1) \oplus E(m_2, k_2) - (k_1 + k_2)) \bmod N &= \\ (m_1 + m_2) \bmod N \end{aligned} \quad (6)$$

从式(5)和式(6)可知，加法操作可以直接在加密数据上进行，而不需要对数据解密之后再行进行。

1.2 图像加密

对于一幅大小为 $W \times H$ 的 8 bit 原始灰度图像，其像素值 $X(i, j) \in [0, 255]$ ， $1 \leq i \leq W$ ， $1 \leq j \leq H$ 。将原始图像分为 $n \times n$ 的无重叠子块。其中， (W/n) 和 (H/n) 为整数，则原始图像可以分为 $(W/n) \times (H/n)$ 个子块，对每个子块依次记为 $B_{w,h}$ ， $w \in [1, W/n]$ ， $h \in [1, H/n]$ 。以 Lena 图像为例，原始图像的分块示意如图 2 所示。

对于每个子块，按照“从左到右，从上到下”的扫描顺序，子块 $B_{w,h}$ 的像素依次记为 $p_{w,h}^1, p_{w,h}^2, \dots, p_{w,h}^{n \times n}$ 。密钥 k_e 产生一个大小为 $(W/n) \times (H/n)$ 的密钥流，对于同一个子块中的像素用同样的密钥流进行加密，加密方式如下。

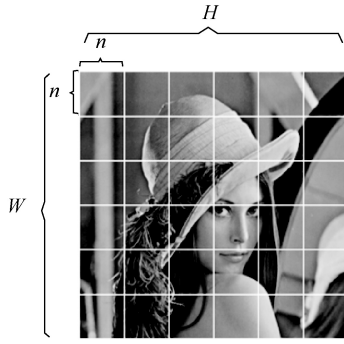


图2 原始图像分块示意
Figure 2 Original image after blocking

$$c_{w,h}^i = (p_{w,h}^i + k_{w,h}) \bmod 256, i = 1, 2, \dots, n \times n \quad (7)$$

其中, $c_{w,h}^i$ 是加密之后的像素值, $k_{w,h}$ 是加密密钥。本文对同一个子块的像素采用相同的密钥进行加法同态加密, 最大程度地保留子块中像素相关。但是, 这种加密方式也会使得加密后的图像可能保留了原始图像的轮廓。为了提高加密图像的安全性, 对加密后的图像再以子块为单位进行 Arnold 置乱。置乱后的加密图像安全性将在 2.1 节中进行分析。

Arnold 置乱^[31]的原理是把图像的每个像素点的位置进行移动, 得到一个相对原图像混乱的效果。本文是以子块为单位, 对每个子块的位置进行移动变化, 同一个子块中的像素点保持原来的相对位置不变。根据置乱密钥 $k_e 2$, 利用 Arnold 置乱对加密图像进行置乱。对每个子块的位置进行如下变换。

$$\begin{bmatrix} w' \\ h' \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} w \\ h \end{bmatrix} \bmod N \quad (8)$$

其中, (w, h) 是原始子块的位置, (w', h') 是经过一次变换后子块的位置, a, b 是参数, N 是图像矩阵的阶数, 即图像的大小, 一般指正方形图像。可对子块的位置进行多次迭代变换, 即利用式(8)进行重复多次置乱操作, 以提升加密后图像的安全性。同时, 保持子块内像素的相对位置不变, 即保留子块内像素位置的相关性。

1.3 加密后预留空间

根据式(9), 对加密后的图像计算同一个子块像素平均值作为该子块所有像素的预测值 $\text{prev}_{w,h}$ 。 i 依次表示子块中 $n \times n$ 个像素。

$$\text{prev}_{w,h} = \frac{1}{n \times n} \sum_{i=1}^{n \times n} c_{w,h}^i \quad (9)$$

然后, 依次得到子块的各个像素值与 $\text{prev}_{w,h}$ 之间差值的绝对值。

$$\text{err}_{w,h}^i = |\text{prev}_{w,h} - c_{w,h}^i|, i = 1, 2, \dots, n \times n \quad (10)$$

若 $\text{err}_{w,h}^i < 2^{m_i-1}$, 则表明该像素的前 $8-m_i$ 高位可腾出用于信息嵌入。其中 m_i 从 1 开始进行条件判断, 若满足则结束, 最大值可到 5。为了能够减少记录多个 m_i 的辅助信息, 取子块中所有像素可嵌入比特的最小值作为子块内每个像素实际可嵌入大小, 如下式所示。

$$t_{w,h} = \text{MIN}(8-m_i), i = 1, 2, \dots, n \times n \quad (11)$$

其中, $\text{MIN}(\bullet)$ 表示取最小值函数。当 $3 \leq t_{w,h} \leq 7$ 时, 表示该子块可嵌入, $\text{blm}_{w,h}$ 标记为“0”, 否则标记为“1”。 $\text{blm}_{w,h}$ 指坐标位于 (w, h) 的子块嵌入标记。为了保证子块内像素可逆, 辅助信息 $t_{w,h}$ 的大小用 3 bit 表示。如果该子块满足嵌入条件, 其可嵌入的总容量大小为 $n \times n \times t_{w,h}$ bit。例如, 图 3(a) 表示一个大小 2×2 的子块, 子块中每个像素与预测值 155 相减再取绝对值得到图 3(b), 根据式(10)得到子块内每个像素最大可嵌入容量, 如图 3(c) 所示。然后根据式(11)取子块内所有像素最小嵌入容量作为该子块所有像素的实际可嵌入大小。最后, 可以得到该子块可嵌入的总容量为 24 bit, 除去辅助信息预测值占用 8 bit, $t_{w,h}$ 编码 3 bit, 以及 $\text{blm}_{w,h}$ 标识位 1 bit, 最终该子块实际可嵌入秘密信息容量为 12 bit。

接下来, 证明满足条件 $\text{err}_{w,h}^i < 2^{m_i-1}$ 的像素能

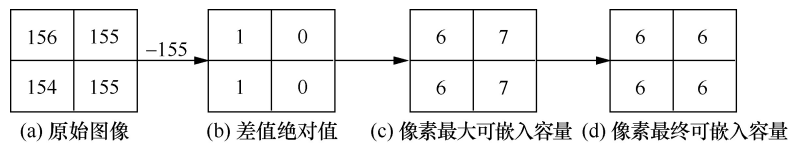


图3 子块嵌入容量示例
Figure 3 Sub-block embedding capacity example

够正确恢复原始值。注意到, 已嵌密的加密像素 $1^{\text{th}} \sim m^{\text{th}}$ LSB 与原始加密像素值 $1^{\text{th}} \sim m^{\text{th}}$ 的 LSB 一样。而 $(m+1)^{\text{th}} \sim 8^{\text{th}}$ MSB 嵌入了秘密信息, 故已嵌密的加密像素与原始加密像素值 $(m+1)^{\text{th}} \sim 8^{\text{th}}$ MSB 存在不同。保持像素的 $1^{\text{th}} \sim m^{\text{th}}$ LSB 不变, $(m+1)^{\text{th}} \sim 8^{\text{th}}$ MSB 的组合有 2^{8-m} 种情况, 假设 x_1 、 x_2 是其中两种情况所对应的像素值, 则它们一定满足以下式子。

$$|x_1 - x_2| \geq 2^m \quad (12)$$

若 x_1 、 x_2 都满足式(10), 则有以下两个不等式。

$$|\text{prev}_{w,h} - x_1| < 2^{m-1} \quad (13)$$

$$|\text{prev}_{w,h} - x_2| < 2^{m-1} \quad (14)$$

将式(13)、式(14)相加并根据绝对值不等式条件得到如下式子。

$$|x_1 - x_2| < |\text{prev}_{w,h} - x_1| + |\text{prev}_{w,h} - x_2| < 2^m \quad (15)$$

则有式(12)与式(15)矛盾, 所以 x_1 、 x_2 的值不可能同时满足式(10)。因此, 这 2^{8-m} 种情况所对应的像素值有且只有一个满足式(10), 即原始的加密像素值。

1.4 嵌入秘密信息

嵌入信息的过程包括辅助信息的嵌入与秘密信息的嵌入。辅助信息包括, 子块中每个像素可嵌入大小 $t_{w,h}$, 占 3 bit; 预测值 $\text{prev}_{w,h}$, 占 8 bit; 以及 $\text{blm}_{w,h}$ 标记, 占 1 bit; 共 12 bit。值得注意的是, 在本文方法中, 每个子块中每个像素至少嵌入 3 bit, 该子块的 $\text{blm}_{w,h}$ 才会标记为 “0”, 否则标记为 “1”。因此, 每个子块中所有像素的高 3 位

就可作为辅助信息的存放位置。以图 3 为例, 图 4(a)展示了子块中每个像素都可嵌入 6 位, 用二进制表示为 “110”。图 4(b)指该子块的预测值的二进制表示, 因为该子块满足嵌入条件, 因此 $\text{blm}_{w,h}$ 标记为 “0”。图 4(c)表示该子块的第一个像素高 3 位被替换为 “110”, 代表该子块像素可嵌入大小; 接着子块内的第 2 与第 3 个像素的 $1^{\text{th}} \sim 3^{\text{th}}$ MSB, 以及第 4 个像素的 $1^{\text{th}} \sim 2^{\text{th}}$ MSB 用于保存 8 bit 的预测值。第 4 个像素的 3^{th} MSB 用于存第一个像素最低位 LSB, 然后第一像素最低位 LSB 存该子块的标记 $\text{blm}_{w,h}$ 。这样能够使得在只拥有解密密钥时, 结合辅助信息直接解密得到的图像更加逼近原始图像。当该子块不满足嵌入条件时, 该子块只需嵌入 1 bit 辅助信息, 即 $\text{blm}_{w,h}$ 标记, 其嵌入位置为该子块第一个像素的最低位 LSB。而原本该像素的最低位 LSB 则拼接在秘密信息后, 同秘密信息一同嵌入。如图 4(c)所示, 剩余的 “x” 则用于嵌入秘密信息。为了提升安全性, 秘密信息在嵌入之前可通过信息嵌入者密钥 k_d 进行加密。秘密信息的嵌入过程如下。

Step 1: 加密图像按照同等大小划分为无重叠子块, 按照式(9)计算同一个子块中的预测值。

Step 2: 利用式(10)、式(11), 分析子块中像素可嵌入容量。

Step 3: 当子块中任意一个像素嵌入容量不满足嵌入条件时, $\text{blm}_{w,h}$ 对应子块标记为 “1”, 否则标记为 “0”。

Step 4: 为了实现提取秘密信息和恢复图像的分离性, 辅助信息 $\text{blm}_{w,h}$ 以及 $t_{w,h}$ 嵌入在每个子

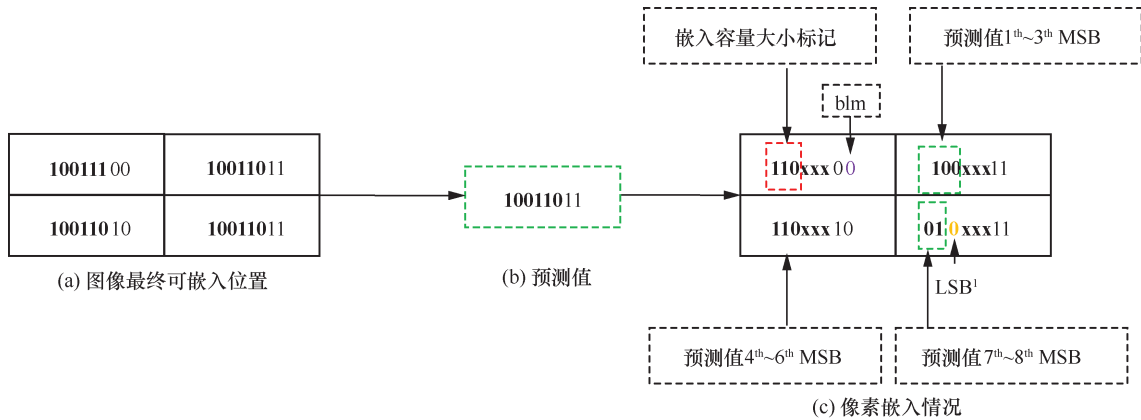


图4 子块中预留嵌入空间
Figure 4 Reserved embedding space in sub block

块易检测位置, 信息嵌入者和接收者共享。

Step 5: 根据 $\text{blm}_{w,h}$ 以及 $t_{w,h}$ 依次在每个子块中嵌入秘密信息。

1.5 信息提取与恢复原始图像

当接收方只有信息隐藏者密钥时, 能够根据共享的 $\text{blm}_{w,h}$ 以及 $t_{w,h}$ 无误地提取秘密信息。当只有加密密钥时, 接收方也可通过共享的 $\text{blm}_{w,h}$ 以及 $t_{w,h}$ 直接解密原始图像, 得到近似原始图像的内容。当接收方同时拥有信息隐藏者密钥以及加密密钥时, 接收方能够无误地提取秘密信息并且无损地重构原始图像内容。本文方案可以无误地提取出信息, 并无损恢复原始图像。信息提取与恢复原始图像的步骤如下。

步骤1 秘密信息提取

当接收者拿到嵌入密钥 k_d 后, 根据嵌入规则, 将嵌入后的加密图像按照大小 $n \times n$ 进行无重叠分块。因为 $\text{blm}_{w,h}$ 以及 $t_{w,h}$ 都嵌入在每个子块的固定位置, 容易被检测, 所以优先提取辅助信息。首先, 接收者提取子块中第一个像素的最低位 LSB, 即 $\text{blm}_{w,h}$ 标记, 根据 $\text{blm}_{w,h}$ 标记内容判断该子块是否嵌入, 如果 $\text{blm}_{w,h}$ 标记为“1”, 则表示该子块不嵌入秘密信息, 则忽略。如果标记为“0”, 提取该子块第一个像素的 1th~3th MSB, 得到子块嵌入容量 $t_{w,h}$ 。如果 $t_{w,h} > 3$, 则从子块中每个像素的 4th MSB 开始提取秘密信息, 提取方法如下。

$$b_k^i = (c_{w,h}^{ti} - c_{w,h}^{ti(3\text{MSB})}) \bmod 2^{5-k} \quad (16)$$

$$i=1, 2, \dots, n \times n, k=1, 2, \dots, (t_{w,h}-3)$$

其中 $c_{w,h}^{ti}$ 表示嵌入秘密信息后的像素, $c_{w,h}^{ti(3\text{MSB})}$ 表示取 $c_{w,h}^{ti}$ 1th~3th MSB, 其余位补 0。 b_k^i 表示在第 i 个像素嵌入的第 k 位秘密比特信息。

步骤2 恢复原始图像像素值

从每个子块第 2 和第 3 个像素提取 1th~3th MSB 以及第 4 个像素提取 1th~2th MSB 拼接出预

测值 $\text{prev}_{w,h}$, 再根据 $t_{w,h}$ 按照以下公式推算出嵌入前的像素值。

$$r_{w,h}^i = x_{w,h}^{(t_{w,h}\text{MSB})} + c_{w,h}^{i(8-t_{w,h})\text{LSB}}, i=1, 2, \dots, n \times n \quad (17)$$

$x_{w,h}^{(t_{w,h}\text{MSB})}$ 指低 $8-t_{w,h}$ 位取 0, 高 $t_{w,h}$ 位从小到大的大循环取。 $c_{w,h}^{i(8-t_{w,h})\text{LSB}}$ 指取嵌入信息后的加密像素 $c_{w,h}^{ti}$ 低 $8-t_{w,h}$ 位, 其余高位取 0。 $r_{w,h}^i$ 表示根据 $x_{w,h}^{(t_{w,h}\text{MSB})}$ 与 $c_{w,h}^{i(8-t_{w,h})\text{LSB}}$ 推算出的恢复值, 如果满足式(10), 则唯一确定 $r_{w,h}^i$ 为原始的加密像素值 $c_{w,h}^i$ 。因为加密图像进行了置乱操作, 所以需要将加密图像的子块还原到置乱前的位置。根据解密密钥 k_e 对图像进行还原, 还原的方法如下。

$$\begin{bmatrix} w \\ h \end{bmatrix} = \begin{bmatrix} ab+1 & -a \\ -b & 1 \end{bmatrix} \begin{bmatrix} w' \\ h' \end{bmatrix} \bmod N \quad (18)$$

其中, (w, h) 是 (w', h') 经过一次解密变换之后得到的子块的位置, 根据密钥, 利用式(18)进行重复变换, 使子块的位置恢复到原始图像的位置。然后, 根据解密密钥 k_{e1} (即加密密钥) 可以恢复得到原始图像的像素值 $p_{w,h}^i$, 具体解密式子如下。

$$p_{w,h}^i = (c_{w,h}^i - k_{w,h}) \bmod 256, i=1, 2, \dots, n \times n \quad (19)$$

通过步骤 1 和步骤 2, 可以无误地提取出秘密信息, 并且无损地恢复原始图像。

2 实验分析

本节首先利用直方图统计分析、香农熵以及 Arnold 置乱效果评估该加密算法的安全性; 接着分析图像重构后的峰值信噪比 (PSNR, peak-signal-to-noise ratio) 与结构相似性 (SSIM, structural similarity), 判断是否可逆; 最后, 分析图像实际嵌入容量大小, 并与现有的一些优秀算法进行比较。本文选择信息隐藏常用的 6 幅标准灰色图像作为测试图像, 如图 5 所示。为

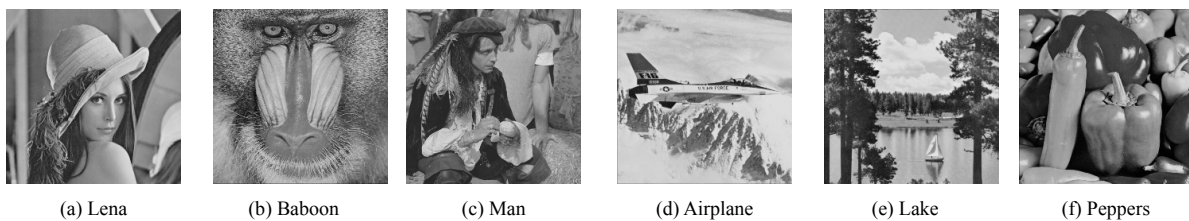


图5 测试图像
Figure 5 Test images

了进一步分析提出算法的性能, 本文在 BOWS-2 数据集^[32]上进行实验, 分析其平均嵌入容量, 并与现有的优秀方法进行比较。

2.1 安全性分析

本文利用加法同态加密与 Arnold 置乱对原始图像进行加密。为了能够评估该加密算法的安全性, 本文主要从直方图统计分析、香农熵以及 Arnold 置乱效果 3 个方面进行验证。

(1) 直方图统计分析

如图 6 所示, 可以看到 Lena、Baboon、Man、Airplane、Lake 以及 Peppers 的原始图像和加密图像的像素分布直方图。与原始图像的像素分布直方图对比, 加密图像的像素分布直方图分布平均, 无法识别出图像特征信息。因此, 从直方图统计特征的角度看, 加密后的图像具有很强的安全性。

(2) 香农熵

香农熵又称为信息熵, 用来衡量信息的信息量大小, 其定义如下。

$$H(x) = -\sum_{i=1}^h p(x_i) \lg p(x_i) \quad (20)$$

其中, H 表示不同信号总的信息量, x_i 表示信号量, $p(x_i)$ 则是信号量 x_i 出现的概率。

对 8 bit 的灰色图像而言, 图像的熵衡量一幅图像的混乱情况。图像熵越接近 8, 表示该图像

越混乱, 也就是攻击者越难在这样一幅图像中分析出信息。表 1 为不同测试图像在分成大小为 2×2 、 4×4 、 8×8 的子块分别进行加密后的熵值。可以看到, 加密后的图像香农熵值相比未加密的原始图像更加接近 8, 这就说明加密后的图像像素特征更少, 更加安全。由表中实验结果可知, 分成 2×2 大小的子块的熵值最高, 故其加密的安全性更高。

表 1 不同大小的子块加密后的熵值

Table 1 Entropy after encryption of sub blocks of different sizes

测试图像	原始图像熵值	加密后图像熵值 (2×2)	加密后图像熵值 (4×4)	加密后图像熵值 (8×8)
Lena	7.445 5	7.999 2	7.998 2	7.997 1
Baboon	7.357 9	7.999 3	7.999 1	7.998 7
Man	7.192 6	7.999 0	7.998 2	7.996 9
Airplane	6.702 5	7.999 1	7.998 2	7.992 8
Lake	7.484 5	7.999 1	7.998 5	7.997 9
Peppers	7.571 5	7.999 3	7.998 7	7.997 4

注: 加粗字体为每列最优值。

(3) Arnold 置乱效果

为了能够证明 Arnold 置乱对加密图像性能有进一步的提高, 本文将 Lena 和 Peppers 图像作为测试图像, 将子块大小设置为 8×8 进行加法同

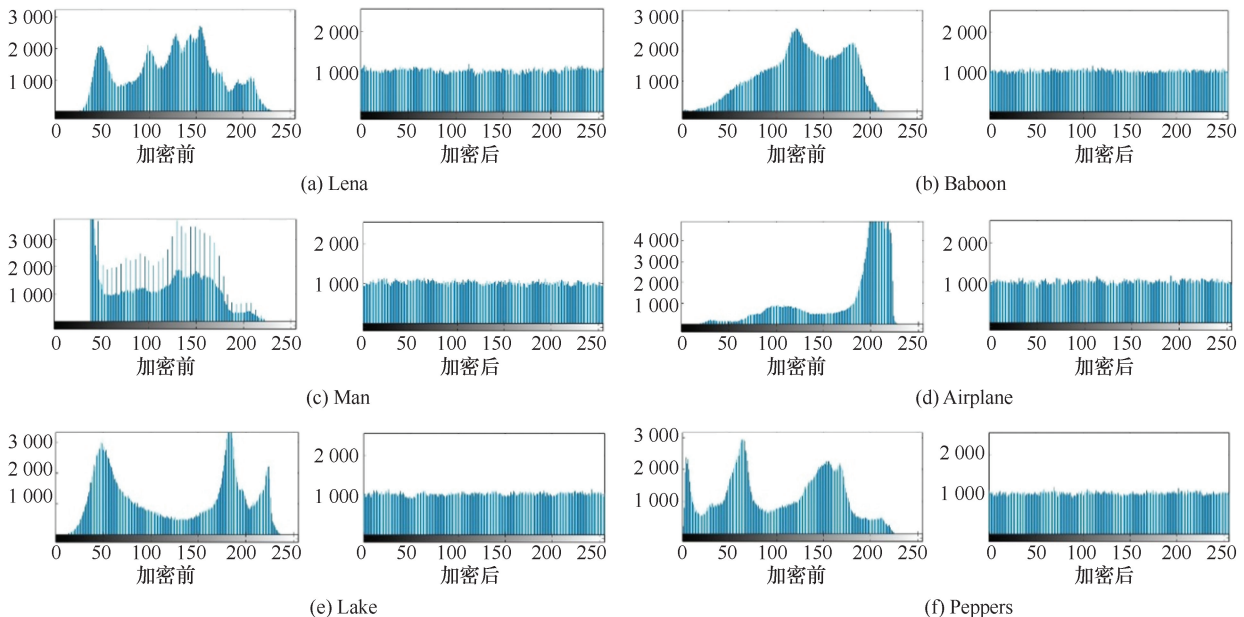


图 6 测试图像加密前与加密后的像素分布直方图

Figure 6 Pixel distribution histogram of test images before and after encryption

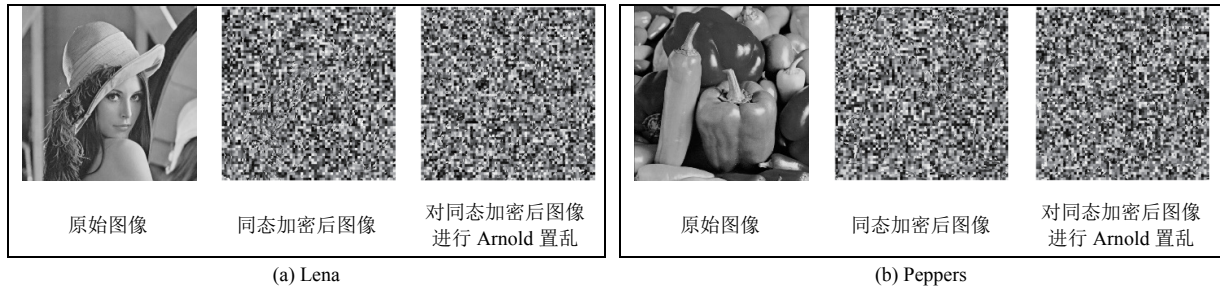


图7 Lena 与 Peppers 的 3 种图像形态
Figure 7 Three forms of Lena and Peppers

态加密与 Arnold 置乱。然后对比原始、同态加密后以及同态加密后进一步进行 Arnold 置乱这 3 种图像形态。

从图 7 中可以得到,只进行同态加密的图像保留了原始图像的轮廓,而置乱后的图像在视觉上完全混乱,无法识别图像内容。因此,可以证明 Arnold 置乱对图像加密安全性有了进一步提高。

2.2 性能分析

为了能够评估本文算法的性能,主要从嵌入容量大小和重构后图像的视觉质量进行评估。

1) 嵌入容量大小

以每个像素能够嵌入的信息比特数 (bpp, bit per pixel) 作为嵌入容量评价指标。在所提算法中,每幅图像的总嵌入容量 capc 可以由下式得到。

$$\text{capc} = \sum_{w=1}^{(W/n)} \sum_{h=1}^{(H/n)} t_{w,h} (n \times n) \quad (21)$$

为了最后能够实现秘密信息无误提取且图像内容无损恢复,必要的辅助信息需要进行保留。如果子块满足嵌入条件,则 $\text{blm}_{w,h}$ 标记为“0”,辅助信息大小为 12 bit。如果子块不满足嵌入条件,则 $\text{blm}_{w,h}$ 标记为“1”,辅助信息大小为 1 bit。假设标记为“0”的子块数为 n_0 ,标记为“1”的子块数为 n_1 ,可推出秘密信息嵌入空间为 $\text{capc} - 12 \times n_0 - n_1$ bit。

对于一幅图像而言,子块的大小会决定图像最终嵌入容量大小,因而在选取的 6 幅图像中,本文分别以 2×2 、 4×4 、 8×8 子块大小来评估图像的嵌入容量。如表 2 所示。可以得知当图像以 4×4 大小为子块时嵌入容量最大。

2) 重构后图像的视觉质量

PSNR 是一种评价图像的客观标准,如下式表示。

$$\text{PSNR} = 10 \lg \left(\frac{(255)^2}{\frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (I_r(i,j) - I(i,j))^2} \right) \quad (22)$$

其中, $I_r(i,j)$ 表示恢复像素值, $I(i,j)$ 表示原始像素值。图像 PSNR 值越大,失真越小。本文方法能够在没有信息嵌入者密钥、只有加密密钥的情况下直接重构近似原始图像的图像内容。如果同时拥有加密密钥以及嵌入密钥,就能够无损恢复出原始图像内容。另一个用于评估两张图像相似性的指标是结构相似性 (SSIM),其计算如下。

表 2 不同大小子块的嵌入容量与嵌入率
Table 2 Embedding capacity and embedding rate of different large and small blocks

测试 图像	2×2		4×4		8×8	
	嵌入 容量/bit	嵌入率/ (bit·pixel ⁻¹)	嵌入 容量/bit	嵌入率/ (bit·pixel ⁻¹)	嵌入 容量/bit	嵌入率/ (bit·pixel ⁻¹)
Lena	372 793	1.42	547 606	2.09	393 738	1.50
Baboon	62 348	0.24	115 555	0.44	38 589	0.15
Man	335 091	1.282	425 940	1.62	215 023	0.82
Airplane	486 397	1.86	640 252	2.44	494 595	1.89
Lake	227 330	0.87	368 548	1.40	245 279	0.94
Peppers	327 585	1.25	515 602	1.97	340 781	1.30

注: 加粗字体为每列最优值。

$$\text{SSIM}(x, y) = \frac{(2\mu_x \mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\mu_x^2 + \mu_y^2 + c_2)} \quad (23)$$

其中, x 与 y 表示两张图像,这里可以认为是恢复的图像 I_r 与原始图像 I ,其中 μ_x 指 x 的平均值, μ_y 指 y 的平均值, μ_x^2 是 x 的方差, μ_y^2 是 y 的

方差, σ_{xy} 是 x 与 y 的协方差, 而 c_1 与 c_2 是用来维持稳定的常数, 可以避免分母为 0。当 SSIM 的值越接近 1, 表示两张图像相似度越高, 如果值等于 1, 则证明两张图像完全一样。在本文中, 直接重构的图像与原始图像之间的 SSIM 值接近于 1。当得到信息嵌入者密钥时, 完全恢复的图像与原始图像之间 SSIM 值为 1, 证明其完全一样。表 3~表 5 是不同测试图像在不同子块大小情况下, 仅有加密密钥时直接重构原始图像的 PSNR 与 SSIM 值, 以及同时拥有加密密钥与嵌入密钥时, 完全重构原始图像的 PSNR 与 SSIM 值。通过表 3、表 4 和表 5 可知, 当子块越大时, 只拥有解密密钥时直接重构图像的恢复性能就会越好。而同时拥有解密密钥和嵌入密钥的重构性能不受子块大小影响, 能够实现图像内容完全可逆恢复。从表 5 可以看到, 当子块大小为 8×8 时, 直接重构性能最优。其中, 测试图像 Lena 直接重构的图像 PSNR 值高达 71 dB。因此, 图像失真小, 图像视觉质量高。

表 3 测试图像直接重构的 PSNR 与 SSIM(2×2)
Table 3 PSNR and SSIM for direct reconstruction of test images(2×2)

测试图像	直接重构 PSNR/dB	直接重构 SSIM	完全重构 PSNR/dB	完全重构 SSIM
Lena	66.85	0.999 9	∞	1
Baboon	60.28	0.999 9	∞	1
Man	65.21	0.999 9	∞	1
Airplane	66.16	0.999 9	∞	1
Lake	63.84	0.999 9	∞	1
Peppers	66.89	0.999 9	∞	1

注: 加粗字体为每列最优值。

表 4 测试图像直接重构的 PSNR 与 SSIM(4×4)
Tab 4 PSNR and SSIM for direct reconstruction of test images(4×4)

测试图像	直接重构 PSNR/dB	直接重构 SSIM	完全重构 PSNR/dB	完全重构 SSIM
Lena	68.16	0.999 9	∞	1
Baboon	64.21	0.999 9	∞	1
Man	66.54	0.999 9	∞	1
Airplane	67.99	0.999 9	∞	1
Lake	66.14	0.999 9	∞	1
Peppers	68.40	0.999 9	∞	1

注: 加粗字体为每列最优值。

表 5 测试图像直接重构的 PSNR 与 SSIM(8×8)
Tab 5 PSNR and SSIM for direct reconstruction of test images(8×8)

测试图像	直接重构 PSNR/dB	直接重构 SSIM	完全重构 PSNR/dB	完全重构 SSIM
Lena	71.89	0.999 9	∞	1
Baboon	69.41	0.999 9	∞	1
Man	70.38	0.999 9	∞	1
Airplane	72.13	0.999 9	∞	1
Lake	70.68	0.999 9	∞	1
Peppers	71.66	0.999 9	∞	1

注: 加粗字体为每列最优值。

2.3 与优秀方法比较

本文方法与 Puteaux 等^[18]、Liu 等^[27]、Qin 等^[28]及 Wang 等^[26]方法进行对比。Puteaux 等^[18]采用 RRBE 方法, 首次提出基于高位预测嵌入信息, 通过预测最高位 MSB 并替换最高位 MSB 方式进行嵌入, 嵌入率平均值接近于 1 bit/pixel。但该作者只利用了最高位, 而忽略了其他高位冗余空间。Liu 等^[27]、Qin 等^[28]以及 Wang 等^[26]是近年来采用 VRBE 方法较新的 3 个算法, Liu 等^[27]为了增加加密后图像的冗余空间, 提出了将原始图像腾出的冗余空间传送到加密后的图像上, 使得加密后的图像可嵌入空间得到大幅提高。如表 6 所示, 在本文测试图中, 其平均嵌入率达到 1.48 bit/pixel。Qin 等^[28]方法同样采用冗余空间传递, 同时加入二进制块编码的技术, 利用高位比特与低位比特随机互换的特殊方式进行加密, 使得信息嵌入者可以在加密后的图像像素低位进行信息嵌入, 其相较于 Liu 等^[27]方法, 平均嵌入率提升了 0.28 bit/pixel。Wang 等^[26]方法以子块为单位采用流加密的方式进行图像加密, 然后在子块中采用多高位预测的方式进行嵌入, 在嵌入率上有了新的突破。与上述文献相比, 本文算法无论在安全性上, 还是在嵌入率上都更出色。如表 6 所示, 选用 Lena、Peppers、Boat、Barbara 以及 Lake 作为测试图, 可以看出本文方法相比采用 RRBE 方法的文献^[18]在嵌入率上有了一定的提高, 相对同样采用 VRBE 方法的文献^[26-28]而言, 本文在嵌入率上表现得更为出色。在对比文献中, 本文的平均嵌入率最大提升 0.81 bit/pixel, 最小提升 0.13 bit/pixel, 平均提升了 0.41 bit/pixel。在 BOWS-2 库的 10 000 张图像测试中, 如表 6 最后一列所示。

表6 信息嵌入率
Table 6 Information embedding rate

测试图像	信息嵌入率/(bit-pixel ⁻¹)				
	Puteaux 等 ^[18] 方法(RRBE)	Liu 等 ^[27] 方法(VRBE)	Qin 等 ^[28] 方法(VRBE)	Wang 等 ^[26] 方法(VRBE)	所提方法
Lena	0.987	1.6052	1.8413	1.6947	2.0889
Peppers	0.9929	1.6347	1.8191	1.5844	1.9669
Boat	0.9913	1.5584	1.9121	1.6733	1.9793
Lake	0.9914	1.405	1.4725	1.2802	1.4059
Barbara	0.9859	1.2165	1.2753	1.2714	1.5447
Avg	0.987	1.484	1.664	1.5008	1.7971
BOWS-2	0.99	1.68	2.06	2.22	2.58

注：加粗字体为每列最优值。

本文在 BOWS-2 库平均嵌入率达到 2.58 bit/pixel，相比上述文献都有不小提升，最大可提升接近 1.6 bit/pixel。通过上述可以证明本文算法在嵌入容量上优于现存的一些算法。

为了能够更加直观地观察到本文方法的嵌入性能，在 BOWS-2 库中随机选了 500 张图像进行嵌入率计算，得到如图 8 所示的嵌入率分布折线图，从图 8 中可以看出，这 500 张的图像的最大嵌入率可以达到 5 bit/pixel 以上，平均嵌入率达到 3 bit/pixel 以上，特别是在图像索引 150 到 200 这个区间，几乎所有的图像嵌入率在 3 bit/pixel 以上。综上，本文方法在嵌入率性能上表现不错，超越上述比较的相关方法。

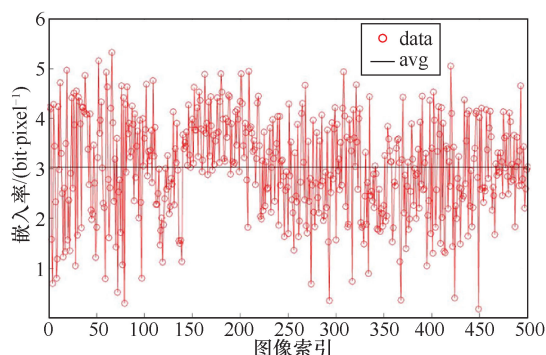


图8 在 BOWS-2 库中随机选择 500 张图像的嵌入率
Figure 8 ER on 500 images randomly selected from BOWS-2 database

图 9 展现了在给定嵌入率要求下，只拥有解密密钥时直接重构原始图像的 PSNR 值曲线。本文采用 Lena 图像与 Peppers 图像作为测试。从图 9 中可以看到，Puteaux 等^[19]和 Wang 等^[26]方法能够在只拥有解密密钥时完全恢复原始图像，但是其最大嵌入率相比其他方法低。另外两种方法

(Liu 等^[27]与 Qin 等^[28])的嵌入容量相较于之前两个方法提升一些，但是直接解密图像 PSNR 值较低，尤其是在它们达到最高负载时，PSNR 值会降低到 45 dB 左右，因而在性能方面相对于本文算法低很多。本文方法在最大嵌入容量时，PSNR 仍然能够接近 70 dB，图像质量非常高。如果能够同时拥有解密密钥与提取密钥，本文方法能够实现完全重构，PSNR 值达到+∞，实现图像的完全可逆。

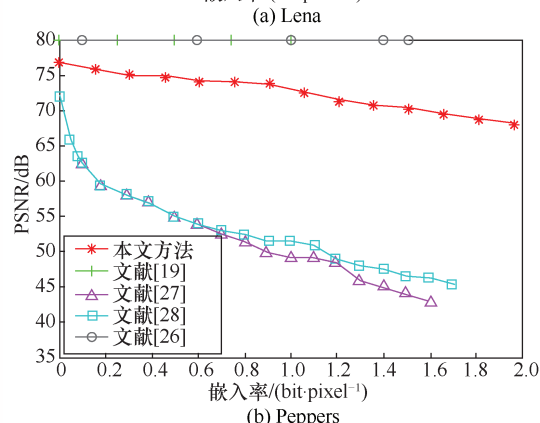
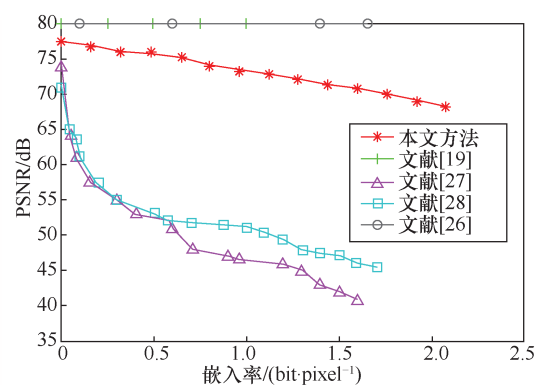


图9 5 种方法进行图像直接重构性能比较
Figure 9 Direct reconstruction performance comparisons with the methods

3 结束语

本文提出了一种新的基于VRBE的RDHEI方法。它采用分块加法同态加密方式,尽可能地将原始像素值之间的关联性转移到加密后的图像。采用多高位嵌入策略,用像素较少的低位保留子块内的像素预测值与预测差值,腾出多高位进行秘密信息嵌入,显著提升了嵌入容量。而且,本文算法的信息提取和图像恢复是可分离并且无误的。通过每个子块的辅助信息 $\text{blm}_{w,h}$ 与 $t_{w,h}$,本文方法能够在只拥有图像加密密钥时,恢复高质量的图像;在只拥有嵌入密钥时,无误提取秘密信息;在同时拥有上述两个密钥时,无损地恢复原始图像并且无误地提取出秘密信息。未来,将继续研究新的嵌入算法以追求更高的嵌入容量。

参考文献:

- [1] SHI Y Q, LI X, ZHANG X, et al. Reversible data hiding: advances in the past two decades[J]. IEEE Access, 2016, 4 (1): 3210-3237.
- [2] MANICCAM S S, BOURBAKIS N. Lossless compression and information hiding in images[J]. Pattern Recognition, 2004, 37(3): 475-486.
- [3] ABBASI R, XU L, AMIN F, et al. Efficient lossless compression based reversible data hiding using multilayered n-bit localization[J]. Security and Communication Networks, 2019, 2019(1):1-13.
- [4] WANG Y, CAI Z, HE W. High capacity reversible data hiding in encrypted image based on intra-block lossless compression[J]. IEEE Transactions on Multimedia, 2020, 23(6): 1466-1473.
- [5] HU Y, LEE H K, CHEN K, et al. Difference expansion based reversible data hiding using two embedding directions[J]. IEEE Transactions on Multimedia, 2008, 10(8): 1500-1512.
- [6] LEE C F, CHEN H L, TSO H K. Embedding capacity raising in reversible data hiding based on prediction of difference expansion [J]. Journal of Systems and Software, 2010, 83(10): 1864-1872.
- [7] LIN C C, YANG S P, HSUEH N L. Lossless data hiding based on difference expansion without a location map[C]//IEEE Congress on Image and Signal Processing. 2008, 2(6): 8-12.
- [8] LI X, LI B, YANG B, et al. General framework to histogram-shifting-based reversible data hiding[J]. IEEE Transactions on Image Processing, 2013, 22(6): 2181-2191.
- [9] HUANG L C, TSENG L Y, HWANG M S. A reversible data hiding method by histogram shifting in high quality medical images[J]. Journal of Systems and Software, 2013, 86(3): 716-727.
- [10] XUAN G, YAO Q, YANG C, et al. Lossless data hiding using histogram shifting method based on integer wavelets[C]//International Workshop on Digital Watermarking. 2006(11): 323-332.
- [11] LI X, LI J, LI B, et al. High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion[J]. Signal processing, 2013, 93(1): 198-205.
- [12] QU X, KIM H J. Pixel-based pixel value ordering predictor for high-fidelity reversible data hiding[J]. Signal Processing, 2015, 111(6):249-260.
- [13] OU B, LI X, ZHAO Y, et al. Reversible data hiding using invariant pixel-value-ordering and prediction-error expansion[J]. Signal processing: image communication, 2014, 29(7): 760-772.
- [14] ZHANG X. Reversible data hiding in encrypted image[J]. IEEE Signal Processing Letters, 2011, 18(4): 255-258.
- [15] HONG W, CHEN T S, WU H Y. An improved reversible data hiding in encrypted images using side match[J]. IEEE Signal Processing Letters, 2012, 19(4): 199-202.
- [16] LIAO X, SHU C. Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels[J]. Journal of Visual Communication and Image Representation, 2015, 28(4): 21-27.
- [17] MA K, ZHANG W, ZHAO X, 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.
- [18] PUTEAUX P, PUECH W. An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images [J]. IEEE Trans on Information Forensics and Security, 2018, 13(7): 1670-1681.
- [19] PUTEAUX P, PUECH W. EPE-based huge-capacity reversible data hiding in encrypted images[C]//IEEE International Workshop on Information Forensics and Security. 2018,12:1-7.
- [20] PUYANG Y, YIN Z, QIAN Z. Reversible data hiding in encrypted images with two-MSB prediction[J]. IEEE International Workshop on Information Forensics and Security, 2018,12:1-7.
- [21] YIN Z, XIANG Y, ZHANG X. Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding [J]. IEEE Trans on Multimedia, 2019 22(4): 874-884.
- [22] MOHAMMADI A, NAKHKASH M, AKHAEI M A. A high-capacity reversible data hiding in encrypted images employing local difference predictor [J]. IEEE Trans on Circuits and Systems for Video Technology, 2020 30(8): 2366-2376.
- [23] GE H, CHEN Y, QIAN Z, et al. A high capacity multi-level approach for reversible data hiding in encrypted images[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2018, 29(8): 2285-2295.
- [24] HUNG F, HUANG J, SHI Y Q. New framework for reversible data hiding in encrypted domain[J]. IEEE Transactions on Information Forensics Security, 2016, 11(12): 2777-2789.
- [25] YI S, ZHOU Y, HUA Z. Reversible data hiding in encrypted images using adaptive block-level prediction-error expansion[J]. Signal Processing: Image Communication, 2018, 64(3): 78-88.
- [26] WANG Y, HE W. High capacity reversible data hiding in encrypted image based on adaptive MSB prediction[J]. IEEE Transactions on Multimedia, 2021, (6):1.
- [27] LIU, ZI-LONG, PUN, CHI-MAN. Reversible data-hiding in en-

encrypted images by redundant space transfer[J]. Information Sciences, 2017, 433(12): 188-203.

- [28] QIN C, QIAN X, HONG W, et al. An efficient coding scheme for reversible data hiding in encrypted image with redundancy transfer[J]. Information Sciences, 2019, 487(3): 176-192.

- [29] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978, 4(11): 169-180.

- [30] STALLINGS W. Network and internetwork security: principles and practice[M]. Prentice-Hall, Inc. 1995.

- [31] WU L, ZHANG J, DENG W, et al. Arnold transformation algorithm and anti-arnold transformation algorithm[C]//First International Conference on Information Science and Engineering, 2009, (1): 1164-1167.

- [32] BAS P, FURON T. Image database of BOWS-2[EB]. .

[作者简介]



肖文乾（1994—），男，广西北海人，湖南大学硕士生，主要研究方向为图像信息隐藏。



杨高波（1974—），男，湖南岳阳人，湖南大学教授、博士生导师，主要研究方向为图像/视频内容安全、多媒体通信。



王德望（1993—），男，福建福州人，湖南大学博士生，主要研究方向为深度学习、隐写和图像处理。



夏明（1973—），男，四川成都人，湖南大学博士生，主要研究方向为图像内容安全。