

增强图像平滑度的可逆信息隐藏方案

王婧晗, 朱辉, 李鹤麟, 李晖, 杨晓鹏

(西安电子科技大学, 陕西 西安 710126)

摘要: 随着互联网技术的发展和社交网络的普及, 可逆信息隐藏技术因其具有无损恢复载体信息的特性而被广泛应用于医疗、军事等领域的隐蔽信息传输。传统的可逆信息隐藏方案大多聚焦于嵌入容量提升和载密图像失真率降低, 并未过多关注人们对图像视觉细节的要求, 难以抵抗隐藏信息检测方法。针对上述挑战, 从增强图像视觉平滑度方面入手, 提出了一种增强图像平滑度的可逆信息隐藏方案, 在嵌入隐蔽信息的同时提升载密图像最终的视觉质量。具体来说, 所提方案将目标图像分为参考区域与非参考区域, 利用非参考区域的图像像素预测值与原始像素值的差值作为信息嵌入的判断依据, 通过差值平移来嵌入信息; 进而构造图像平滑机制, 采用高斯滤波作为秘密信息嵌入时像素值修改的模板, 对预测值进行滤波计算, 将滤波差值无损地加入载体图像中, 以达到图像平滑的效果; 同时将参考区域的像素值作为边信息, 用于实现信息提取方对原始载体图像和秘密信息的无损恢复和提取; 并以高斯函数中的滤波系数作为预置秘密信息对嵌入信息进行加密处理以保证嵌入信息的机密性。大量经典图像数据集的测试与分析结果表明, 所提方案处理过的载密图像视觉平滑度得到了显著增强, 具有较低的失真率、较高的嵌入率和较高的嵌入提取效率。在典型环境下, 其生成的载密图像与高斯滤波后的图像相似度可达 0.996 3, 且可获得 37.346 的峰值信噪比和 0.328 9 的嵌入容量。

关键词: 可逆信息隐藏; 载密图像; 高斯滤波; 预测误差

中图分类号: TP309.2

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022040

Reversible data hiding scheme based on enhanced image smoothness

WANG Jinghan, ZHU Hui, LI Helin, LI Hui, YANG Xiaopeng

Xidian University, Xi'an 710126, China

Abstract: With the prosperity of Internet technology and the popularity of social networks, reversible data hiding

收稿日期: 2021-12-21; 修回日期: 2022-03-04

通信作者: 朱辉, zhuhui@xidian.edu.cn

基金项目: 国家重点研发计划 (2021YFB3101300); 国家自然科学基金 (61972304, 61932015); 公安部技术研究计划 (2019JSYJA01); 陕西省重点研发计划 (2020ZDLGY08-04)

Foundation Items: The National Key R&D Program of China (2021YFB3101300), The National Natural Science Foundation of China (61972304, 61932015), Technical Research Program of the Ministry of Public Security (2019JSYJA01), Shaanxi Provincial Key R&D Program (2020ZDLGY08-04)

引用格式: 王婧晗, 朱辉, 李鹤麟, 等. 增强图像平滑度的可逆信息隐藏方案[J]. 网络与信息安全学报, 2022, 8(3): 66-75.

Citation Format: WANG J H, ZHU H, LI H L, et al. Reversible data hiding scheme based on enhanced image smoothness[J]. Chinese Journal of Network and Information Security, 2022, 8(3): 66-75.

technology has been widely adopted in concealed information transmission of medical and military fields with its advantages on secret information recovery. Traditional reversible data hiding schemes mainly focus on the enhancement of embedding capacity and the reduction of the distortion rate of stego image, but pay less attention to the understanding of image details with the human eyes. Thus, it is difficult to resist hidden information detection methods. To solve the above challenge, a reversible data hiding algorithm was proposed, which ensured the visual quality of the stego image in the process of data hiding through the image visual smoothness enhancement. Specifically, the original image was divided into reference area and non-reference area. The secret data was embedded through the translation of the difference, which was calculated according to the predicted pixel value and the original pixel value of the non-reference area. To guarantee the visual quality of the image, smoothing mechanism was constructed, in which a Gaussian filter was utilized as a template to filter the predicted value and to add the filter difference into the cover image without loss. The pixel value of the reference region was used as edge information for lossless restoration of the original image. The filtering coefficient in Gaussian function was exploited as the embedded key to ensure the security of secret information. Simulation results regarding a large number of classical image data sets illustrated that the visual smoothness of stego image processed by this scheme was effectively enhanced with lower distortion rate, higher embedding rate, and higher embedding and extraction efficiency. In a typical circumstance, the similarity between the generated stego image and the Gaussian filter image can reach 0.9963. The PSNR and the embedded capacity can be up to 37.346 and 0.3289 BPP, respectively.

Keywords: reversible data hiding, secret image, Gaussian filter, prediction error

0 引言

信息隐藏技术^[1]通过将秘密信息隐藏在可公开的媒体数据中从而实现隐蔽通信的目的。近年来,随着互联网和数字通信技术的快速发展,数字媒体的数据量爆发增长,信息隐藏技术的应用场景持续拓展,受到人们越来越多的关注,被广泛应用于隐蔽信息传输、身份认证等场景。传统的信息隐藏技术在嵌入信息时会一定程度上给原始载体带来不可逆转的失真,从而破坏原始载体的数据完整性。为解决上述问题,可逆信息隐藏(RDH, reversible data hiding)^[2]应运而生,其可以将数据隐藏在数字图像中的同时,实现原始载体信息在信息提取方的完全无损恢复。

当前,可逆信息隐藏方案聚焦于在提高嵌入容量的同时降低载密图像的失真率,其主要采用基于直方图移动^[2-5]和差值拓展^[6-9]的方法进行设计。Ni等^[2]首次提出通过平移图像的强度直方图来嵌入数据的方法,将灰度直方图中处于峰值的像素值整体向左或向右平移,使峰值点的像素个数降为零,进而将秘密信息嵌入峰值点处。该算法通过维持高峰值信噪比(PSNR, peak signal to

noise ratio)来获得载密图像更低的失真程度,进而得到更高质量的载密图像,但由于不同图像的强度直方图的峰值不同,该算法嵌入容量稳定性较差。Hu等^[6]通过扩大相邻像素的差值,创建一个冗余的最小有效位(LSB, least significant bit)用于信息嵌入,在可逆信息隐藏中取得了重要进展。之后,作为差值拓展的扩充,陆续有学者提出通过计算预测因子提高嵌入容量的算法^[6-7]。该类算法使用相邻像素间的相关性对原始载体图像进行像素值预测,并进一步利用预测差值拓展与直方图平移的思想进行嵌入运算,保证了原始图像无损恢复。Li等^[8]利用图像之间的相关性,通过隔位构造预测器,解决了覆盖图像失真率随嵌入有效载荷增加而增加的问题,获得了更高的PSNR值和失真度更低的载密图像。

随着图像处理技术的日益成熟,基于图像增强的可逆信息隐藏技术开始在医学图像和卫星图像等领域应用,研究人员相继提出了一批结合对比度增强的可逆信息隐藏方案,实现了在传输秘密信息的同时提升图像明暗对比度的效果^[10-12],所提的算法不再试图保持高PSNR值,而是强调人眼对图像亮度变化的敏感性以及对图像细节的理解。其中,Wu等^[12]使用锐化算法,增强图像

高频部分的内容,通过预测因子与像素真实值的差值和锐化差值来携带秘密信息,从而提升图像明暗对比度的视觉效果,但由于其对锐化差值修改的阈值过小,导致算法的嵌入容量较现有的算法提升不大。与此同时,增强图像平滑度逐渐成为图像发布前的常规操作,文献[13]首次提出可逆的肤色平滑算法,将信息嵌入人脸图像后对载密图像进行肤色平滑,可以在数据传输的同时增加载密图像的视觉效果。但该方案并未将肤色平滑算法与信息隐藏算法结合,计算复杂且安全性较低。

鉴于目前的大部分文献聚焦于增强图像的对

比度,而很少关注图像视觉平滑度的问题,本文提出一种增强图像平滑度的可逆信息隐藏方案,根据高斯滤波算法具有消除噪声保持达到图像平滑的特征,构造高斯滤波机制,进而将其与可逆信息隐藏算法结合,实现了在保证原始载体图像嵌入容量与失真率的同时增强载密图像视觉平滑度的效果。

1 系统框架

典型的可逆信息隐藏系统框架由信息嵌入方、信息提取方和攻击者组成,其系统框架如图 1 所示,具体说明如下。

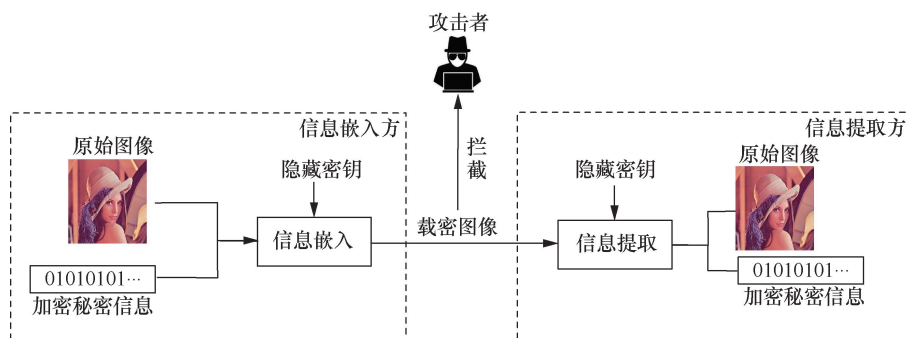


图 1 系统框架

Figure 1 system framework

信息嵌入方: 原始图像的采集者和秘密信息的拥有者。首先通过与信息提取方协商生成隐藏密钥和加解密密钥,然后选择原始图像和待嵌入的二进制比特秘密信息,并根据隐藏密钥将加密后的秘密信息嵌入原始图像中,发送给信息提取方。

信息提取方: 待获取秘密信息的合法接收者。根据隐藏密钥提取载体图像中加密的秘密信息,并且恢复原始载体图像。授权的图像提取方可以正确提取载密图像中加密的秘密信息,从而使用解密密钥恢复秘密信息,并最终获得原始图像。图像可以发送到多个接收器,非授权的信息提取方即使获得载密图像也无法得到秘密信息。

攻击者: 试图通过非法途径获取秘密信息的实体。在载密图像传输过程中,假设攻击者可以获取该方案的变换过程和部分载密图像,在没有隐藏密钥与加解密密钥的情况下破解信息嵌入方的秘密信息。

2 基于高斯滤波的可逆信息隐藏方案

本文方案由图像预处理、信息嵌入、信息提取 3 部分组成。所提方案的工作流程如图 2 所示,信息嵌入方选择不同的高斯滤波核系数作为隐藏密钥 E_K 来控制模拟高斯滤波过程,使用中值预测器获得预测差值^[14],在预测差值上使用差值平移的方法嵌入加密后的数据,并采用高斯滤波的方式,对预测值进行高斯计算获得滤波差值,将滤波差值可逆地插入载体数据中得到载密图像。信息提取方在收到载密图像后恢复预测差值与滤波差值,并使用预测差值来提取秘密信息,借助滤波差值来恢复原始载体图像。

其中,根据不同的情况用户可以设计不同的滤波核系数生成隐藏密钥 E_K 。在秘密信息传输前,信息嵌入方和信息提取方可以使用任意非对称加密算法将隐藏密钥 E_K 与加解密密钥 S_K 进行共享。表 1 为所提方案中涉及的相关符号说明。

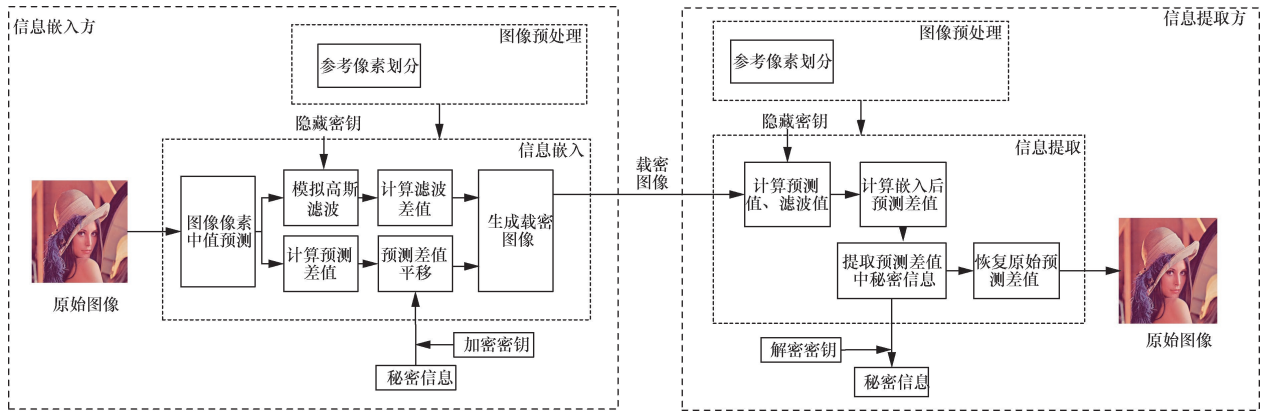


图2 所提方案的工作流程

Figure 2 The workflow of the proposed scheme

表1 所提方案中涉及的相关符号说明

Table 1 The symbols involved in the proposed scheme

符号	说明
$O(x, y)$	载体图像
s	秘密信息
m	加密后秘密信息
E_k	隐藏密钥
S_k	加密密钥
LM	位置图
$P(x, y)$	预测像素值
Δ	预测差值
n	秘密信息比特数
$C(x, y)$	滤波值
fd	滤波差值
$S'(x, y)$	更正前载密图像
$S(x, y)$	载密图像
Δ'	嵌入后预测差值
T	嵌入阈值

2.1 图像预处理

令 $O(x, y)$ 表示 8 bit $N \times N$ 大小的原始灰度图像, 并将除去前 r 行 (r 由载体图像实际情况确定, 建议取值为 4) 像素的 $O(x, y)$ 按照图 3 所示区域划分为参考像素与非参考像素。由于本文所提方案中使用的中值预测器需保证左上方像素值不变, 同时在不拓展图像大小的前提下滤波器无法覆盖到图像的边缘像素值, 需要将载体图像的外围像素, 即灰色区域设置为参考像素, 白色区域设置为非参考像素。为了保证载体图像可以无恢复, 参考像素在嵌入过程中保持不变。

2.2 信息嵌入与图像平滑

本环节中输入原始灰度图像 $O(x, y)$ 和秘密信息 s , 应用所提出的基于高斯滤波的可逆信息嵌入算法 (如算法 1 所示), 输出载密图像。其中, LM 为记录特殊像素点的位置图。具体工作流程如下。

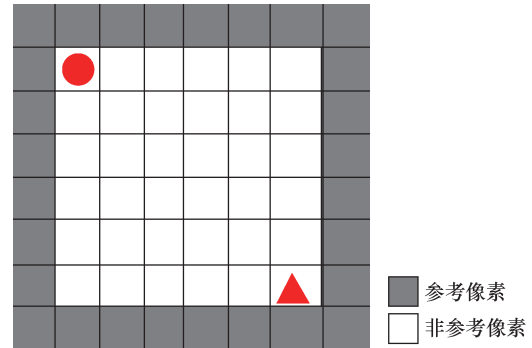


图3 参考像素与非参考像素分布示例

Figure 3 Example of reference and non-reference pixels

(1) 生成加密秘密信息

将载体图像前 r 行像素值的最低有效位 (LSB, least significant bit) 与秘密信息比特流 s 拼接后使用 AES 加密算法^[15]加密得到加密后的秘密信息比特流 m 。除前 r 行外的像素进行下述操作。

(2) 计算预测差值

如图 3 所示, 从左上角圆形像素为起点扫描 $O(x, y)$, 根据式(2)计算当前扫描点的预测值, 并通过 $\Delta = P(x, y) - O(x, y)$ 计算得到预测差值 Δ 。

算法1 信息嵌入算法

输入 原始图像 O , 高斯滤波核 W , 秘密信息 s , 位图 LM

输出 载密图像 S

```

1)  $m \leftarrow \text{Enc}(O(x, y) + s)$ 
2) for  $i = 1 \rightarrow m$  do
3)   for  $j = 1 \rightarrow n$  do
4)      $P(x, y) \leftarrow \text{Predict}(O(x, y))$ 
5)      $C(x, y) \leftarrow \text{Gaussian}(P(x, y), W)$ 
6)      $\Delta \leftarrow P(x, y) - O(x, y)$ 
7)      $\text{fd} \leftarrow C(x, y) - P(x, y)$ 
8)     If  $-T \leq \Delta \leq T$  then
9)        $\Delta' \leftarrow 2\Delta + m_k$ 
10)    End if
11)    If  $\Delta < -T$  then
12)       $\Delta' \leftarrow \Delta - T$ 
13)    Else
14)       $\Delta' \leftarrow \Delta + T - 1$ 
15)    End if
16)     $S'(x, y) = P(x, y) + \Delta' + \text{fd}$ 
17)    If  $0 \leq S' \leq 255$  then
18)       $S(x, y) \leftarrow S'(x, y)$ 
19)    Else
20)       $S(x, y) \leftarrow O(x, y)$ 
21)       $\text{LM}(x, y) \leftarrow 1$ 
22)    end if
23)  end for
24) end for
25)  $S(x, y) \leftarrow \text{LSB}(\text{LM})$ 
26) return  $S$ 

```

(3) 计算滤波差值

根据隐藏密钥 E_k 和式(1)对预测值 $P(x, y)$ 应用高斯滤波算法得到预测滤波值 $C(x, y)$ ，进而计算滤波差值 $\text{fd} = C(x, y) - P(x, y)$ 。

(4) 预测差值拓展

使用预测差值拓展和直方图平移的方法按照式(1)将秘密信息 m 嵌入预测差值 Δ 中，得到修改预测差值 Δ' 。

$$\Delta' = \begin{cases} \Delta \cdot 2 + m_k, & -T \leq \Delta \leq T \\ \Delta - T, & \Delta < -T \\ \Delta + T + 1, & T < \Delta \end{cases} \quad (1)$$

其中， T 为控制预测差值拓展的嵌入阈值， $\{i \in m \mid k = 1, 2, 3, \dots, n\}$ 。

(5) 生成载密图像

通过数据可逆嵌入后，原始像素 $O(x, y)$ 最终

被修改为

$$S'(x, y) = P(x, y) + \Delta' + \text{fd} \quad (2)$$

(6) 更正像素值

若通过生成载密图像步骤计算得到的 S' 值 $0 \leq S' \leq 255$ ，则最终的载密图像像素值 $S(x, y) = S'(x, y)$ ；否则该点像素值超出范围， $S(x, y) = O(x, y)$ ；并在 LM 中将该位置的点标记为 1。按照从左到右、从上到下的顺序计算 $S(x, y)$ ，但到灰色区间时不做任何操作。

(7) 辅助信息嵌入

对 LM 使用稀疏矩阵的压缩算法进行压缩，并使用最末比特位算法^[16]将压缩后的 LM 嵌入 S 的前 r 行的像素中。

2.3 信息提取与图像恢复

信息提取方在得到载密图像后，首先，通过隐藏密钥 E_k 获得与信息嵌入方嵌入时相同的滤波核系数 σ ；然后，使用最末比特位算法提取出 LM 后即可提取秘密信息，借助该位秘密信息恢复出原始载体图像像素值 $O(x, y)$ 。具体工作流程如下。

1) 获取计算位置。如图 3 中三角形像素点所示，以右下角像素为起点扫描 $S(x, y)$ ，同时进行原始图像恢复。此时，图像中已携带信息或被更改的非参考像素与原始图像的像素值不同，而参考像素由于不携带信息未被更改。

2) 计算预测值和滤波值。若 LM 在当前位置的值为 1，表明该点并未携带信息，则更新下一个像素值；否则，根据式(2)计算当前 $S(x, y)$ 的预测值 $P(x, y)$ ，并根据由 σ 计算出的滤波模板对预测值 $P(x, y)$ 进行滤波计算，得出 $C(x, y)$ 。

3) 计算滤波差值和修改预测差值。计算滤波差值 $\text{fd} = C(x, y) - P(x, y)$ ，进而计算得出嵌入秘密信息的修改预测差值 $\Delta' = S(x, y) - P(x, y) - \text{fd}$ 。

4) 提取加密秘密信息。根据对得到的 Δ' 不同取值进行判断即可得到位置 (x, y) 所携带的

$$\text{秘密信息 } m_{(k)} = \begin{cases} \text{mod}(\Delta', 2), & -2T \leq \Delta' \leq 2T + 1 \\ \text{none}, & \text{其他} \end{cases}。$$

5) 计算原始预测差值。在提取出当前像素点 $S(x, y)$ 所携带的加密秘密信息后，计算原始预测

$$\text{差 } \Delta = \begin{cases} (\Delta' - m_{(k)}) / 2, & -2T \leq \Delta' \leq 2T + 1 \\ \Delta' + T, & \Delta' < -2T \\ \Delta' - T - 1, & \Delta' > 2T + 1 \end{cases}。$$

6) 恢复原始像素值。在得到和原始像素值相同的预测值 $P(x, y)$ 和预测差值 Δ 后, 计算得到位置 (x, y) 的原始载体像素值 $O(x, y) = P(x, y) + \Delta$ 。

7) 循环修正图像。恢复载体图像。按照从右到左、从下到上的顺序对像素值进行循环计算, 但到灰色区间时不做任何操作, 在提取信息的同时即可恢复出原始载体图像信息。

8) 解密原始信息。使用加解密密钥 E_K 对加密秘密信息 m 进行解密, 得到前 r 行像素值的 LSB 与秘密信息比特流 s , 并根据最末比特位算法将前 4 行像素值的 LSB 恢复。

2.4 正确性分析

在嵌入阶段, 秘密信息 m 通过对原始载体图像像素值 $O(x, y)$ 按照从左到右、从上到下的顺序修改进行嵌入。对于满足阈值的像素点, 通过对其进行预测差值平移来嵌入秘密信息 m_i , 使平移后的预测差值 Δ' 与秘密信息 m_i 形成对应关系; 信息提取方基于这种对应关系可以正确地提取信息并恢复出原始载体像素值 $O(x, y)$ 。

在载密图像生成过程中, 对于每个像素而言, 无论是否携带秘密信息 m_i , 都需要经过像素值平滑度增强的处理。信息提取方按照与嵌入算法相反的顺序进行处理可以得到每个像素点在嵌入阶段的原始预测值 $P(x, y)$ 和滤波值 $C(x, y)$, 借助预测值 $P(x, y)$ 和滤波值 $C(x, y)$ 恢复出平移后的预测差值即可得到秘密信息和平移前预测差值 Δ , 从而恢复出该点的原始像素值 $O(x, y)$ 。

通过逐层提取恢复, 原始图像恢复的正确性可以达到 100%。进一步, 由式(2)所知, 所提方案的载密图像 $S(x, y)$ 由预测值 $P(x, y)$ 、滤波差值 fd 、嵌入后预测差值 Δ' 叠加而成。因此, 本文方案的正确恢复性由 $P(x, y)$ 、 fd 、 Δ' 的可逆性支撑。

1) 预测值 $P(x, y)$ 的可逆性。在信息提取方进行图像恢复时, 提取信息的顺序与嵌入时是完全相反的。预测器只需要保证当前像素点的左、上、左上方的像素值没有变化即可正确恢复出预测值。按照与嵌入算法相反的顺序进行信息提取, 可以确保信息提取方计算每个像素点时该点的左、上、左上方的像素值已经被正确恢复, 从而保证预测值的可逆性。

2) 滤波差值 fd 的可逆性。在提取信息时, 信息提取方从右下角的非参考像素开始进行计算, 以图 3 中三角形像素点为例, 此时该像素左、上、左上方的像素值均未改变, 由预测值的可逆性可以计算得到与该像素点嵌入时完全相同的预测值 $P(x, y)$ 。由于该点在嵌入算法中是最后一个更新计算的像素点, 此时其周围 3×3 区域内的像素都没有变化, 且卷积的过程是完全可逆的, 故使用预测值 $P(x, y)$ 进行卷积计算后可以得到与嵌入时相同的滤波差值 fd , 以此来达到滤波差值 fd 的可逆性。对于其他位置的像素点来说, 因为提取的顺序与嵌入的顺序相反, 当计算到当前像素点时, 与它相关的像素点已经全部恢复完毕, 从而保证了整张图片平滑效果的可逆性。

3) 嵌入后预测差值 Δ' 可逆性。在嵌入秘密信息时, 预测差值 Δ 的修改结果与所携带的秘密信息一一对应。以图 4 所示的 $\Delta=1$ 为例, 当 $T=1$ 、待嵌入的秘密信息比特为 0 或 1 时, 由式(1)分别得到 Δ' 为 2 或 3, 并且不同的 Δ 在经过式(1)的嵌入后得到的 Δ' 互不相交, 形成了 Δ 、 Δ' 、秘密信息比特之间的一一对应关系。所以, 当信息提取方通过预测值可逆性和滤波差值可逆性计算得到 Δ' 后可以正确提取秘密信息同时获得 Δ 值。综上, 本文方案可保证原始载体信息无损地正确恢复。

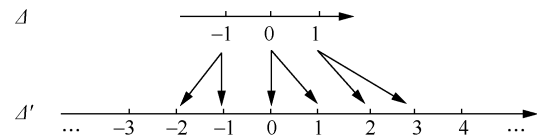


图4 嵌入可逆性示例
Figure 4 Embed reversibility example

此外, 通过在信息嵌入方和信息提取方间共享隐藏密钥 E_K 与秘密信息加密密钥 S_K 构建数据安全传输通道。对于拥有隐藏密钥的信息提取方, 只需要得到载密图像即可完成提取和恢复的步骤, 不需要信息嵌入方传输原始图像。本文通过执行暴力攻击^[17]来分析安全性, 假设攻击者获得了该方案的变换过程并通过特殊方法得到了载密图像, 并在不知道密钥的情况下推断秘密信息, 可以对密钥的可能性进行搜索。由于 AES-256 的加密密钥长度为 256 bit, 且由滤波核系数 σ 组成

的隐藏密钥的密钥空间为 $2^6 \sim 2^7$ ，因此，攻击者通过穷举的方法搜索密钥值的试验次数为 $2^{262} \sim 2^{263}$ ，在现有的计算环境下是无法实现的。

3 实验结果与分析

为验证本文所提方案的有效性和性能，本节对提出的可逆信息隐藏方案进行视觉效果分析、图像质量分析、嵌入容量分析和方案效率分析，并选取经典灰度图像、BOSSBase 数据集^[18]和 LFW 数据集^[19]作为测试对象。其中，BOSSBase 数据集包含 10 000 幅 512×512 的灰度图像，LFW 数据集包含 13 233 幅 250×250 的彩色人脸图像。

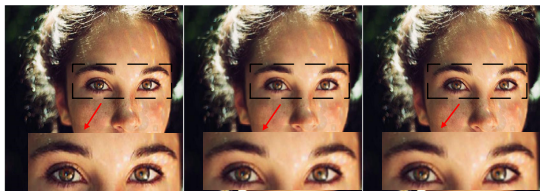
3.1 视觉效果分析

为验证本文方案对载体图像平滑度的增强效果，本文通过对比分析所提方案和高斯滤波方案分别处理后生成的图像矩阵相似度 $r =$

$$\frac{\sum_{i=1}^M \sum_{j=1}^N (A_{mn} - \bar{A})}{\sqrt{(\sum_{i=1}^M \sum_{j=1}^N (A_{mn} - \bar{A})^2) (\sum_{i=1}^M \sum_{j=1}^N (B_{mn} - \bar{B})^2)}} \text{ 进行评估。}$$

其中， M 、 N 为图像宽度与高度， A 、 B 为待评估图像， $\bar{A}$ 、 $\bar{B}$ 为图像像素值平均值。

通过对图 5(a) 的原始图像分别应用高斯滤波方法和本文所提方案生成图 5(b) 和图 5(c)。对比三张图片箭头处区域可以看出，所提方案生成的载密图像与原始图像相比具有一定的平滑效果。



(a) 原始图像 (b) 高斯滤波生成图像 (c) 本文方案生成图像

图 5 视觉质量对比

Figure 5 Contrast of visual quality

进一步，随机选取图 5(a)、图 5(b) 和图 5(c) 中相同位置的 4×4 区域的 R 通道像素值，进行对比分析，如图 6 所示，原始图像中像素值为 40 的点（图 6(a) 红框区域），通过滤波核为 1 的高斯滤波后像素值变为 52（图 6(b) 红框区域），通过本文所提方案处理后变为 47（图 6(c) 红框区域），两者 R 通道像素值相近。证明通过所提

方案可以在一定程度上取得类似高斯滤波的图像平滑效果。

178	40	8	9	169	51	13	9	173	47	10	11
178	40	8	9	170	52	13	9	172	47	10	11
178	40	8	9	170	52	13	9	172	47	10	11
178	41	9	10	170	52	14	10	172	48	11	9

(a) 原始图像像素值 (b) 高斯滤波图像像素值 (c) 本方案图像像素值

图 6 4×4 区域 R 通道像素值对比
Figure 6 Comparison of pixel values of R channel in 4×4 area

最后，选取图 7 中所示的 4 幅 512×512 经典灰度图像，采用所提方案和高斯滤波方案分别进行处理，然后计算所提方案生成图像与原始图像的相似度 r_1 及高斯滤波生成图像的相似度 r_2 。其中，生成高斯滤波图像时的滤波核与所提方案中使用的滤波核相同。

如表 2 所示，相较原始图像，本文所提方案生成的载密图像与经过高斯滤波平滑后的图像有更高的相似度。

表 2 所提方案与高斯滤波图像相似度对比

Table 2 Comparison of image similarity between the proposed scheme and Gaussian filtering image

图像	相似度 r_1	相似度 r_2
Lena	0.987 3	0.996 3
Cameraman	0.987 5	0.997 0
Baboon	0.957 5	0.974 9
Woman	0.979 8	0.987 7

3.2 图像质量分析

为了验证本文所提方案的视觉效果质量，选取图 7 所示的 4 张经典灰度图像，进行结构化相似度 (SSIM, structural similarity)^[20] 和峰值信噪比统计性能分析。其中，SSIM 和 PSNR 越高代表待评估的图像较所对比图像的视觉质量越高，失真率越低。

具体来说，为验证所提方案与高斯滤波方法在视觉质量上的相似度，选取不同的嵌入阈值 T ，分别计算所提方案生成图像、对比方案生成图像与高斯滤波方法生成图像的 SSIM、PSNR，以分析所提方案相对高斯滤波方案的图像质量。为了从多角度验证本文所提方案图像质量，分别选取基于对比度增强的可逆信息隐藏方案^[21]、经典可逆信息隐藏方案^[22]与所提方案进行对比。



图7 经典灰度图像
Figure 7 Classical gray image

如表3所示,在 $T=1$ 时,本文所提方案相较于其他方案可以获得更高的PSNR和SSIM,即所提方案生成的载密图像可以获得与高斯滤波图像更加相近的图像质量。然而,本文所提方案随着 T 增加,像素值的修改幅度相应增大,也会导致图像质量下降。

3.3 嵌入容量分析

本文选择平均每像素所嵌入的比特数(bpp,

$\text{bit per pixel}) = \frac{\text{秘密信息比特数}}{\text{载体图像像素值总值}}$,即嵌入率

作为评判有效负载的关键指标。在所提方案中,使用LSB替换的方法将压缩的位置图嵌入前4行载体图像的LSB中,前4行像素被替换的LSB将作为有效载荷的一部分嵌入覆盖图像中。也就是说,嵌入的有效负载包括:替换的LSB和秘密信息。具体来说,通过测试如图7所示的4幅经典灰度图像在不同阈值下的嵌入率来分析嵌入阈值对载密图像视觉效果和嵌入容量的影响。

测试结果如表4所示,随着嵌入阈值 T 增加,嵌入容量逐渐增大,但载密图像与高斯滤波图像的相似度逐渐变低,同时生成的载密图像的图像质量相应降低。此外,选择文献[21]和文献[22]作为净嵌入容量的对比方案,结果如图8所示。显然,本文所提方案在 $T=1$ 时的嵌入率已明显优于文献[21],在 $T=5$ 时超过文献[22],而且本文方案中随着参数 T 增大嵌入率还会有较大的提高。

3.4 方案效率分析

在Intel Core i5-10210U 1.60 GHz、8.00 GB RAM, Windows10和Eclipse 4.20的测试环境下,

表3 使用不同可逆信息隐藏方案生成载密图像的统计评估
Table 3 The statistic estimation on stego images in terms of different reversible data hiding schemes

载密图像	$T=1$		$T=2$		$T=5$		文献[21]		文献[22]	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Lena	37.346	0.916 8	34.638	0.872 8	28.089	0.797 0	20.000	0.764 9	23.457	0.893 8
Cameraman	35.723	0.898 1	29.044	0.800 9	27.381	0.711 1	22.986	0.755 4	22.682	0.846 4
Baboon	31.996	0.769 9	29.749	0.642 5	25.600	0.607 0	15.720	0.457 1	19.446	0.649 6
Woman	37.392	0.844 5	32.009	0.781 7	28.964	0.716 4	17.348	0.476 4	23.253	0.705 1
均值	32.364 2	0.832 3	28.110	0.761 9	27.508 5	0.707 9	19.014	0.613 5	22.209 5	0.773 7
标准差	4.994 8	0.075 9	2.3828	0.085 1	1.2363	0.067 5	2.755 7	0.146 9	1.620 6	0.099 8

表4 嵌入阈值 T 对嵌入率和载密图像相似度的影响
Table 4 Influence of embedding threshold T on embedding rate and image similarity

测试图像	$T=1$		$T=2$		$T=5$		$T=10$	
	嵌入率/ bit-pixel^{-1}	相似度	嵌入率/ bit-pixel^{-1}	相似度	嵌入率/ bit-pixel^{-1}	相似度	嵌入率/ bit-pixel^{-1}	相似度
Lena	0.328 9	0.996 3	0.523 2	0.981 9	0.763 7	0.975 3	0.900 7	0.967 0
Cameraman	0.190 3	0.997 0	0.293 2	0.980 5	0.517 8	0.972 8	0.729 1	0.962 0
Baboon	0.434 8	0.974 9	0.512 8	0.972 5	0.564 6	0.966 7	0.710 7	0.960 0
Woman	0.315 4	0.987 7	0.450 8	0.974 1	0.687 1	0.965 9	0.853 5	0.954 9
均值	0.317 4	0.989 0	0.445 0	0.977 3	0.633 3	0.970 2	0.798 5	0.961 0
标准差	0.086 7	0.008 9	0.091 9	0.004 0	0.097 4	0.004 0	0.080 6	0.004 3

对本文所提方案的效率进行分析。具体来说, 分别使用 LFW 彩色图像数据集和 Bossbase 灰度图像数据集作为测试对象, 计算每张图在不同嵌入阈值 T 下的平均运行时间。

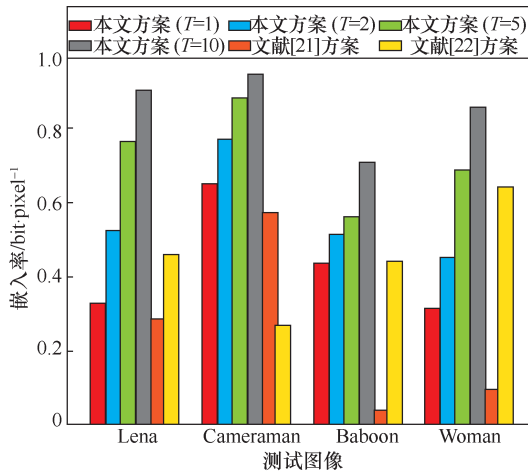


图 8 嵌入率性能对比
Figure 8 Comparison of embedded rate

如表 5 所示, 本文所提方案的信息嵌入和提取过程运行时间开销均较小。其中, 由于 LFW 为彩色图像数据集, 且处理彩色图像时, 需要对 R、G、B 这 3 个通道分别处理, 所以方案的运行时间高于灰度图像 Bossbase 数据集的运行时间。此外, 尽管阈值 T 的不同取值会影响嵌入容量和图像平滑度, 但对方案的运行时间影响较小。因此, 在特定的嵌入容量下, 图像拥有者能够通过选择更小的嵌入阈值 T 来获得更好的图像质量。

4 结束语

本文提出了一种增强图像平滑度的可逆信息隐藏方案, 在保证一定信噪比的同时提升了载密

图像最终的视觉效果。与传统的可逆信息隐藏技术不同, 该方案将图像平滑技术与可逆信息隐藏结合, 使用高斯滤波作为秘密信息嵌入时像素值修改的模板, 通过将预测值与原始像素值的差值作为判别嵌入的条件, 实现信息提取方对原始载体图像和秘密信息完全无损的恢复和提取。实验结果表明, 该方案具有较低的失真率、良好的视觉质量、较高的嵌入率和较短的处理时耗。下一步研究将关注自适应选取预测器以进一步提升图像视觉质量和嵌入容量。

参考文献:

- [1] PROVOS N, HONEYMAN P. Hide and seek: an introduction to steganography[J]. IEEE Security and Privacy Magazine, 2003, 1(3): 32-44.
- [2] NI ZC, SHI Q, ANSARI N, et al. Reversible data hiding[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2006, 16(3): 354-362.
- [3] 何玉芬, 殷赵霞, 汤进, 等. 基于非对称直方图平移的可逆信息隐藏算法[J]. 网络信息安全学报, 2019, 5(5): 80-89.
- [4] ZHOU L M N, HAN H Y, WU H Z. Generalized reversible data hiding with content-adaptive operation and fast histogram shifting optimization[J]. Entropy, 2021, 23(917): 1-20.
- [5] KIM S, QU X C, SACHNEV V. Skewed histogram shifting for reversible data hiding using a pair of extreme predictions[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2019, 29(11): 3236-3246.
- [6] 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.
- [7] LI Y H, CHANG C C, HE M X. High capacity reversible data hiding for VQ-compressed images based on difference transformation and mapping technique[J]. IEEE Access, 2020, 8: 32226-32245.

表 5 嵌入、提取过程运行时间分析
Table 5 Analysis of time of embedding and extraction process

单位: s

数据集	$T=1$		$T=2$		$T=5$		$T=10$	
	嵌入过程 运行时间	提取过程 运行时间	嵌入过程 运行时间	提取过程 运行时间	嵌入过程 运行时间	提取过程 运行时间	嵌入过程 运行时间	提取过程 运行时间
BossBase 数据集	0.078 526	0.018 296	0.066 314	0.019 002	0.061 431	0.019 885	0.065 124	0.017 546
LFW 数据集	0.238 079	0.120 348	0.248 885	0.157 854	0.276 047	0.165 235	0.232 198	0.135 445
均值	0.158 303	0.069 322	0.157 600	0.088 428	0.168 739	0.092 560	0.148 661	0.076 496
标准差	0.079 777	0.051 026	0.091 286	0.069 426	0.107 308	0.072 675	0.083 537	0.058 950

- [8] MANDALI P C, MUKHERJEE I, CHATTERJI B N. High capacity reversible and secured data hiding in images using interpolation and difference expansion technique[J]. Multimedia Tools and Applications, 2021, 80(3): 3623-3644.
- [9] KE Y, ZHANG MQ, LIU J, et al. Fully homomorphic encryption encapsulated difference expansion for reversible data hiding in encrypted domain[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2020, 30(8): 2353-2365.
- [10] LEE C F, JAU J S, YU H L. Data hiding using multi-pixel difference expansion[C]//2018 3rd International Conference on Computer and Communication Systems. 2018: 56-60.
- [11] JAFAR I F, MAGHAYDAH H, DARABKH K A. Employing unsharp masking for contrast enhancement in reversible data hiding[C]//2019 IEEE International Symposium on Signal Processing and Information Technology. 2019.
- [12] WU H T, DUGELAY J L, SHI Y Q. Reversible image data hiding with contrast enhancement[J]. IEEE Signal Processing Letters, 2014, 22(1): 81-85.
- [13] YANG Y, CAI X, XIAO X X, et al. A novel reversible data hiding with skin tone smoothing effect for face images[C]//International Workshop on Digital-forensics and Watermarking. 2019: 204-212.
- [14] WEINBERGER MJ, SEROUSSI G, SAPIRO G. The LOCO-I lossless image compression algorithm: principles and standardization into JPEG-LS[J]. IEEE Transactions on Image Processing, 2000, 9(8): 1309-1324.
- [15] MENEZES A, STEBILA D. The advanced encryption standard: 20 years later[J]. IEEE Security & Privacy, 2021, 19(6): 98-102.
- [16] 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.
- [17] Brute force[EB].
- [18] BAS P, FILLER T, PEVNY T. Break our steganographic system: the ins and outs of organizing BOSS[C]//Proceedings of the 13th International Workshop on Information Hiding, 2011: 59-70.
- [19] Labeled Faces in the Wild[EB].
- [20] ZHOU W, BOVIK A C, SHEIKH H R, et al. Image quality assessment: from error visibility to structural similarity[J]. IEEE Trans Image Processing, 2004, 13(4): 600-612.
- [21] JIA Y J, YIN Z X, ZHANG X P, et al. Reversible data hiding based on reducing invalid shifting of pixels in histogram shifting[J]. Signal Processing, 2019, 163: 238-246.
- [22] KIM S, LUSSI R, QU X, et al. Reversible data hiding with automatic brightness preserving contrast enhancement[J]. IEEE

Transactions on Circuits and Systems for Video Technology, 2019, 29(8): 2271-2284.

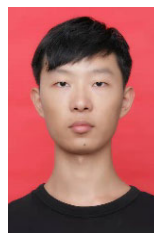
[作者简介]



王婧晗(1998-), 女, 河南新乡人, 西安电子科技大学硕士生, 主要研究方向为信息安全、信息隐藏。



朱辉(1981-), 男, 河南周口人, 西安电子科技大学教授、博士生导师, 主要研究方向为数据安全与隐私保护、安全方案及协议设计、网络及应用安全。



李鹤麟(1996-), 男, 河北保定人, 西安电子科技大学博士生, 主要研究方向为可信推荐、用户行为分析、隐私保护。



李晖(1968-), 男, 陕西西安人, 西安电子科技大学教授、博士生导师, 主要研究方向为密码信息安全、信息论与编码理论。



杨晓鹏(1991-), 男, 河南林州人, 西安电子科技大学博士生, 主要研究方向为生物特征隐私保护、密码学及其应用。