

文章编号: 1007-2780(2012)06-0820-07

基于图像复杂度的隐写算法

张 倩¹, 刘 圆²

(1. 武警工程大学 信息工程系, 陕西 西安 710038, E-mail: zhangqianjy@163.com;
2. 武警云南总队 二支队, 云南 昆明 650020)

摘 要: 提出了一种新的基于图像复杂度的隐写算法。该算法充分利用了复杂度高的图像, 包含更多的信息, 因而能承载更多秘密信息的特点, 将图像划分为 3×3 的图像块, 借助图像块的信息熵和对比度描述图像块的复杂度, 根据各块复杂度统计值确定阈值, 以判定各块复杂度高低, 并针对不同复杂度的图像块进行不同强度的嵌入, 实现了基于图像复杂度的隐写算法。性能分析与实验对比表明, 在相同的嵌入率下, 该算法具有较高峰值信噪比和较强的统计安全性。

关 键 词: 图像复杂度; 熵; 对比度; 隐写算法

中图分类号: TP391 **文献标识码:** A **DOI:** 10.3788/YJYXS20122706.0820

Steganographic Algorithm Based on Image Complexity

ZHANG Qian¹, LIU Yuan²

(1. Department of Information Engineering, Chinese People's Armed Force Engineering University, Xi'an 710038, China, E-mail: zhangqianjy@163.com;
2. The Second Detachment of Yun Nan Corps of CAPF, Kunming 650020, China)

Abstract: A new adaptive steganographic algorithm based on image complexity in space domain was proposed. The algorithm takes full advantage of the image's feature that the image with high complexity contains more information and thus can load more secret message. In order to measure the complexity of image blocks in a better way, the algorithm divides the cover image into 3×3 pixel blocks, and then measures the complexity of blocks by computing information entropy and contrast. After that, the algorithm analyzes the statistics of all the blocks' complexity to get the threshold for evaluating the complexity of every block, and then chooses steganographic algorithms with different strength at the different complexity of blocks. The performance analysis and comparison experiments showed that in the same embedded rate, the proposed algorithm has higher R_{PSN} and stronger statistical security in the same embedded rate.

Key words: mage complexity; entropy; contrast; steganography

1 引 言

随着网络技术的飞速发展, 网络通信使数据传递变得方便快捷。作为信息安全的重要分支, 数字图像隐写已经成为信息安全领域研究的一个

热门课题。图像的复杂程度不仅与人的视觉特性有关, 还与图像的统计特性也有着密切关系, 因而将秘密信息隐藏在图像纹理复杂区域不易引起视觉异常和统计特性的变化。基于图像复杂度的图像隐写技术由于良好的视觉不可见性和统计不可

见性在信息隐藏研究成为一个亮点。

1998年Kawaguchi E等人提出位平面复杂度分割(Bit-Plane Complexity Segmentation, BPCS)密写^[1],该方法定义小块复杂度为所有相邻像素对中取值不同的像素对数目,虽然较LSB^[2]有较好的视觉隐蔽性,但忽略了像素差值对图像复杂度度量的影响。Wu D. C.等人提出的PVD(Pixel-Value Differencing)密写^[3]及改进的PVD密写^[4]根据两个相邻像素的差值来度量人眼对图像的区域敏感性,体现了像素差值对图像复杂度度量的影响,但没有考虑到复杂度与各个方向上的相邻像素的统计特性的关系。随后BPCS算法与PVD算法的改进算法^[5-7]层出不穷,但算法中对图像复杂度的度量都没有同时考虑到以上提出的两个方面。结合上述问题利用像素值转移矩阵定义了每个像素块复杂度,针对不同复杂度的块进行不同程度的数据嵌入。

2 信息隐藏算法及提取原理

在图像复杂度度量中,熵和对比度的衡量权重较其他统计量更重。为了快速全面地度量图像块的复杂度,将图像分为 3×3 的小块,借助信息熵和对比度描述图像块的复杂度,并通过统计各小块复杂度得到度量块复杂度的阈值,利用阈值度量图像块复杂度高低,针对不同复杂度的图像块进行不同强度的嵌入,实现了基于图像复杂度的隐写算法。

2.1 像素块复杂度定义

为了方便计算,算法中取图像块大小为 3×3 ,如图1所示, $x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x$ 分别为图像块各像素值,统计 $x_1, x_2, x_3, x_4, x_5, x_6, x_7, x$ 得到一维像素矩阵形如 $(x_{x_1} \cdots x_{x_7})_{1 \times 8}$ 其中 $i, j \in \{1, 2, 3, 4, 5, 6, 7\}$,统计 $(x_{x_{i_1}} \cdots x_{x_{i_j}})$ 中各元素在图1中出现的比例得到相应的概率矩阵形如 $(\frac{1}{8} p_{i_1} \cdots p_{i_j})_{1 \times 8}$,即 p_{i_j} 表示 x_{i_j} 在图1中出现的比例。利用上述两个矩阵即可提取熵和对比度这两个图像块纹理特征:

(1)熵

$$S = - \sum_{m=1}^j p_{im} \log_2(p_{im}) \quad (1)$$

熵用于表示像素块的纹理随机性,当概率矩阵中 p_{ij} 值均相等时,概率分布最均匀, S 值最大,

像素块包含的信息量多,即块复杂度高,嵌入秘密信息被查觉的概率小;反之亦然。

(2)对比度

$$D = \sum_{m=1}^j |x_{im} - x| p_{im} \quad (2)$$

对比度用于表示像素块纹理清晰度和沟纹深浅,纹理较粗, $|x_{im} - x|$ 较大,则 D 值较大,即块复杂度高,嵌入秘密信息被查觉的概率小;反之亦然。

如图2所示,其所对应的像素矩阵为 $(151 \ 139 \ 144 \ 149 \ 150 \ 153 \ 155)$,相应的概率矩阵为 $(\frac{1}{8} \ \frac{1}{8} \ \frac{1}{4} \ \frac{1}{8} \ \frac{1}{8} \ \frac{1}{8} \ \frac{1}{8})$,由式(1)与式(2)可得 $S=2.75, D=4.375$ 。

x_1	x_2	x_3
x_4	x	x
x_6	x_7	x_7

图1 图像块示意

Fig. 1 Pattern of image blocks

139	144	149
144	151	153
150	155	160

图2 图像块示例

Fig. 2 Example of image blocks

2.2 信息嵌入简介

将秘密信息转化为二进制比特,利用二进制伪随机序列加密后得到预嵌入序列;将图像分成大小为 3×3 的像素块,计算块熵 S 和块对比度 D ,通过熵与对比度确定小块的复杂度,对复杂度高的像素块进行强度较大的嵌入,复杂度低的则进行强度较小的嵌入。

2.3 信息嵌入过程

将秘密信息转化为二进制比特,将转化后的二进制比特与二进制伪随机序列作模2运算,得到加密后的预嵌入序列。将图像分成大小为 3×3 的像素块,计算块熵 S 和块对比度 D ,利用熵与对比度确定小块的复杂度,对复杂度高的像素块进行强度较大的嵌入,复杂度低的则进行强度较小的嵌入。

Step1:秘密信息预处理。将秘密信息转化为

二进制比特,与二进制伪随机序列作模 2 和,保证秘密的机密性。

Step2:将图像分为 3×3 的图像块,计算各图像块的复杂度,并得出度量块复杂度的阈值。利用式(1)和式(2)分别计算每个图像块的熵和对比度,记为 S_i 和 D_i 。设共有 n 个小块,则熵平均值为:

$$\bar{S} = \frac{1}{n} \sum_{i=1}^n S_i \quad (3)$$

对比度平均值为:

$$\bar{D} = \frac{1}{n} \sum_{i=1}^n D_i \quad (4)$$

设度量块复杂度的阈值为 $\alpha\bar{S}, \beta\bar{D}$, 其中, α, β 为视觉敏感度参数, α, β 取值越小,用于度量块复杂度的阈值就越小,判定复杂度为高的像素块就越多,可嵌入的秘密信息量就越多。同时,嵌入后的图像视觉变化会越大,安全性也将随着嵌入量的增加而降低。因而,在视觉敏感度要求较高时,视觉敏感度参数选取较高的值;在视觉敏感度要求低时,视觉敏感度参数选取较低的值。一般情况下 $\alpha, \beta \in [0, 10]$, 大多数情况下 α, β 取值均为 1,即以熵和对比度的平均值为阈值。

Step3:判定块复杂度,进行信息嵌入。步骤如下:

1. 取 3×3 的像素块,如图 1,若 $S_i \geq \alpha\bar{S}, D_i \geq \beta\bar{D}$,则判定块复杂度为高,此时,令标记位 $x_8 \bmod 2 = 1$,即标记位最低比特位为 1;其余情况则令 $x_8 \bmod 2 = 0$ 。

2. 当 $x_8 \bmod 2 = 0$ 时,块复杂度为低,能承载的秘密信息相对少,选择如下嵌入算法:

记 $(x_i - x) \bmod 2 = \Delta x_i, 1 \leq i \leq 7$, 设有二进制秘密比特序列为 $s_1 s_2 s_3 s_4 s_5 s_6 s_7$, 通过改变 x_i 和 x 的值使 Δx_i 的值与嵌入的二进制秘密比特位 s_i 相等。根据 $(s_{ij} - \Delta x_{ij}) \bmod 2$ 值的不同,有如下 8 种情况:

- (1) $\forall j, 1 \leq j \leq 7, s_{ij} = \Delta x_{ij}$, 不用改动;
- (2) $\forall j, 1 \leq j \leq 6, s_{ij} = \Delta x_{ij}$, 即仅有 $\Delta x_{i7} \neq s_{i7}$, 则令 x_{i7} 加 1 或减 1;
- (3) $\forall j, 1 \leq j \leq 5, s_{ij} = \Delta x_{ij}$, 即 $\Delta x_{i6} \neq s_{i6}, \Delta x_{i7} \neq s_{i7}$, 则令 x_{i6} 加 1 或减 1, x_{i7} 加 1 或减 1;
- (4) $\forall j, 1 \leq j \leq 4, s_{ij} = \Delta x_{ij}$, 即 $\Delta x_{i5} \neq s_{i5}, \Delta x_{i6} \neq s_{i6}, \Delta x_{i7} \neq s_{i7}$, 则令 x_{i5} 加 1 或减 1, x_{i6} 加 1 或减 1, x_{i7} 加 1 或减 1;

(5) $\forall j, 1 \leq j \leq 3, s_{ij} = \Delta x_{ij}$, 即 $\Delta x_{i4} \neq s_{i4}, \Delta x_{i5} \neq s_{i5}, \Delta x_{i6} \neq s_{i6}, \Delta x_{i7} \neq s_{i7}$, 则令 x_{i4} 加 1 或减 1, x_{i5} 加 1 或减 1, x_{i6} 加 1 或减 1, x_{i7} 加 1 或减 1;

(6) $\forall j, 1 \leq j \leq 2, s_{ij} = \Delta x_{ij}$, 即仅有 $s_{i1} = \Delta x_{i1}, s_{i2} = \Delta x_{i2}$, 则令 x 加 1 或减 1, x_{i1} 加 1 或减 1, x_{i2} 加 1 或减 1;

(7) 仅有 $s_{i1} = \Delta x_{i1}$, 则令 x 加 1 或减 1, x_{i1} 加 1 或减 1;

(8) $\forall j, 1 \leq j \leq 7, s_{ij} \neq \Delta x_{ij}$, 则令 x 加 1 或减 1;

特别地,以上 8 种情况中当 $x=0$ 或 $x_{ij}=0$ 时选择加 1;当 $x=255$ 或 $x_{ij}=255$ 时选择减 1;其余情况中对像素改动时选择加 1 还是减 1 由二进制伪随机决定。这样可在嵌入秘密时更少地改变直方图的统计特性,同时,在信息提取时不需要二进制伪随机序列也可以提取秘密信息。

3. 当 $x_8 \bmod 2 = 1$ 时,块复杂度为高,能承载的秘密信息相对多,选择如下算法:

记 $(x_i - x) \bmod 3 = \Delta x_i, 1 \leq i \leq 7$, 设有三进制秘密比特序列为 $s'_1 s'_2 s'_3 s'_4 s'_5 s'_6 s'_7$, 通过改变 x_i 和 x 的值使 Δx_i 的值与嵌入的三进制秘密比特位 s'_i 相等。根据 $(s'_{ij} - \Delta x_{ij}) \bmod 3$ 的值的不同,有如下 7 种情况:

- (1) $\forall j, 1 \leq j \leq 7, s'_{ij} = \Delta x_{ij}$, 不用改动;
- (2) $\forall j, 1 \leq j \leq 7, (s'_{ij} - \Delta x_{ij}) \bmod 3 = 1$, 则令 x 减 1 或加 2;
- (3) $\forall j, 1 \leq j \leq 7, (s'_{ij} - \Delta x_{ij}) \bmod 3 = 2$, 则令 x 加 1 或减 2;
- (4) $\forall j, 1 \leq j \leq 7, (s'_{ij} - \Delta x_{ij}) \bmod 3 = 0$ 或 $(s'_{ij} - \Delta x_{ij}) \bmod 3 = 1$ 时,即 $(s'_{ij} - \Delta x_{ij}) \bmod 3$ 结果仅存在 0 或 1 的情况时,使用 $x_8 \bmod 2 = 0$ 时的算法,此处不再重复;
- (5) $\forall j, 1 \leq j \leq 7, (s'_{ij} - \Delta x_{ij}) \bmod 3 = 0$ 或 $(s'_{ij} - \Delta x_{ij}) \bmod 3 = 2$ 时,即 $(s'_{ij} - \Delta x_{ij}) \bmod 3$ 结果仅存在 0 或 2 的情况时,使用 $x_8 \bmod 2 = 0$ 时的算法,此处不再重复;
- (6) $\forall j, 1 \leq j \leq 7, (s'_{ij} - \Delta x_{ij}) \bmod 3 = 1$ 或 $(s'_{ij} - \Delta x_{ij}) \bmod 3 = 2$ 时,即 $(s'_{ij} - \Delta x_{ij}) \bmod 3$ 结果仅存在 1 或 2 的情况时,则有如下 6 种情况:
 - ① $\forall j, 1 \leq j \leq 6, (s'_{ij} - \Delta x_{ij}) \bmod 3 = 2$, 即仅有 $(s'_{i7} - \Delta x_{i7}) \bmod 3 = 1$ 时,令 x 加 1 或减 2, x_{i7} 加 2 或减 1;
 - ② $\forall j, 1 \leq j \leq 5, (s'_{ij} - \Delta x_{ij}) \bmod 3 = 2$, 即仅

有 $(s_{i6}' - \Delta x_{i6}) \bmod 3 = 1, (s_{i7}' - \Delta x_{i7}) \bmod 3 = 1$ 时,令 x 加 1 或减 2、 x_{i6} 加 2 或减 1、 x_{i7} 加 2 或减 1;

③ $\forall j, 1 \leq j \leq 4, (s_{ij}' - \Delta x_{ij}) \bmod 3 = 2$, 即有 $(s_{i5}' - \Delta x_{i5}) \bmod 3 = 1, (s_{i6}' - \Delta x_{i6}) \bmod 3 = 1, (s_{i7}' - \Delta x_{i7}) \bmod 3 = 1$ 时,令 x 加 1 或减 2、 x_{i5} 加 2 或减 1、 x_{i6} 加 2 或减 1、 x_{i7} 加 2 或减 1;

④ $\forall j, 1 \leq j \leq 3, (s_{ij}' - \Delta x_{ij}) \bmod 3 = 2$, 即有 $\forall j, 4 \leq j \leq 7, (s_{ij}' - \Delta x_{ij}) \bmod 3 = 1$ 时,令 x 加 2 或减 1、 x_{i1} 加 1 或减 2、 x_{i2} 加 1 或减 2、 x_{i3} 加 1 或减 2;

⑤ $\forall j, 1 \leq j \leq 2, (s_{ij}' - \Delta x_{ij}) \bmod 3 = 2$, 即有 $\forall j, 3 \leq j \leq 7, (s_{ij}' - \Delta x_{ij}) \bmod 3 = 1$ 时,令 x 加 2 或减 1、 x_{i1} 加 1 或减 2、 x_{i2} 加 1 或减 2;

⑥ $(s_{i1}' - \Delta x_{i1}) \bmod 3 = 2$, 即有 $\forall j, 2 \leq j \leq 7, (s_{ij}' - \Delta x_{ij}) \bmod 3 = 1$ 时,令 x 加 2 或减 1、 x_{i1} 加 1 或减 2;

⑦ 除以上 6 种情况,计算 $(s_i' - \Delta x_i) \bmod 3 = k$,根据 k 有如下操作:

当 $k=0$ 时,不操作;

当 $k=1$ 时,若 $x_i=255$,则令 $x_i=x_i-2$,否则 $x_i=x_i+1$;

当 $k=2$ 时,若 $x_i=0$,则令 $x_i=x_i+2$,否则 $x_i=x_i-1$ 。

特别地,以上 7 种情况中当 $x=0$ 或 $x_{ij}=0$ 时选择加 1,当 $x=255$ 或 $x_{ij}=255$ 时选择减 2;其余情况中对像素改动时首选加 1,像素修改方式的变化对信息的提取没有影响。

2.4 信息提取过程

Step1:将图像分为 3×3 的像素块如图 1 所示,利用标志位 x_8 判定像素块复杂度,选择相应的提取算法:

(1) 当 $x_8 \bmod 2 = 0$ 时,计算 $(x_i - x) \bmod 2 = \Delta x_i, 1 \leq i \leq 7$,则有 $\Delta x_i = s_i$,即 $(s_1 s_2 s_3 s_4 s_5 s_6 s_7)_2 = (\Delta x_1 \Delta x_2 \Delta x_3 \Delta x_4 \Delta x_5 \Delta x_6 \Delta x_7)_2$;

(2) 当 $x_8 \bmod 2 = 1$ 时,计算 $(x_i - x) \bmod 3 = \Delta x_i, 1 \leq i \leq 7$,则有 $\Delta x_i = s_i'$,即

$$s_1' s_2' s_3' s_4' s_5' s_6' s_7')_3 =$$

$$(\Delta x_1 \Delta x_2 \Delta x_3 \Delta x_4 \Delta x_5 \Delta x_6 \Delta x_7)_3$$

将三进制序列 $(s_1' s_2' s_3' s_4' s_5' s_6' s_7')_3$ 转换为二进制比特流。

Step2:将嵌入过程的 Step1 中所得的二进制比特流与预先的二进制伪随机序列作模 2 和,得

到秘密信息。

在上述过程中,尽管信息嵌入过程相对略为复杂,但是提取过程简单快捷。

3 性能分析与比较

本文通过将图像分为 3×3 的像素块,计算图像块的熵和对比度,利用熵和对比度度量图像块的复杂度,针对不同复杂度的像素块进行不同强度的嵌入,实现了基于图像复杂度的隐写算法,算法在具有较高嵌入容量的同时保证了秘密信息的安全性。

3.1 BT. 656 视频格式时序的产生

安全性、隐写容量和嵌入效率是衡量隐写算法的 3 个重要指标。

本章算法在进行嵌入前先与伪随机序列作模 2 和,保证了秘密消息的机密性。同时块复杂度低时使用的算法也是通过伪随机序列决定像素值加 1 还是减 1,从而使嵌入秘密时更少地改变直方图的统计特性,更好地保证了算法的安全性。

以大小为 512×512 的图像为例,计算其最大嵌入容量和最小嵌入容量,及其相应的嵌入效率。一幅 512×512 的图像可得到 29 127 个 3×3 的像素块,当使用低复杂度像素块的嵌入算法时,嵌入量小;如表 1 所示该算法中出现第一种情况的概率是 $1/128$,此时像素值不需要改动;出现第二种和第七种情况的概率是 $7/128$,此时像素块需要改动的像素值个数分别是 1 个和 2 个;第三种和第六种情况的概率是 $21/128$,此时像素块需要

表 1 低复杂度嵌入算法情况

Table 1 Embedding algorithm with low complexity			
类别	概率	改变像素值个数	
$\forall j, 1 \leq j \leq 7, s_{ij} = \Delta x_{ij}$	$\frac{1}{128}$	0	
$\forall j, 1 \leq j \leq 6, s_{ij} = \Delta x_{ij}$	$\frac{7}{128}$	1	
$\forall j, 1 \leq j \leq 5, s_{ij} = \Delta x_{ij}$	$\frac{21}{128}$	2	
$\forall j, 1 \leq j \leq 4, s_{ij} = \Delta x_{ij}$	$\frac{35}{128}$	3	
$\forall j, 1 \leq j \leq 3, s_{ij} = \Delta x_{ij}$	$\frac{35}{128}$	4	
$\forall j, 1 \leq j \leq 2, s_{ij} = \Delta x_{ij}$	$\frac{21}{128}$	3	
$s_{i1} = \Delta x_{i1}$	$\frac{7}{128}$	2	
$\forall j, 1 \leq j \leq 7, s_{ij} \neq \Delta x_{ij}$	$\frac{1}{128}$	1	

改动的像素值个数分别是 2 个和 3 个;第四种和第五种情况的概率是 35/128,此时像素块需要改动的像素值个数分别是 3 个和 4 个;第八种情况的概率是 1/128,此时像素块需要改动的像素值个数为 1 个;标志位为需要改动得概率为 1/2,那么每个像素块平均改变的像素值为 3.41,能嵌入 7 个二进制秘密信息。一幅图像平均改变的像素个数为 99 215,像素点改变的幅度为 1,可以嵌入 203 889 bit,图像嵌入效率为 2.1。

当使用高复杂度像素块的嵌入算法时,嵌入量大;如表 2 所示,根据 $(s_{ij}' - \Delta x_{ij}) \bmod 3$ 的值的不同,算法中出现第一种情况为全 0 的情况,其概率是 1/2 187,此时像素值不需要改动;第二种情况为仅有 1 的情况,其概率是 1/2 187,此时像素块需要改动的像素值个数为 1 个;第三种情况为仅有 2 的情况,其概率是 1/2 187,此时像素块需要改动的像素值个数为 1 个;第四和第五种情况分别仅有 0 和 1 的情况(含全 0 和全 1 的情况)和仅有 0 和 2 的情况(含全 0 和全 2 的情况),其概率均为 128/2 187,此时与复杂度低的嵌入算法一致,由上述内容可知,此时像素块需要改动的像素值平均个数为 2.9;第六种情况是除去全 1 和全 2 的情况后,仅有 1 和 2 的情况,其概率是 126/2 187,此时像素块需要改动的像素值平均个数为 3.1;第七种情况的概率是 1 806/2 187,此时像素块每个像素点需要改动的概率为 2/3,一个像素块需要改动的平均个数约为 4.6 个;标志位为需

表 2 高复杂度嵌入算法情况

Table 2 Embedding algorithm with high complexity		
类 别	概率	改变像素值个数
$\forall j, 1 \leq j \leq 7, s_{ij}' = \Delta x_{ij}$	$\frac{1}{2\ 187}$	0
$\forall j, 1 \leq j \leq 7, (s_{ij}' - \Delta x_{ij}) \bmod 3 = 1$	$\frac{1}{2\ 187}$	1
$\forall j, 1 \leq j \leq 7, (s_{ij}' - \Delta x_{ij}) \bmod 3 = 2$	$\frac{1}{2\ 187}$	1
$\forall j, 1 \leq j \leq 7, (s_{ij}' - \Delta x_{ij}) \bmod 3 = 0$ 或 $(s_{ij}' - \Delta x_{ij}) \bmod 3 = 1$	$\frac{128}{2\ 187}$	2.9
$\forall j, 1 \leq j \leq 7, (s_{ij}' - \Delta x_{ij}) \bmod 3 = 0$ 或 $(s_{ij}' - \Delta x_{ij}) \bmod 3 = 2$	$\frac{128}{2\ 187}$	2.9
$\forall j, 1 \leq j \leq 7, (s_{ij}' - \Delta x_{ij}) \bmod 3 = 1$ 或 $(s_{ij}' - \Delta x_{ij}) \bmod 3 = 2$	$\frac{126}{2\ 187}$	3.1
其余情况	$\frac{1\ 806}{2\ 187}$	4.6

要改动得概率为 1/2,由上所述,此时每个像素块平均改变的像素值为 4.81,能嵌入 7 个三进制秘密信息,约 11.1 bit 二进制秘密信息,一幅图像平均改变的像素个数为 141 650,基本每个像素点改变的幅度为 1,至少嵌入 323 309 bit,图像嵌入效率为 2.3。表 3 为以上两个强度不同的算法的性能对比。

表 3 不同复杂度时选择的算法性能对比

Table 3 Performance contrast of algorithms with different complexity		
	低复杂度时 的嵌入算法	高复杂度时 的嵌入算法
图像块大小	3×3	3×3
每个图像块平均修改像素个数	3.4	4.8
每个图像块平均嵌入率(bpp)	7	11.1
每个图像块平均嵌入效率	2.1	2.3

3.2 性能比较

为了验证本章算法的安全性,本节以 UCID 图像库^[8]为测试图像库,图像格式均为未经 JPEG 压缩的 24 位彩色 TIFF 图像,大小为 512×384。图 3 为原始图像,图 4 为用本章算法嵌入秘密后的图像,其中视觉敏感度参数 $\alpha=1, \beta=1$ 。以峰值信噪比(PSNR)作为图像质量评价的客观标准,表 4 对库中 5 幅图像隐写后的质量进行了对比。当嵌入率为 0.5 bpp 时,3 个算法的 PSNR 值如表 4 所示。相比 LSB 匹配算法和 PVD 算法,本章算法的 PSNR 值有较大提高。

Pevny 的差分像素邻接矩阵分析法(Subtractive Pixel Adjacency Matrix, SPAM)^[9]根据隐写会改变像素间的独立性这一特点,提取差分图像的一步或二步马尔可夫转移概率矩阵作为特征,能对空域隐写算法和 JPEG 隐写算法进行较好的分析。本节以 SPAM 为特征(特征参数如表 5 所示),选用非线性的径向基函数为核函数(RBF 核)的 SVM 分类器^[9]对特征进行训练和分类。具体方法如下:以嵌入率为 0.5 bpp 对库中的 1 338 张图片分别使用 LSB 匹配算法、PVD 算法及本章算法进行加密,得到 3 组图片。将每组图片平分为互不交迭的两部分,每部分为 669 张图片,一部分用于训练,另一部分用于分类。3 个算法的分析数据如表 6 所示,AN 为原始图像检

出率,AS 为隐写图像检出率,Average 为平均检出率;在嵌入率均为 0.5 bpp 的情况下,本章算法



图 3 原始图片 UCID001
Fig. 3 Original image UCID 001



图 4 隐写图片
Fig. 4 Steganographic image

表 4 三种方案的 PSNR 值对比
Table 4 PSNR values of the three scheme

	PVD (1.5 bpp)	PVD (0.5 bpp)	LSB 匹配 (0.5 bpp)	本方案 (0.5 bpp)
UCID001	40.26	42.08	54.86	60.37
UCID002	39.42	44.90	55.38	61.85
UCID003	40.21	45.86	55.37	63.27
UCID004	37.40	39.89	55.05	59.47
UCID005	36.76	39.27	55.18	57.89

表 5 SPAM 参数表
Table 5 SPAM parameters

类别	T	维数
1st	4	162
2nd	3	686

抵抗 SPAM 分析的能力强于 PVD 算法,与 LSB 匹配算法基本持平,统计不可见性较好。

表 6 SPAM 隐写分析结果
Table 6 Steganalysis of SPAM

	PVD		LSB 匹配		本方案	
	SPAM1st	SPAM2nd	SPAM1st	SPAM2nd	SPAM1st	SPAM2nd
AN	0.7877	0.7900	0.5800	0.6936	0.6100	0.6871
AS	0.8251	0.8517	0.8371	0.9178	0.8212	0.8763
Average	0.8064	0.8334	0.7086	0.8057	0.7156	0.7817

综上所述,与 PVD 算法与 LSB 匹配算法相比,本章算法在嵌入率一定的情况下,具有较好的安全性。

4 结 论

通过计算图像块的熵和对比度,提出了新像素块复杂度的度量算法和高效的像素差嵌入算法。该算法计算各图像小块的复杂度,统计

复杂度阈值,根据复杂高的图像可承载更多像素改动的原则,针对不同复杂度的图像块进行不同强度的嵌入,实现了基于图像复杂度的隐写算法。性能分析表明算法的嵌入效率达到了 2.1~2.3,高于 LSB 算法;通过实验对比,本章算法具有较高的 PSNR 值,同时能够更好地抵抗 SPAM 的分析,具有较好的视觉不可见性和统计不可见性。

参 考 文 献:

[1] Kawaguchi E, Eason R O. Principle and application of BPCS-steganography [J]. *Proceedings of SPIE:Multimedia Systems and Applications*,1998,3528:464-472.

[2] BenderW, Gruhl D,Morimoto N,*et al.* Techniques for data hiding [J]. *IBM System Journal*, 1996, 35 (3,4):313-336.

[3] Wu D C, Tsai W H. A steganographic method for images by pixel-value differencing [J]. *Pattern Recognition*

Letters, 2003,24:1613-1626.

- [4] Zhang X, Wang S. Vulnerability of pixel-value differencing steganography to histogram. [J]. *Pattern Recognition Letters*, 2004,25:331-339.
- [5] Wu H C, Wu N I, Tsai C S, et al. Image steganographic scheme based on pixel-value differencing and LSB replacement methods [J]. *IEE Proc. Image Signal Process*, 2005,152(5):611-615.
- [6] Yang C H, Weng C Y, Wang S J, et al. Varied PVD+ LSB evading detection programs to spatial domain in data embedding systems [J]. *The Journal of Systems and Software*, 2010, 83:1635-1643.
- [7] Lin C C. An information hiding scheme with minimal image distortion [J]. *Computer Standards & Interfaces*, 2011,33:477-484.
- [8] Schaefer G, Stich M. UCID-An uncompressed colour image database [R]. Technical Report, UK; School of Computing and Mathematics, Nottingham Trent University, 2003.
- [9] Pevny T, Bas P, Fridrich J. Steganalysis by subtractive pixel adjacency matrix [C]//*Proceedings of the 11th ACM Multimedia & Security Workshop*, Princeton, NJ:ACM, 2009:75-84.

科技参考文献著录的规则

根据中华人民共和国国家标准“文后参考文献著录规则”(GB/T7714-2005),《液晶与显示》编辑部希望广大作者在向本刊投稿时注意参考文献的著录。

1. 文后参考文献书写格式

期刊:[序号]作者. 文献题名[文献类型标志]. 连续出版物题名:其他题名信息,年份,卷号(期号):起止页码[引用日期]. 获取和访问路径.

例:[1]凌志华. STN-LCD 技术的发展[J]. 液晶与显示,2002,17(4):233-242.

例:[2]李晓东,张庆红,叶瑾琳. 气候学研究的若干理论问题[J]. 北京大学学报:自然科学版,1999,35(1):101-106.

例:[3]邵喜斌,王丽娟,李梅. a-Si:H TFT 亚阈值区 SPICE 模型的研究[J/OL]. 液晶与显示,2005,20(4):267-272. [2005-10-18]. http://www.wanfangdata.com.cn/src/szhqk/wf_szhqk_browser.Asp.

专著:[序号]作者. 题名[文献类型标志]. 析出文献其他责任者//专著主要责任者. 专著题名:其他题名信息. 版本项(第1版略). 出版地:出版者,出版年:析出文献的页码[引用日期]. 获取和访问路径.

例:[4]周其凤,王新久. 液晶高分子[M]. 北京:科学出版社,1994:27-38.

例:[5]日本学术振兴会第142委员会. 液晶器件手册[M]. 黄锡珉,黄辉光,李之熔,译. 北京:航空工业出版社,1992.

例:[6]母国光. 白光光学信息处理及期彩色摄影术[M]//陈星旦. 光学与光学工程,北京:科学出版社,2005:62-72.

例:[7]赵耀东. 新时代的工业工程师[M/OL]. 台北:天下文化出版社,1998[1998-09-26]. <http://www.ie.nthu.edu.tw/inf/ie.newie.htm>(Big5).

例:[8]陈兵,徐寿颐. 新型烷基环己基炔类液晶的合成与性质[C]//2002年中国平板显示会议论文集. 深圳:深圳天马微电子股份有限公司,2002:167-168.

例:[9]闫石. 液晶光控取向膜材料的研究[D]. 长春:中国科学院长春光学精密机械与物理研究所,2001.

例:[10]全国文献工作标准化技术委员会第七分委员会. GB/T5795-1986 中国标准书号[S]. 北京:中国标准出版社,1986.

专利:[序号]专利所有者. 专利题名:专利国别,专利号[文献类型标志]. 公告日期或公开日期[引用日期]. 获取和访问路径.

例:[11]吕永积,王群伟,邵佑军,等. 平板真空摄像器件:中国,ZL95241185.7[P]. 1997-08-09.

(下转 P831)

