基于图像块分组的加密域可逆信息隐藏

程 航[1,2], 王子驰[1], 张新鹏[1]
(1. 上海大学通信与信息工程学院,上海 200444; 2. 福州大学数学与计算机科学学院,福州 350108)

摘 要: 为了提升加密域可逆信息隐藏的方法性能,提出了一种基于图像块分组的加密域可逆信息隐藏方案. 在该方案中,内容所有者采用流密码异或加密图像,随后数据隐藏者将加密的图像进行分块,并按一定比例将图像块分组,再根据待嵌入的信息修改每组中相应的图像块,从而实现信息嵌入. 对于含有秘密信息的加密图像,接收者可使用加密密钥解密得到与原始图像近似的解密图像,然后根据自然图像空间相关性,通过比较每组中各图像块的平滑度找出被修改的图像块,从而实现秘密信息正确提取和图像完美恢复. 实验证明本方法在保证一定图像质量的情况下有较大的信息嵌入量.

关键词: 图像加密;可逆信息隐藏;平滑度
中图分类号: TP 309 **文献标志码**: A **文章编号**: 0254 - 0037(2016)05 - 0722 - 07
doi: 10.11936/bjutxb2015080007

Reversible Data Hiding for Encrypted Image Based on Image Blocks Grouping

CHENG Hang[1,2], WANG Zichi[1], ZHANG Xinpeng[1]
(1. College of Communication and Information Engineering, Shanghai University, Shanghai 200444, China;
2. College of Mathematics and Computer Science, Fuzhou University, Fuzhou 350108, China)

Abstract: In order to achieve better performance, a reversible data hiding scheme for encrypted image was proposed based on image block grouping. Using this scheme, the original image of the content owner was encrypted by exploiting a stream cipher. When obtaining an encrypted image by the content owner, the encrypted image was divided into non-overlapping blocks by the data-hider, and the image blocks were grouped by the data hiding key. Subsequently, additional data was embedded into the encrypted image by modifying one of the image blocks in each group. With an encrypted image containing additional data, the receiver can readily gain decrypted version similar to the original image using the encryption key. Meanwhile, with the aid of spatial correlation in natural image, he or she can perfectly recover the original image and correctly extract additional data by comparing the smoothness of image blocks in each group. Experimented result shows that the proposed scheme can acquire a higher payload with good image quality. Furthermore, this scheme is suitable for practical application due to its simple operation and easy realization.

Key words: image encryption;reversible data hiding;smoothness

信息隐藏是通过轻微改变载体数据将额外信息嵌入到载体中,以实现隐蔽通信、版权保护等功能.

收稿日期: 2015-08-03
基金项目: 国家自然科学基金资助项目(61472235); 上海市浦江人才计划资助项目(13PJ1403200)
作者简介: 程 航(1979—), 男, 博士研究生, 主要从事图像处理、密码学、信息隐藏方面的研究,E-mail: hcheng@shu.edu.cn

在军事、医学、司法等特殊领域中除了提取额外信息外，还需要无失真地恢复载体内容，即需要可逆的信息隐藏方案. 目前已存在许多优秀的可逆信息隐藏方法，如差值扩展[1-4]、直方图平移[5-9]、无损压缩[10]、整数变换[11-13]等. 但这些可逆信息隐藏方法均需要在明文图像中进行. 近年来，个人隐私保护意识逐渐加深，数据往往经过加密，如何对加密后的数据进行进一步处理，即加密域信号处理，已吸引了众多学者的广泛关注. 本文研究主要关注加密域可逆信息隐藏，即内容所有者在发送前先将原始载体加密，加密后的载体经数据隐藏者获取并嵌入信息后发送给接收者，接收者根据相应密钥进行解密及信息提取. 由于在某些场合下内容所有者并不信任数据隐藏者[14]，即内容所有者担心载体内容被数据隐藏者泄露，因此，需要一种加密域的可逆信息隐藏方案. 例如，为了保护病人隐私需要将医学图像加密，而管理员希望在加密图像中嵌入用以区分病人的信息，即管理员需要在加密后的医学图像中嵌入信息.

现有的加密域可逆信息隐藏方法可分为 4 类：1）加密前不做任何处理，通过简单修改部分密文数据以嵌入信息[15-18]；2）将密文数据压缩以腾出空间容纳额外信息[19-21]；3）加密图像前先进行预处理，预留出空间以便于信息嵌入[22-25]；4）用公钥机制加密载体数据，利用加密技术的同态性嵌入信息[26].

其中第 2 类方法有较大嵌入量，但方法操作复杂，计算量较大；第 3 类方法中内容所有者需要为数据隐藏者做额外工作，但实际应用中内容所有者不应进行除图像加密外的任何操作，所以此类方法不能满足实际所需；第 4 类方法加密安全性好，但加密后数据量膨胀以及计算复杂度急剧增加；第 1 类方法较好地解决了以上问题，如文献[15]根据秘密信息翻转加密图像部分像素的最低 3 位以嵌入信息，但文献[15]中每个图像块只能嵌入 1 bit 额外信息，导致该方法的容量较小. 随后，研究者提出了一些改进方法，如文献[16]利用各个块边沿像素的相关性特征来降低信息提取误码率；文献[17]提出选取部分像素最低有效位进行比特嵌入，在降低信息提取误码率的同时，能有效改善嵌入信息后图像的峰值信噪比. 文献[18]提出了一种计算图像平滑度的方法，改善了方法性能. 但这些改进方法对性能的提升较小.

本文提出了一种基于图像块分组的加密域可逆信息隐藏方案，较大程度上改善了方法性能且操作简单、易于实现. 首先，用加密密钥将原始图像加密，然后，将加密图像分块并分组，最后，通过修改每组图像块中的 1 块来嵌入秘密信息. 接收端将含有秘密信息的加密图像解密后，得到 1 幅与原始图像近似的解密图像，再根据自然图像的空间相关性恢复图像并提取秘密信息.

1　本文方案

方案整体结构如图 1 所示. 内容所有者利用加密密钥对原始图像进行加密，得到加密图像；数据隐藏者将加密图像分块，利用信息嵌入密钥将图像块分组，在每组中嵌入多比特信息，之后将含有秘密信息的加密图像发送给接收者. 接收者先利用加密密钥将密文图像解密，得到 1 幅与原始图像近似的解密图像，之后根据自然图像空间相关性与信息嵌入密钥提取秘密信息并恢复原始图像.

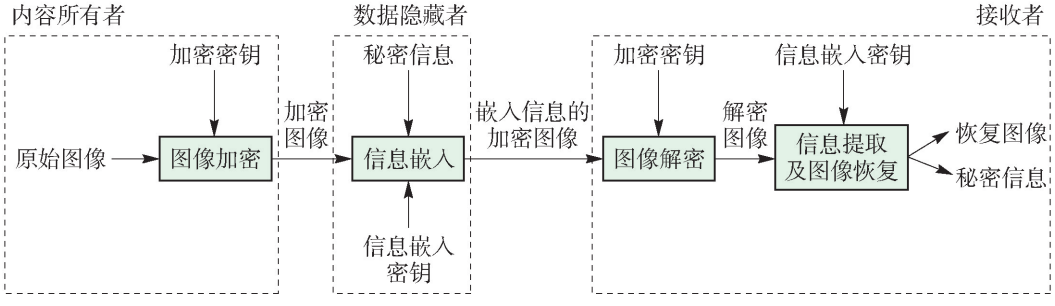


图 1　方案结构图

Fig. 1　Sketch of proposed scheme

1.1　图像加密

对于未经压缩的灰度图像，任意 1 个图像像素 $p_{i,j}$ 的取值范围为[0,255]，(i, j) 表示像素在块中的位置. $p_{i,j}$ 可用 8 *bit* 来表示，设各像素的比特位为 $b_{i,j,0}, b_{i,j,1}, \cdots, b_{i,j,7}$，则

$$b_{i,j,k}=\left\lfloor\frac{p_{i,j}}{2^k}\right\rfloor \bmod 2,\quad k=0,1,\cdots,7 \tag{1}$$

$$p_{i,j}=\sum_{k=0}^{7}(b_{i,j,k}\cdot 2^k) \tag{2}$$

其中$\lfloor\cdot\rfloor$表示向下取整. 内容所有者利用加密密钥产生 1 个伪随机比特流 $r_{i,j,k}$,与图像像素各比特位 $b_{i,j,k}$逐位进行异或运算

$$B_{i,j,k}=b_{i,j,k}\oplus r_{i,j,k} \tag{3}$$

所得到的 $B_{i,j,k}$即图像像素 $p_{i,j}$加密的结果,之后将加密图像传送给数据隐藏者.

1.2 信息嵌入

数据隐藏者获得加密图像后,在不知道原始图像内容情况下,也能执行秘密信息嵌入操作. 首先将加密图像分块,再将图像块分组,修改每组图像块中 1 个嵌入信息. 具体步骤如下:

步骤 1 将图像分块,每块大小 $s\times s$. 设图像大小为 $M\times N$,则共有 n 个图像块($n=\lfloor M/s\rfloor\cdot\lfloor N/s\rfloor$).

步骤 2 将 k 个图像块分为 1 组($k\leqslant n$),记为 $H_1,H_2,\cdots,H_k$,各组互不重叠,则共有 $g=\lfloor n/k\rfloor$组. 图像块的分组方式由信息嵌入密钥决定,即由信息嵌入密钥决定图像块的排列顺序,按此顺序每 k 个块分为 1 组. 对每组通过修改 k 个图像块中 1 个块来嵌入信息. 修改方式如步骤 3 所示. 由于 k 个图像块对应了数据修改时的 k 种可能,因此,在每组中可嵌入 t 比特二进制信息($t=\lfloor\log_2 k\rfloor$).

步骤 3 将加密后的 t 比特二进制信息转换为十进制数 m ($0\leqslant m\leqslant 2^t-1\leqslant k-1$),修改第 $m+1$ 个图像块 H_{m+1},即在当前组中嵌入了 t 比特信息. 对 H_{m+1}的修改方式如图 2 所示,将图像块按棋盘格方式划分,之后将绿色部分所代表像素的第 L 位取反($1\leqslant L\leqslant 8$),即通过翻转绿色部分像素的第 L 位实现秘密信息嵌入.

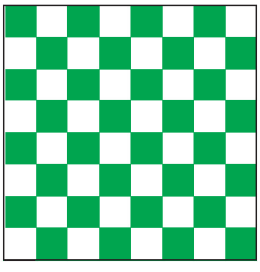


图 2 图像块中的像素分布

Fig. 2 Distribution of pixels in a block

步骤 4 对各组均按步骤 3 嵌入信息即完成信息嵌入操作.

由于图像共分为 g 组,每组嵌入 t 比特信息. 因此信息嵌入容量为

$$C=g\cdot t=\left\lfloor\frac{n}{k}\right\rfloor\cdot\lfloor\log_2 k\rfloor \tag{4}$$

1.3 图像解密

将密文图像像素用 8 bit 表示:$b'_{i,j,0},b'_{i,j,1},\cdots,b'_{i,j,7}$,利用加密密钥产生 1 个伪随机比特流 $r_{i,j,k}$,并与 $b'_{i,j,k}$逐位进行异或运算

$$B'_{i,j,k}=b'_{i,j,k}\oplus r_{i,j,k} \tag{5}$$

所得到的 $B'_{i,j,k}$为像素各比特的解密结果,则解密像素灰度值为

$$p'_{i,j}=\sum_{u=0}^{7}(B'_{i,j,u}\cdot 2^u) \tag{6}$$

解密图像内容与原始图像近似,由信息嵌入过程可知,包含额外信息的解密图像相对于原始图像的最小均方误差 MSE (mean square error)为

$$\mathrm{MSE}=\frac{(2^{L-1})^2}{2k} \tag{7}$$

则解密图像的峰值信噪比 PSNR (peak signal to noise ratio)为

$$\mathrm{PSNR}=10\log_{10}\frac{255^2}{\mathrm{MSE}}=10\log_{10}\frac{520\,200k}{4^L} \tag{8}$$

根据式(8)对应不同参数 L、k,解密图像峰值信噪比的理论值如表 1 所示. 不难看出,设置合适的参数可获得质量较高的解密图像.

表 1 解密图像峰值信噪比的理论值

Table 1 Theoretical value of PSNR dB

项目	$k=4$	$k=8$	$k=16$	$k=32$	$k=64$
$L=3$	45.1	48.1	51.1	54.2	57.2
$L=4$	39.1	42.1	45.1	48.1	51.1
$L=5$	33.1	36.1	39.1	42.1	45.1
$L=6$	27.1	30.1	33.1	36.1	39.1
$L=7$	21.0	24.0	27.1	30.1	33.1

1.4 信息提取及图像恢复

接收者用加密密钥将密文图像解密后,得到与原始图像大致相同的解密图像. 此时,可根据信息嵌入密钥恢复原始图像并提取秘密信息. 每组图像块中有且仅有 1 个被修改,则接收者只需找出每组图像块中被修改的块即可恢复图像并提取信息.

由于自然图像具有空间相关性,因此,图像被修改后的平滑度小于修改前. 对于被修改的图像块,其平滑度较小,将其以相同方式再次修改后便返回到未修改状态,此时平滑度较大. 被修改的图像块

经二次修改后平滑度变大，而未被修改的图像块经二次修改后平滑度变小. 据此便可找出每组图像块中被修改的块. 衡量图像块平滑度的公式为

$$d_1 = \sum_{u=2}^{s-1}\sum_{v=2}^{s-1}\left| p_{u,v} - \frac{p_{u-1,v} + p_{u,v-1} + p_{u+1,v} + p_{u,v+1}}{4} \right| \tag{9}$$

$$d_2 = \sum_{u=1}^{s}\sum_{v=1}^{s-1}\left| p_{u,v} - p_{u,v+1} \right| + \sum_{u=1}^{s-1}\sum_{v=1}^{s}\left| p_{u,v} - p_{u+1,v} \right| \tag{10}$$

$$\begin{aligned} d_3 = {} & \sum_{u=2}^{s-1}\left| p_{1,u} - \frac{p_{1,u-1} + p_{1,u+1} + p_{2,u}}{3} \right| + \sum_{u=2}^{s-1}\left| p_{s,u} - \frac{p_{s,u-1} + p_{s,u+1} + p_{s-1,u}}{3} \right| + \\ & \sum_{u=2}^{s-1}\left| p_{u,1} - \frac{p_{u-1,1} + p_{u+1,1} + p_{u,2}}{3} \right| + \sum_{u=2}^{s-1}\left| p_{u,s} - \frac{p_{u-1,s} + p_{u+1,s} + p_{u,s-1}}{3} \right| + \\ & \left| p_{1,1} - \frac{p_{1,2} + p_{2,1}}{2} \right| + \left| p_{1,s} - \frac{p_{1,s-1} + p_{2,s}}{2} \right| + \\ & \left| p_{s,1} - \frac{p_{s-1,1} + p_{s,2}}{2} \right| + \left| p_{s,s} - \frac{p_{s,s-1} + p_{s-1,s}}{2} \right| \end{aligned} \tag{11}$$

$$f = d_1 + d_2 + d_3 \tag{12}$$

式中：$p_{u,v}$为块中对应的像素值，(u,v)为像素在块中的位置；d_1 反映了中心像素与其预测值的差异；d_2 反映了相邻像素的差异；d_3 表示边沿像素与其预测值的差异；f 为衡量当前块的平滑度，f 越大表示平滑度越小.

信息提取及图像恢复的具体步骤如下：

步骤 1　将图像按照与发送端相同方式分块并分组，对每组按步骤 2 恢复图像并提取信息.

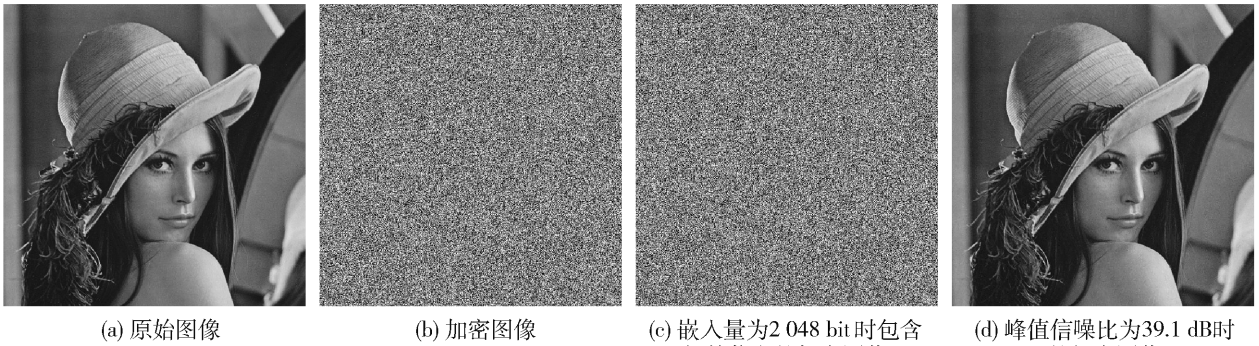
步骤 2　对当前组的 k 个图像块 $H_1, H_2, \cdots, H_k$ 按式(9) ~ (12)分别计算 f 值，记为 $f_1, f_2, \cdots, f_k$. 按图 2 所示方式，将此 k 个图像块中黑色部分所代表像素的第 L 位取反，得到 k 个新图像块 $H'_1, H'_2, \cdots, H'_k$，再按式(9) ~ (12)分别计算 f 值，记为$f'_1, f'_2, \cdots, f'_k$.

令 $A = f_a - f'_a (1 \leqslant a \leqslant k)$，分别计算各图像块所对应的 A 值，记为 $A_1, A_2, \cdots, A_k$. 对于未经修改的图像块，$f_a < f'_a$；而对于被修改的图像块，$f_a > f'_a$. 即被修改图像块的 A 值最大. 设 $A_w = \max\{A_1, A_2, \cdots, A_k\}, (1 \leqslant w \leqslant k)$，则认为第 w 个图像块被修改，将 $H_1, H_2, \cdots, H'_w, \cdots, H_k$ 作为恢复的图像块，$w-1$ 作为当前组提取的十进制数，转换为二进制后即为提取的秘密信息.

步骤 3　对各组均重复步骤 2 即得到秘密信息与恢复图像.

2　实验结果

本文将大小为 512 像素 ×512 像素的灰度图像作为原始图像进行实验. 图 3(a)为 Lena 原始灰度图像，图 3(b)为加密图像. 设置参数 $L=4, s=8, k=4$，在加密图像中嵌入 2 048 bit 额外信息，包含额外信息的加密图像如图 3(c)所示.



(a) 原始图像　(b) 加密图像　(c) 嵌入量为2 048 bit时包含额外信息的加密图像　(d) 峰值信噪比为39.1 dB时的解密图像

图 3　图像 Lena 实验结果

Fig. 3　Experiment results of Lena

对图 3(c)所示的包含额外信息的加密图像直接解密后的图像如图 3(d)所示，其峰值信噪比为 39.1 dB. 通过同时使用信息嵌入密钥和加密密钥，能成功地从包含额外信息的加密图像中提取信息并恢复原始图像，恢复后的图像与图 3(a)完全相同.

表 2、3 分别列出了图像 Lena 与 Baboon 在不同参数取值下，嵌入量、解密图像峰值信噪比以及恢复图像峰值信噪比的部分实验数据，其中“ $+\infty$ ”表示

原始图像被无误地恢复. 其中解密图像峰值信噪比 与表 1 所示的理论值吻合.

表 2 图像 Lena 嵌入量,解密图像峰值信噪比及恢复图像峰值信噪比与不同参数取值关系

Table 2 Relationship with different parameter values among embedding capacity, PSNR of directly decrypted image, and PSNR of recovered image of Lena **bit,dB, dB**

项目		$k=4$	$k=8$	$k=16$	$k=32$	$k=64$
$L=4$	$s=4$	8 192,39. 1,55. 1	6 144,42. 1,54. 0	4 096,45. 1,55. 1	2 560,48. 1,56. 9	1 536,51. 1,56. 4
	$s=8$	2 048,39. 1, + ∞	1 536,42. 1, + ∞	1 024,45. 1, + ∞	640,48. 1, + ∞	384,51. 1, + ∞
	$s=16$	512,39. 1, + ∞	384,42. 1, + ∞	256,45. 1, + ∞	160,48. 1, + ∞	96,51. 1, + ∞
$L=5$	$s=4$	8 192,33. 1,60. 2	6 144,36. 1,63. 2	4 096,39. 1,60. 2	2 560,42. 1, + ∞	1 536,45. 1,66. 2
	$s=8$	2 048,33. 1, + ∞	1 536,36. 1, + ∞	1 024,39. 1, + ∞	640,42. 1, + ∞	384,45. 1, + ∞
	$s=16$	512,33. 1, + ∞	384,36. 1, + ∞	256,39. 1, + ∞	160,42. 1, + ∞	96,45. 1, + ∞
$L=6$	$s=4$	8 192,27. 1, + ∞	6 144,30. 1, + ∞	4 096,33. 1, + ∞	2 560,36. 1, + ∞	1 536,39. 1, + ∞
	$s=8$	2 048,27. 1, + ∞	1 536,30. 1, + ∞	1 024,33. 1, + ∞	640,36. 1, + ∞	384,39. 1, + ∞
	$s=16$	512,27. 1, + ∞	384,30. 1, + ∞	256,33. 1, + ∞	160,36. 1, + ∞	96,39. 1, + ∞

表 3 图像 Baboon 嵌入量、解密图像峰值信噪比及恢复图像峰值信噪比与不同参数取值关系

Table 3 Relationship with different parameter values among embedding capacity, PSNR of directly decrypted image, and PSNR of recovered image of Baboon **bit,dB, dB**

项目		$k=4$	$k=8$	$k=16$	$k=32$	$k=64$
$L=4$	$s=4$	8 192,39. 1,42. 4	6 144,42. 1,43. 6	4 096,45. 1,45. 2	2 560,48. 1,47. 4	1 536,51. 1,49. 7
	$s=8$	2 048,39. 1,48. 6	1 536,42. 1,48. 6	1 024,45. 1,51. 0	640,48. 1,52. 6	384,51. 1,53. 4
	$s=16$	512,39. 1, + ∞	384,42. 1, + ∞	256,45. 1, + ∞	160,48. 1, + ∞	96,51. 1,60. 2
$L=5$	$s=4$	8 192,33. 1,41. 6	6144,36. 1,41. 9	4 096,39. 1,43. 6	2560,42. 1,45. 1	1536,45. 1,46. 0
	$s=8$	2 048,33. 1,53. 2	1 536,36. 1,55. 4	1 024,39. 1,57. 2	640,42. 1,55. 4	384,45. 1,55. 4
	$s=16$	512,33. 1, + ∞	384,36. 1, + ∞	256,39. 1, + ∞	160,42. 1, + ∞	96,45. 1, + ∞
$L=6$	$s=4$	8 192,27. 1,44. 4	6 144,30. 1,44. 7	4 096,33. 1,45. 4	2 560,36. 1,45. 5	1 536,39. 1,46. 2
	$s=8$	2 048,27. 1, + ∞	1 536,30. 1, + ∞	1 024,33. 1, + ∞	640,36. 1, + ∞	384,39. 1, + ∞
	$s=16$	512,27. 1, + ∞	384,30. 1, + ∞	256,33. 1, + ∞	160,36. 1, + ∞	96,39. 1, + ∞

图 4 展示了对于图像 Lena、Man、Lake、Baboon,在原始图像被无误恢复的前提下(即恢复图像的峰值信噪比为“ + ∞ ”),信息嵌入量与解密图像峰值信噪比的关系.

由以上结果可知,纹理较平滑的图像有利于可逆信息的嵌入. 因为图像内容的恢复需要利用空间相关性,所以图像纹理较复杂或方法参数设置不当时会导致接收端得到的平滑度有较大误差,从而错误定位被修改的图像块,最终导致图像不能完全恢复.

对同一幅图像,在原图像被无误地恢复的前提下,L 越大误码率越小. 但 L 越大解密图像的峰值信噪比越低,即嵌入额外信息引起的图像失真越严重. 因为 L 取值越大时像素修改幅度越大,这有利于接收者识别被修改的图像块,从而能更容易地恢复原始图像,因此误码率越小. 另一方面,像素修改

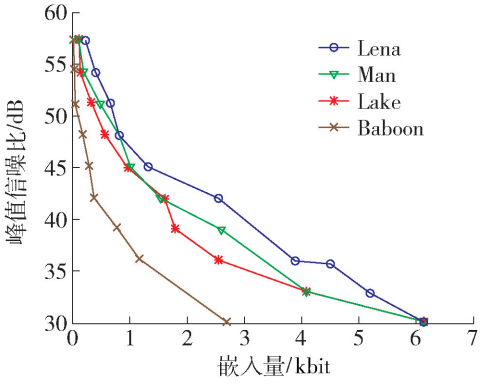


图 4 图像 Lena、Man、Lake、Baboon 嵌入量与解密图像峰值信噪比关系对比

Fig. 4 Comparison results of the relationship between capacity and PSNR in decrypted image of Lena, Man, Lake and Baboon

幅度的增大也会导致解密图像的峰值信噪比降低. 对于参数 s 与 k 可按相同方式进行分析，参数 L、s、k 与方法性能的关系如表 4 所示.

表 4　参数与方法性能关系

Table 4　Relationship between parameter values and performance

项目	容量	解密图像质量	误码率
s	↘	—	↘
L	—	↘	↘
k	↘	↗	↘

注：“↗”表示正相关，“↘”表示负相关，“—”表示无关.

在原始图像被无误恢复的前提下，本方法与文献[15-18]的对比情况如图 5 所示，显然本方法性能最优. 对于满嵌情况，即所有图像块都负载秘密信息时，在本方法中每组图像块只修改 1 个，而文献[15-18]中每个图像块均被修改，则对每个图像块均需判断修改情况. 本方法中只需找出被修改的块，无需对每块逐一判断，因此，判断准确性高于其余 4 种方法. 此外，本文衡量图像块平滑程度的方法结合了文献[15,16,18]，能更好地识别被修改的图像块，因此，本方法性能自然有所提升.

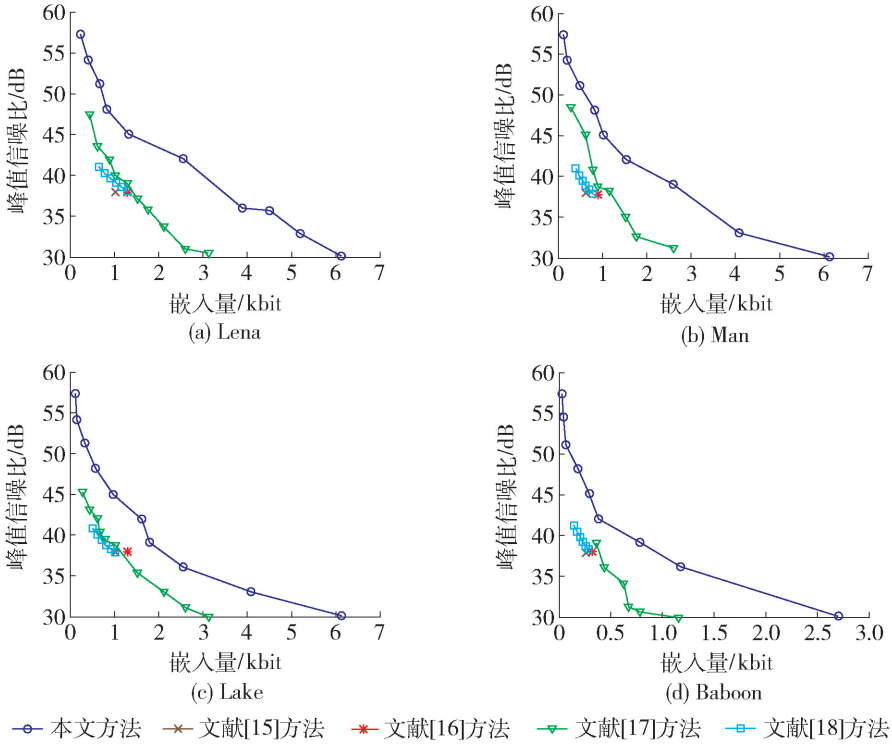


图 5　不同方法嵌入量与解密图像峰值信噪比关系对比

Fig. 5　Comparison results of the relationship between capacity and PSNR in decrypted image of different methods

3　结论

本文提出了一种基于图像块分组的加密域可逆信息隐藏方法，图像加密后将其分块，再将图像块分组，通过修改每组图像块中的 1 个块来嵌入信息. 接收端解密后根据自然图像空间相关性恢复图像并提取秘密信息. 实验结果证明本文方法性能有较大提升. 进一步研究工作将从以下 2 方面进行：

1）信息嵌入过程尽量少修改加密图像，以提高解密图像的峰值信噪比.

2）设计更准确的恢复机制，如图像平滑度的计算、被修改区域的寻找机制等.

参考文献：

[1] TIAN J. Reversible data embedding using a difference expansion[J]. IEEE Trans on Circuits and Syst for Video Techn, 2003, 13(8): 890-896.

[2] KIM H J, SACHNEV V, SHI Y Q, et al. A novel difference expansion transform for reversible data embedding [J]. IEEE Transactions on Information Forensics and Security, 2008, 3(3): 456-465.

[3] KUMAR V, NATARAJAN V. Difference expansion based reversible data hiding for medical images [C] // 2014 International Conference on Communications and Signal Processing (ICCSP). [S. l.]: IEEE, 2014: 720-723.

[4] HU Y J, LEE H K, LI J W. DE-based reversible data

hiding with improved overflow location map[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2009, 19(2): 250-260.

[5] NI Z C, SHI Y Q, ANSARI N, et al. Reversible data hiding [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2006, 16(3): 354-362.

[6] TAI W L, YEH C M, CHANG C C. Reversible data hiding based on histogram modification of pixel differences[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2009, 19(6): 906-910.

[7] KUO W C, JIANG D J, HUANG Y C. Reversible data hiding based on histogram [C] // Third International Conference on Intelligent Computing, Qingdao, China, August 21-24, 2007. Heidelberg: Springer, 2007: 1152-1161.

[8] LIN C C, TAI W L, CHANG C C. Multilevel reversible data hiding based on histogram modification of difference images[J]. Pattern Recognition, 2008, 41(12): 3582-3591.

[9] SHI Y Q, XUAN G R. Reversible data hiding: 8175324 [P]. 2012-05-08.

[10] CELIK M U, SHARMA G, TEKALP A M, et al. Lossless generalized-LSB data embedding[J]. IEEE Transactions on Image Processing, 2005, 14(2): 253-266.

[11] COLTUC D, CHASSERY J M. Very fast watermarking by reversible contrast mapping [J]. Signal Processing Letters, 2007, 14(4): 255-258.

[12] WANG X, LI X L, YANG B, et al. Efficient generalized integer transform for reversible watermarking[J]. Signal Processing Letters, 2010, 17(6): 567-570.

[13] PENG F, LI X L, YANG B. Adaptive reversible data hiding scheme based on integer transform[J]. Signal Processing, 2012, 92(1): 54-62.

[14] QIAN Z X, HAN X Y, ZHANG X P. Separable reversible data hiding in encrypted images by n-nary histogram modification [C] // The Third International Conference on Multimedia Technology. Paris: Atlantis Press, 2013: 869-876.

[15] ZHANG X P. Reversible data hiding in encrypted image [J]. Signal Processing Letters, 2011, 18(4): 255-258.

[16] HONG W, CHEN T S, WU H Y. An improved reversible data hiding in encrypted images using side match[J]. Signal Processing Letters, 2012, 19(4): 199-202.

[17] YU J, ZHU G P, LI X L, et al. An improved algorithm for reversible data hiding in encrypted image [M] // Digital Forensics and Watermaking. Heidelberg: Springer, 2013: 384-394.

[18] LIAO X, SHU C W. 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: 21-27.

[19] ZHANG X P. Separable reversible data hiding in encrypted image[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 826-832.

[20] ZHANG X P, QIN C, SUN G L. Reversible data hiding in encrypted images using pseudorandom sequence modulation[M] // Digital Forensics and Watermaking. Heidelberg: Springer, 2013: 358-367.

[21] ZHANG X P, QIAN Z X, FENG G R, et al. Efficient reversible data hiding in encrypted images[J]. Journal of Visual Communication and Image Representation, 2014, 25(2): 322-328.

[22] MA K, ZHANG W M, ZHAO X F, 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.

[23] JAGDALE M V, HINGWAY S P, SURESH S S. Reversible encryption and data hiding [J/OL]. International Journal of Advance Research in Computer Science and Management Studies, 2014, 2(1): 293-299 [2015-07-30]. http://www.ijarcsms.com/docs/paper/volume2/issue1/V211-0079.pdf.

[24] LATHA K, SUNDARAMBAL M. A novel encryption and extended dynamic histogram shifting modulation for reversible data hiding in encrypted image [J/OL]. International Journal of Computer Trends and Technology (IJCTT), 2014, 7(2): 115-118[2015-07-30]. http://www.ijcttjournal.org/Volume7/number-2/IJCTT-V7P130.pdf.

[25] ZHANG W M, MA K, YU N H. Reversibility improved data hiding in encrypted images[J]. Signal Processing, 2014, 94: 118-127.

[26] CHEN Y C, SHIU C W, HORNG G. Encrypted signal-based reversible data hiding with public key cryptosystem [J]. Journal of Visual Communication and Image Representation, 2014, 25(5): 1164-1170.

(责任编辑 郑筱梅)