一种基于像素块的纹理优先自适应隐写算法

师夏阳[1],马赛兰[1],胡永健[1],周琳娜[2]
(1.华南理工大学电子与信息工程学院,广东广州 510641; 2.北京电子技术应用研究所,北京 100091)

摘 要: 与平坦区域相比,图像纹理区域在结构上表现出更多的随机性,因此将密信嵌入到纹理丰富的区域可获得更好的安全性.本文利用相邻像素的LSB与次低LSB位之间的关系,提出一种基于像素块的纹理优先自适应隐写算法,将密信优先嵌入到复杂纹理区域.所设计的纹理判别准则能结合待嵌入密信长度,自适应选择嵌入区域.针对在嵌密过程中嵌密块可能出现的异常情况,提出一种像素值调整方案,并从理论上证明了其可行性.实验结果表明本文算法比两种经典的LSB算法和一种现有的基于边缘优先的自适应算法具有更高的嵌入效率,且对四种有代表性的隐写分析算法通常具有更强的抵御能力.

关键词: LSB隐写; 图像纹理; 自适应嵌入; 安全性; 隐写分析
中图分类号: TP391 **文献标识码:** A **文章编号:** 0372-2112 (2015)06-1094-07
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.06.009

A Pixel Block-Based Adaptive Steganographic Algorithm with Embedding Priority Given to Image Textures

SHI Xia-yang[1], MA Sai-lan[1], HU Yong-jian[1], ZHOU Lin-na[2]
(1. *School of Electronic and Information Engineering, South China University of Technology, Guangzhou, Guangdong* 510641, *China*;
2. *Beijing Application Institute of Electronic Technology, Beijing* 100091, *China*)

Abstract: Compared with flat regions, image textures have more randomness in structure. As a result, the embedding of secret message in rich textures can obtain better security. Based on the relationship between the least two significant bits of neighboring pixels, we propose a pixel block-based adaptive steganographic algorithm with embedding priority given to image texture regions. In other words, the embedding order is from rich textures to flat regions. Our criterion for texture assessment can adaptively allocate image regions for embedding according to the length of the secret message. To deal with possible irregular embedding blocks, we propose a pixel value modification solution. We have justified this solution mathematically. Experimental results have demonstrated that our algorithm outperforms two established LSB (least significant bit) embedding algorithms and one current edge adaptive steganographic algorithm in terms of embedding efficiency; meanwhile, our algorithm often has stronger resistance to the four representative steganalytic algorithms.

Key words: LSB embedding; image texture; adaptive embedding; security; steganalysis

1 引言

LSBR(LSB Replacement,最小意义位替换)是目前最常用的隐写方法之一,它在嵌入密信时对载体图像的偶数像素加1或者保持不变,但绝不会减小偶数像素;对奇数像素反之亦然.这种操作规则会导致隐写图像像素值统计上的异常,即使在很小嵌入率下,隐写分析者也能检测到密信的存在[1],某些隐写分析算法甚至还可估计出嵌入密信的长度[2].LSBM(LSB Matching)是LSBR的改进算法,通过对像素值随机±1操作,消除了LSBR引起的统计不对称.与LSBR隐写算法相比,LSBM更难检测.事实上,仅利用单个像素值进行隐写时,LSBM隐写算法近乎最优[3].但LSBM算法最大的弱点在于假设了载体图像像素的LSB位之间是不相关的,不能真实反映自然图像的特性.隐写分析者可利用这个弱点攻破LSBM算法[4~7].不同于LSBR和LSBM算法,LSBMR(LSB Matching Revisited)隐写算法[8]利用相邻像素值对作为嵌入单元,实现了两个像素嵌入两个密信比特,具体为第一个像素的LSB位嵌入第一个密信比特,而利用两个像素值的奇偶关系嵌入余下的那个密信比特.通过像素

收稿日期:2014-01-06;修回日期:2014-04-20;责任编辑:梅志强
基金项目:国家973重点基础研究发展计划(No.2011CB707003);广东省自然科学基金团队项目(No.9351064101000003);华南理工大学中央高校基本科研业务费专项资金(No.2014ZZ0036)

对关系嵌入机制,算法的安全性有了明显改善.借助文献[8]的嵌入机制,文献[9]用相邻两个像素的差值判别自然图像的边缘,提出了一种优先利用图像边缘特性进行嵌入的方法,改善了安全性.然而,Tan 等人[10]利用 B-样条函数从含密图像绝对差值直方图拟合出近似原始图像的绝对差值直方图,通过比较拟合前后直方图的局部差异,成功实现了对文献[9]隐写方法的检测.通常利用三个或更多像素作为嵌入单元可提高隐写算法的安全性.最近 Omoomi 等人[11]提出一种多像素 ±1 隐写算法 (EPES),选择多个像素作为一个嵌入单元,利用相邻像素的 LSB 与次低 LSB 位之间的关系,对像素的修改更少,算法的安全性得到进一步改善.本文在文献[11]的基础上提出一种基于图像块的纹理优先自适应嵌入算法,更充分地利用了自然图像的纹理特性,得到比文献[9]更高的嵌入效率和更好的安全性.

2　密信的嵌入和抽取原理

为了利用一个像素对之间的关系嵌入两个比特密信,文献[11]引入了一个刻画次低 LSB 位与最低 LSB 位关系的二值函数 $B(u,v)$:

$$B(u,v)=b_1(u)\oplus b_0(v),\ \forall\ u,v\in Z \tag{1}$$

这里 $b_i(u)$是单变量二值函数,$b_i(u)=\lfloor u/2^i\rfloor \bmod 2$,$i=0,1,2\cdots$,$b_i(u)$表示像素值 u 的第 $i+1$ 个 LSB 位,且 $B(u,v)$有如下两个性质:

性质 1　因为 $b_0(v)=v \bmod 2$,而 $b_0(v)$为 v 的 LSB,必有 $b_0(v+1)=b_0(v-1)=\bar{b}_0(v)$,故当 u 值不变时,v 值的 ±1 操作必然引起 $B(u,v)$值的翻转,即

$$B(u,v+1)=B(u,v-1)=\bar{B}(u,v),\ \forall\ u,v\in Z \tag{2}$$

性质 2　因为 $b_1(u)=\lfloor u/2\rfloor \bmod 2$,而 $b_1(u)$为 u 的次低 LSB,必有 $b_1(u+1)=\bar{b}_1(u-1)$,故当 v 值不变时,u 值的 ±2 操作必然引起 $B(u,v)$值的翻转,则有 $B(u+1,v)=\bar{B}(u-1,v)$;当 u 为偶数时,$b_1(u)=b_1(u+1)$,当 u 为奇数时,$b_1(u)=b_1(u-1)$,即

$$B(u,v)=\begin{cases}B(u+1,v), & u\text{ 为偶数}\\ B(u-1,v), & u\text{ 为奇数}\end{cases},\ \forall\ u,v\in Z.$$

综上,可得二值函数 B 的性质 2:

$$B(u,v)=B(u+(-1)^u,v)=\bar{B}(u-(-1)^u,v),\quad \forall\ u,v\in Z \tag{3}$$

这里 $\bar{b}_i,\bar{B}$ 分别表示 b_i,B 值的翻转.

文献[11]所提出的 EPES 算法的嵌入过程是将上述 B 函数作用于两个相邻像素,利用 B 的两个性质实现 l 个像素值嵌入 l 个比特密信.下面简单介绍其做法.

首先引入一个差异量 d_i 来描述密信与 B 值之间的差异,即:

$$\begin{cases}d_i=m_i\oplus B(x_i,x_{i+1}),\ i\in 1,\cdots,l\\ x_{i+1}=x_1\end{cases} \tag{4}$$

在密信嵌入过程中,根据差异量值 d_i 的变化并结合二值函数 B 的性质确定将要修改的像素值.这里以两个像素的情形(即 $l=2$)为例具体描述密信的嵌入和抽取机制.记 x_1,x_2 和 y_1,y_2 分别为载体和含密像素,m_1,m_2 为待嵌密信比特.EPES 算法设计其密信提取公式

$$\begin{cases}m_1=B(y_1,y_2)\\ m_2=B(y_2,y_1)\end{cases} \tag{5}$$

为了做到这一点,其嵌入过程被精心构造.首先根据式(4)计算差异量 d_1 和 d_2:

$$\begin{cases}d_1=m_1\oplus B(x_1,x_2)\\ d_2=m_2\oplus B(x_2,x_1)\end{cases} \tag{6}$$

然后根据差异量 d_1,d_2 的四种组合,并结合二值函数 B 的性质,按表 1 修改像素值 x_1,x_2.具体为:若 $d_1=0$ 且 $d_2=0$,则由式(6)可知,要嵌入的密信 m_1 和 m_2 与两个载体像素 x_1 和 x_2 的 B 函数满足异或关系,即有 $m_1=B(x_1,x_2)$和 $m_2=B(x_2,x_1)$,故在嵌入时对 x_1 和 x_2 不做修改,即 $y_1=x_1,y_2=x_2$.则抽取时仍有 $m_1=B(y_1,y_2),m_2=B(y_2,y_1)$.若 $d_1=0$ 且 $d_2=1$,则由式(6)可知 $m_1=B(x_1,x_2)$且 $m_2\neq B(x_2,x_1)$.要使 $m_1=B(y_1,y_2)$成立,根据式(2)和式(3),须满足 $y_2=x_2$ 或 $y_1=x_1+(-1)^{x_1}$;另一方面,为了使 $m_2=B(y_2,y_1)$,可使 $B(y_2,y_1)=\bar{B}(x_2,x_1)$,则只要 $y_2=x_2-(-1)^{x_2}$或 $y_1=x_1\pm 1$ 就行.显然,$y_1=x_1+(-1)^{x_1}$且 $y_2=x_2$ 可同时使式(5)成立.同理可分析 $d_1=1$ 且 $d_2=0$ 和 $d_1=1$ 且 $d_2=1$ 的情况.归总可得表 1 所示的嵌入方式.

表 1　$l=2$ 时密信嵌入查找表

d_1d_2	y_1	y_2
00	x_1	x_2
01	$x_1+(-1)^{x_1}$	x_2
10	x_1	$x_2+(-1)^{x_2}$
11	$x_1-(-1)^{x_1}$	x_2

若一次嵌入 3 个比特的密信 m_1,m_2 和 $m_3(l=3)$,则可利用三个载体像素 x_1,x_2 和 x_3,得到含密像素 y_1,y_2 和 y_3,使其满足 $m_1=B(y_1,y_2)$,$m_2=B(y_2,y_3)$,$m_3=B(y_3,y_1)$.广义而言,可利用 l 个载体像素嵌入 l 个比特密信,其抽取关系仍为

$$\begin{cases}m_i=B(y_i,y_{i+1})\\ y_{i+1}=y_1\end{cases},\ i\in 1,\cdots,l \tag{7}$$

3　容量自适应嵌入算法的设计

将密信嵌入到纹理区域更不易被人眼所察觉,因此本文提出纹理优先的原则自适应选择嵌入区域.首先引入一个简单判别图像局部复杂度的准则.将尺寸为 $p\times q$ 的载体图像划分为互不相交的大小为 $m\times n$ 的块 $\boldsymbol{D}_{i,j}$,定义该块纹理复杂度 block($\boldsymbol{D}_{i,j}$)为:

$$\text{block}(\boldsymbol{D}_{i,j}) = \text{Sum}(\boldsymbol{D}_{i,j}) - m \times n \times \text{Min}(\boldsymbol{D}_{i,j}) \quad (8)$$

这里 $\text{Sum}(\boldsymbol{D}_{i,j})$为块内全体像素值之和,$\text{Min}(\boldsymbol{D}_{i,j})$为块内的最小像素值,$i \in 1,2,\cdots,\lfloor p/m \rfloor$,$j \in 1,2,\cdots,\lfloor q/n \rfloor$.对于一个给定阈值 T,若 $\text{block}(\boldsymbol{D}_{i,j}) \geq T$,则认为 $\boldsymbol{D}_{i,j}$是纹理区域;否则,则认为 $\boldsymbol{D}_{i,j}$是平坦区域.本文将密信嵌入到所选中的纹理块中.可通过调整 T 值来控制嵌入容量.若密信长度为 M,则可用下述方法求门限 T:

$$T = \arg\max_{t} \{ m \times n \times \boldsymbol{D}(t) \geq M \} \quad (9)$$

这里,$\boldsymbol{D}(t) = \{ \boldsymbol{D}_{i,j} \mid \text{block}(\boldsymbol{D}_{i,j}) \geq t \}$,$i \in 1,2,\cdots,\lfloor p/m \rfloor$,$j \in 1,2,\cdots,\lfloor q/n \rfloor$,且 $\boldsymbol{D}(t)$为 $\text{block}(\boldsymbol{D}_{i,j})$的值大于或者等于参数 t 的集合.

下面用一个例子具体描述单块密信的嵌入和提取过程.在嵌入密信前,先对每个待嵌块从左上角开始进行 Zigzag 扫描,生成像素序列.嵌入密信完成后重新还原成像素块.密信提取时与嵌入的扫描方式相同.设块大小为 2×2,阈值 $T = 8$,扫描得到的像素序列为 $(x_1, x_2, x_3, x_4) = (22,25,27,24)$,由式(8)可得 $\text{block}(\boldsymbol{D}_{i,j}) = 10 > 8$,则此块为待嵌块.若待嵌密信为 $(m_1, m_2, m_3, m_4) = (1,0,1,1)$,计算差异量 d_i,可得

$$\begin{cases} d_1 = 1 \oplus B(22,25) = 1 \oplus (1 \oplus 1) = 1, \\ d_2 = 0 \oplus B(25,27) = 0 \oplus (0 \oplus 1) = 1, \\ d_3 = 1 \oplus B(27,24) = 1 \oplus (1 \oplus 0) = 0, \\ d_4 = 1 \oplus B(24,22) = 1 \oplus (0 \oplus 0) = 1. \end{cases}$$

此时,4 个比特分别嵌入 4 个像素对:(x_1, x_2),(x_2, x_3),(x_3, x_4),(x_4, x_1).根据表 1 并综合考虑 x_1, x_2, x_3, x_4 这 4 个像素之间的关系,只需修改 x_1 和 x_3 就行,具体为 $y_1 = 22 - (-1)^{22} = 21$ 和 $y_3 = 27 + (-1)^{27} = 26$.抽取时,扫描此块后像素序列为 $(y_1, y_2, y_3, y_4) = (21,25,26,24)$,按式(8)进行判断,有 $\text{block}(\boldsymbol{D}'_{i,j}) = 11 > 8$,则为嵌入块.利用式(5)抽取密信,有 $m_1 = B(21,25) = 1$,$m_2 = B(25,26) = 0$,$m_3 = B(26,24) = 1$,$m_4 = B(24,21) = 1$.可见所抽取出的密信与原始密信完全一致.

4 问题与解法

上述自适应算法将对 $\text{block}(\boldsymbol{D}'_{i,j}) \geq T$ 的块抽取密信,但可能出现嵌入密信后像素块不满足提取条件的情况.仍用上例来解释,只将待嵌密信改为 $(m_1, m_2, m_3, m_4) = (0,1,1,1)$.由于此时 $(d_1, d_2, d_3, d_4) = (0,0,0,1)$,根据 4 个像素之间的关系,只需修改一个像素 x_1,且改动为 $y_1 = x_1 + (-1)^{x_1} = 23$.所得嵌密像素序列为 $(y_1, y_2, y_3, y_4) = (23,25,27,24)$.异常发生在抽取端.当抽取时,由式(8)可知 $\text{block}(\boldsymbol{D}'_{i,j}) = 7 < 8$,不满足抽取条件,这就造成密信丢失.本文称这类块为异常块.

为解决上述问题,本文提出一种像素值调整方案使得调整后的块仍满足抽取条件.具体做法是对异常块 $\boldsymbol{D}'_{i,j}$内的每一个像素值进行 $\pm 4k$ 操作,即

$$y' = y \pm 4k, \ k = 0, \pm 1, \pm 2, \cdots.$$

为了保证上述操作不影响密信的抽取,调整后块中的像素序列需满足下列条件:

$$B(u,v) = B(u \pm 4k, v \pm 4k), k = 0, \pm 1, \pm 2, \cdots.$$

定理 1 $\forall u, v \in N$,存在整数 k,$k = 0, \pm 1, \pm 2, \cdots$,使得函数 $B(u,v)$的值与函数 $B(u \pm 4k, v \pm 4k)$的值恒相等.

证明 根据 B 函数的定义式(1)可得

$$B(u \pm 4k, v \pm 4k) = \{\lfloor (u \pm 4k)/2 \rfloor \bmod 2\} \oplus \{(v \pm 4k) \bmod 2\} \quad (10)$$

首先考察式(10)右边异或操作的后项,因为 $\pm 4k$ 恒为偶数,那么任一正整数 v 加上 $\pm 4k$,其奇偶性不变,恒有 $v \bmod 2 = = (v \pm 4k) \bmod 2$,即 $b_0(v) = b_0(v \pm 4k)$.又考察式(10)等号右边异或操作的前项 $\lfloor (u \pm 4k)/2 \rfloor \bmod 2$.因为 $\pm 4k$ 恒为偶数,则有

$$\lfloor (u \pm 4k)/2 \rfloor \bmod 2 = (\lfloor u/2 \rfloor + \lfloor \pm 2k \rfloor) \bmod 2$$

下面分成两种情形进行讨论:

(1)当 u 为偶数时,则 $\lfloor u/2 \rfloor = u/2$,且 $(\lfloor u/2 \rfloor + \lfloor \pm 2k \rfloor)$的奇偶性与 $\lfloor u/2 \rfloor$相同,则 $(u/2 + \lfloor \pm 2k \rfloor) \bmod 2 = (u/2) \bmod 2$,那么 $b_1(u \pm 4k) = b_1(u)$.

(2)当 u 为奇数时,$\lfloor u/2 \rfloor = (u-1)/2$,且 $(\lfloor u/2 \rfloor + \lfloor \pm 2k \rfloor)$的奇偶性与 $\lfloor u/2 \rfloor$相同,则 $(u-1)/2 + \lfloor \pm 2k \rfloor \bmod 2 = (u-1)/2 \bmod 2$,那么 $b_1(u \pm 4k) = b_1(u)$.

综上,必有

$$B(u,v) = B(u \pm 4k, v \pm 4k), k = 0, \pm 1, \pm 2, \cdots$$

成立.

证毕.

参数 k 的大小直接影响异常块中像素值的调整,且存在不同的 k 值满足调整方案.为了使得对载体图像的改动尽可能小,并使调整后的像素值仍落在 0 到 255 范围内,本文提出一种寻找 k 值的优化方案

$$\begin{aligned} &\min \sum_{m \times n} | y' - y | \\ &\text{s.t.} \quad 0 \leqslant y' \leqslant 255 \\ &y' = y \pm 4k, k = 0, \pm 1, \pm 2, \cdots \end{aligned} \quad (11)$$

这里 y 表示 $\boldsymbol{D}'_{i,j}$块内的像素值,y' 表示 $\boldsymbol{D}''_{i,j}$块内的像素值.仍用上例解释本文的调整方案.调整前 $(y_1, y_2, y_3, y_4) = (23,25,27,24)$,有 $\text{block}(\boldsymbol{D}'_{i,j}) = 7 < 8$,根据式(11)对含密像素值 y 进行调整.解得最优调整参数 $(k_1, k_2, k_3, k_4) = (-1,0,0,0)$,则

$$(y_1', y_2', y_3', y_4') = (y_1, y_2, y_3, y_4) + (4k_1, 4k_2, 4k_3, 4k_4)$$
$$= (23, 25, 27, 24) + (-4, 0, 0, 0)$$
$$= (19, 25, 27, 24)$$

此时,
$$\begin{cases} B(y_1', y_2') = B(23, 25) = 1 \oplus 1 = 0, \\ B(y_2', y_3') = B(25, 27) = 0 \oplus 1 = 1, \\ B(y_3', y_4') = B(27, 24) = 1 \oplus 0 = 1, \\ B(y_4', y_1') = B(24, 23) = 0 \oplus 1 = 1. \end{cases}$$

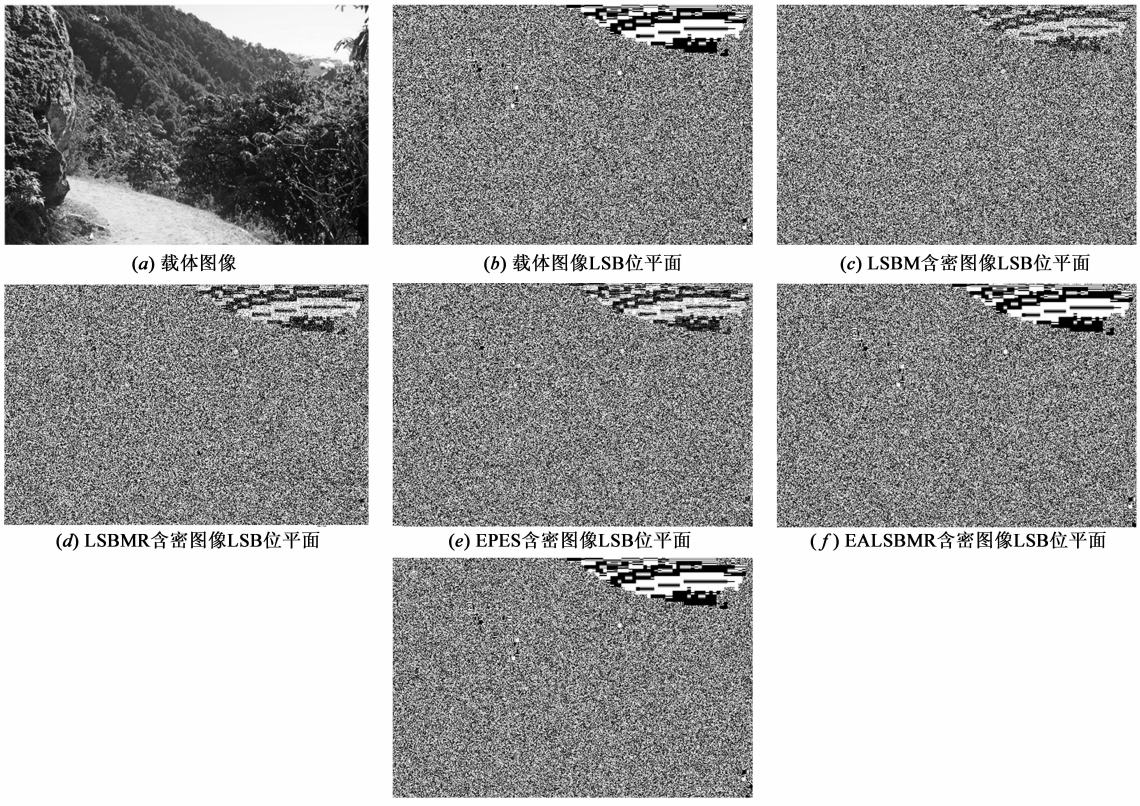
显然,调整前后函数 B 的值不变,但 $\text{block}(\boldsymbol{D}_{i,j}') = 19 > 8$,满足抽取条件,即调整后的块 $\boldsymbol{D}_{i,j}''$仍能被正确地判别含密块.

值得指出的是,LSB 隐写算法存在一个普遍的问题:当载体图像的像素值为 0 或 255 时,对 LSB 位的 -1 或 +1 操作会导致像素值边界的溢出.为解决上述问题,本文对满足嵌入条件的块进行预处理.若预嵌入块中含有 0(或者 255),则将 0 变为 1(255 变为 254).这就避免了嵌入溢出问题.

5　隐写性能比较与安全性分析

5.1　密信嵌入位置分析

图 1 显示 5 种隐写算法(即 LSBM, LSBMR, EALSBMR[9], EPES[11]和本文算法)对含密图像的 LSB 位平面的影响.实验在灰度图像上进行,且本文算法在嵌入密信时采用 3×3 分块.传统基于 LSB 的隐写算法通常假设 LSB 位的值是随机的,但图 1(*b*)右上角显示天空位置的 LSB 值有一定的结构性,这里是整块的白或黑,故传统算法或多或少的破坏了载体图像平坦区域的 LSB 位平面结构.图 1(*c*)显示 LSBM 算法将密信随机散布在载体图像中,使得平坦区域也嵌入了密信,白色区域出现了黑点而黑色区域也出现了白点,从而降低了图像的视觉质量,影响了隐写算法的安全性.LSBMR 是 LSBM 的改进,比较图 1(*c*)和图 1(*d*)发现,LSBMR 算法对平坦区域的 LSB 位平面结构分布的破坏有所减弱.EPES 算法同样是基于 LSB 的 ±1 修改,不过它利用了相邻像素 LSB 与次低 LSB 之间的关系,进一步降低了像素的修改概率,观察图 1(*e*)发现,与 LSBMR 和 LSBM 相比,EPES 在保留平坦区域结构分布方面有进一步改善.为了减小对自然图像平坦区域结构分布的破坏,EALSBMR 利用像素对的差值为依据,把密信比特嵌入到自然图像的边缘.图 1(*f*)显示,EALSBMR 对平坦区域的结构保留完好,仅能观察到一些边缘处的毛刺.图 1(*g*)是本文算法的结果,与图 1(*f*)比,几乎观察不到平坦区结构分布的变化.为了更清楚地说明本文算法对平坦区域的影响,我们将图 1(*b*),图 1(*f*)和图 1(*g*)右上角分别放大为图 2(*a*)、图 2(*b*)和图 2(*c*).对比可发现,EALSBMR 边缘毛刺较明显,而且在一些全白的区域



(*a*) 载体图像　(*b*) 载体图像LSB位平面　(*c*) LSBM含密图像LSB位平面

(*d*) LSBMR含密图像LSB位平面　(*e*) EPES含密图像LSB位平面　(*f*) EALSBMR含密图像LSB位平面

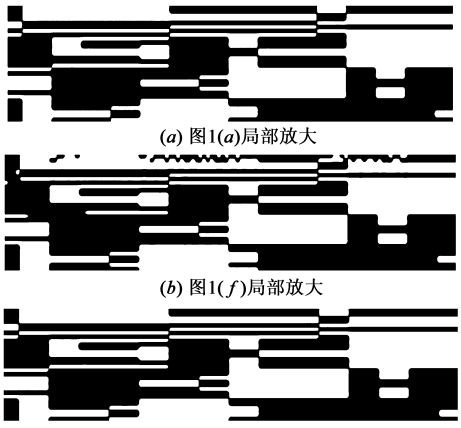
(*g*) 本文算法含密图像LSB位平面

图 1　载体图像LSB位平面和5种隐写算法嵌入率为0.5bpp的含密图像LSB位平面

还出现了较大黑点.图 2(*c*)与图 2(*a*)最接近,原因是本文算法优先将密信比特隐藏到载体图像的纹理区域,最大限度保留了载体图像平坦区域的结构.

5.2 嵌入效率比较

嵌入效率 EE(Embedding Efficiency)定义为嵌入率 ER(Embedding Rate)和嵌入改变率 CR(Change Rate)的比值[11].同样与 LSBM,LSBMR,EALSBMR,EPES 进行比较.由于篇幅所限,这里仅给出 Baboon,Lena 和 Boat 的实验结果.图像大小为 512×512.图 3 显示在相同嵌入率下本文算法的嵌入效率明显高于 LSBM,LSBMR 和 EALSBMR 隐写算法,而与 EPES 相近,这是因为本文算法继承了 EPES 的优点,同时利用相邻像素 LSB 与次低 LSB 之间的关系,从而减少了嵌入对像素的修改.由于本文算法与 EPES 在嵌入位置上有差异,所以两者的曲线有细微的不同.

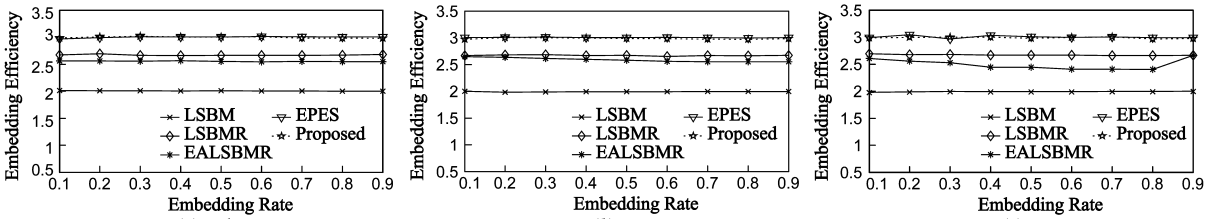


(*a*) 图1(*a*)局部放大

(*b*) 图1(*f*)局部放大

(*c*) 图1(*g*)局部放大

图2 图1(*a*)、图1(*f*)和图1(*g*)右上角平坦区域LSB位平面相同位置的局部放大



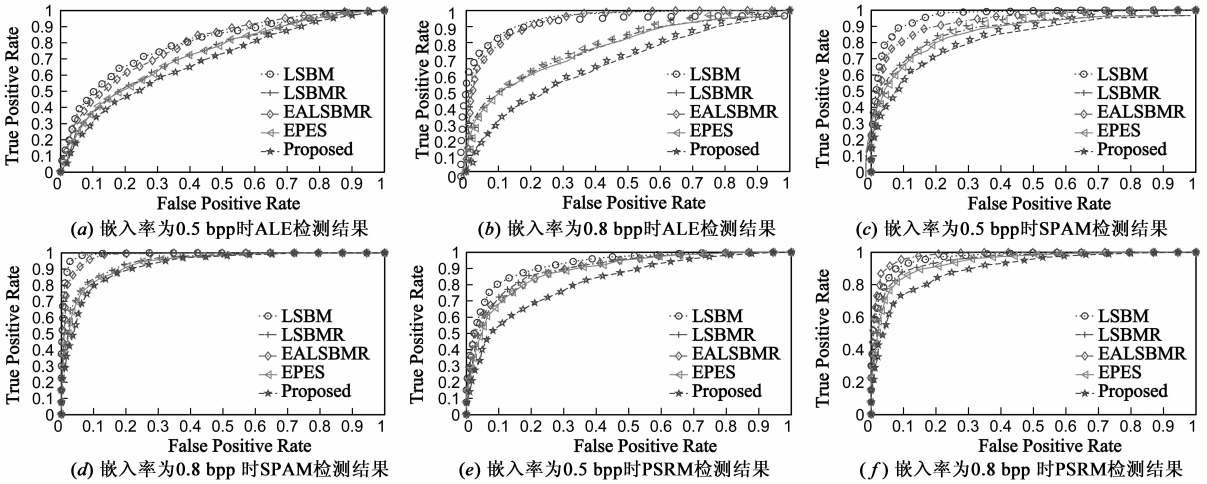
(*a*) Baboon (*b*) Lena (*c*) Boat

图3 相同嵌入率下LSBM,LSBMR,EALSBMR, EPES与本文算法嵌入效率比较

5.3 抗隐写分析攻击能力评估

安全性是评估隐写算法性能的重要指标之一.本文使用两种主流和一种最新的通用隐写分析算法来评估隐写算法的安全性,它们按顺序分别是基于直方图极值的隐写分析算法(ALE)[6],基于灰度图像的高阶马尔科夫链(SPAM)隐写分析算法[7]和基于投影空间富模型(Projection Spatial Rich Model,PSRM)的隐写分析算法[12].其中文献[12]不同于传统的基于共生矩阵的隐写分析算法(例如文献[7]),对图像残差引入一种新的统计描述子,从而获得更好的检测性能.该算法既可检测空域隐写,也可检测压缩域隐写.本文实验在 UCID[13]和 NRCS[14]这两个常用的图像库中进行.UCID 和 NRCS 数据库分别包含 1338 幅 TIFF 图像和 3148 幅 TIFF 图像,其中 UCID 图像大小分为 512×384 和 384×512 两种,NRCS 原始图像较大,为计算方便,以图像中心为基准,剪切成 512×512 大小.全部实验在灰度图像中进行.

图 4 和图 5 分别显示 ALE(10 维特征),SPAM(686 维特征)和 PSRM(12870 维特征)对 5 种隐写算法检测的

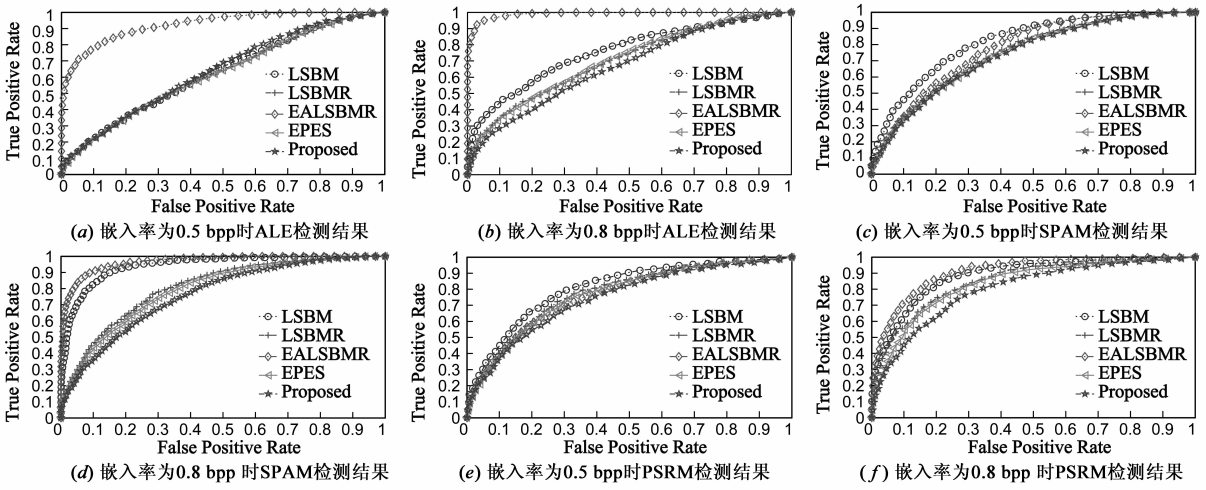


(*a*) 嵌入率为0.5 bpp时ALE检测结果 (*b*) 嵌入率为0.8 bpp时ALE检测结果 (*c*) 嵌入率为0.5 bpp时SPAM检测结果

(*d*) 嵌入率为0.8 bpp 时SPAM检测结果 (*e*) 嵌入率为0.5 bpp时PSRM检测结果 (*f*) 嵌入率为0.8 bpp 时PSRM检测结果

图4 在UCID图像库中ALE、SPAM和PSRM检测的ROC曲线图

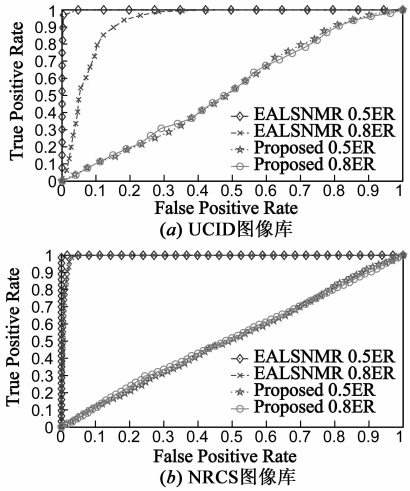
ROC 曲线(接收机工作特性曲线).图 4 显示,在 UCID 图像库中,本文算法的 ROC 曲线明显最偏向于右下,说明本文算法的隐写最难被发现.图 5 是 NRCS 图像库的检测结果.在嵌入率为 0.5bpp 时,图 5(a)显示本文算法的 ROC 曲线与 LSBM,LSBMR,EPES 的曲线很接近,说明此时这 4 种算法的抗隐写分析能力接近.出现这种现象的原因可能是 NRCS 库中的图像为扫描图像,因此含有扫描设备噪声,对检测所用的局部极值振幅特征影响较大,故干扰了 ALE 算法的检测结果.另一方面,图 5(c)显示 SPAM 算法的表现.本文算法的 ROC 曲线最偏向于右下,其次是 EPES,它们都低于 LSBM,LSBMR 和 EALSBMR,说明本文算法抗 SPAM 分析的能力最强.而图 5(e)是 PSRM 算法的表现.LSBM 的 ROC 曲线最偏于左上方,LSBMR,EALSBMR 和 EPES 三种算法的性能基本接近,此时本文算法的 ROC 曲线仍位于最右下,比较说明本文算法抗 PSRM 分析能力最强.当嵌入率增加到 0.8bpp 时,本文算法的 ROC 曲线更偏右下方,如图 5(b)、图 5(d)和图 5(f)所示.对于 SPAM 而言,为了降低维数灾难,SPAM 优先以图像的平坦区域为检测对象,对图像纹理区域的特征描述相对弱一些,而本文算法则是优先利用纹理区域进行嵌入,故对 SPAM 有较明显的抗分析能力.值得指出的是图 5(a)和图 5(b)显示 EALSBMR 的 ROC 曲线较其它四种算法更大幅度地靠近左上角,反映其抗 ALE 攻击能力最弱.出现上述现象的原因可能是 NRCS 是扫描图像库,扫描操作引入了扫描噪声,而 EALSBMR 算法一次只利用两个相邻像素(水平或垂直)的差值来简单判别图像边缘,故这些因扫描而引入的高频噪声对其检测结果有较明显的影响.



(a) 嵌入率为0.5 bpp时ALE检测结果　(b) 嵌入率为0.8 bpp时ALE检测结果　(c) 嵌入率为0.5 bpp时SPAM检测结果

(d) 嵌入率为0.8 bpp 时SPAM检测结果　(e) 嵌入率为0.5 bpp时PSRM检测结果　(f) 嵌入率为0.8 bpp 时PSRM检测结果

图5　在NRCS图像库中ALE、SPAM和PSRM检测的ROC曲线图



(a) UCID图像库

(b) NRCS图像库

图6　文献[10]中算法对本文算法和EALSBMR检测的ROC曲线图

除了上述抗通用隐写分析能力,本文算法对文献[10]中专用的隐写分析算法也有较好的抵御能力.Tan 等人在文献[10]中指出文献[9]的再调整机制会引起含密图像的绝对差分图像直方图(Histogram of the Absolute Difference of the Pixel Pairs,HADPP)的局部脉冲失真,提出利用 B-样条拟合得到与原始图像近似的 HADPP,通过比较拟合前后直方图的局部变化,可检测是否存在隐写.图 6 显示,在两种嵌入率下,不论是在 UCID 图像库还是 NRCS 图像库,本文算法的 ROC 曲线与 EALSBMR 算法的 ROC 曲线相比都大幅偏向右下,说明它比 EALSBMR 算法具有强得多的抗此类攻击的能力.我们注意到,在 NRCS 库中,无论嵌入率为 0.5 bpp 还是 0.8 bpp,EALSBMR 算法对文献[10]的隐写分析攻击都非常敏感.

6　结论

本文提出了一种基于像素块的纹理优先自适应隐写算法,与经典的 LSB 隐写算法(即 LSBM 和 LSBMR)以及现有的基于边缘优先的自适应嵌入算法(即 EALSBMR)相比,提高了嵌入效率,更好保护了图像的平坦区

域,间接地提高了安全性.针对四种有代表性的隐写分析算法,本文算法与 LSBM,LSBMR,EALSBMR 以及 EPES 这 4 种算法相比,具有更佳的抗隐写分析能力.本文在理论上的贡献是针对自适应嵌入过程中可能出现的异常块问题,提出了一种像素值调整方案,并严格证明了这种方案能确保密信的正确、完整的抽取.我们还具体给出了减少像素值改动的优化方案.目前本文只对 3×3 的嵌入块进行了讨论,将来会对更大的块和更多的相邻像素(例如位于"+"和"×"形的近邻)进行研究,期望进一步提高算法的嵌入率和安全性.

参考文献

[1] 王朔中,张新鹏,张卫明.以数字图像为载体的隐写分析进展[J],计算机学报,2009,32(7):1247-1263.
WANG Shuo-Zhong,ZHANG Xin-Peng,ZHANG Wei-Ming. Recent advances in image-based steganalysis research[J]. Chinese Journal of Computers,2009,32(7):1247-1263.(in Chinese)

[2] Westfeld A, Pfitzmann A. Attacks on steganographic systems [A]. Proceedings of Third International Workshop, Information Hiding[C]. Berlin: Springer-Verlag, 2000. 61-76.

[3] Filler T, Fridrich J. Fisher information determines capacity of ε-secure steganography[A]. Proceedings of 11th International Workshop, Information Hiding[C]. Germany: Darmstadt, 2009. 31-47.

[4] Goljan M, Fridrich J, Holotyak T. New blind steganalysis and its implications[A]. Proceedings of SPIE 6072, Security, Steganography, and Watermarking of Multimedia Contents VIII [C]. San Jose, CA: SPIE, 2006. 1-13.

[5] Harmsen J J, Pearlman W A. Steganalysis of additive-noise modelable information hiding[A]. Proceedings of SPIE 5020, Security and Watermarking of Multimedia Contents V[C]. Santa Clara, CA: SPIE, 2003. 131-142.

[6] Cancelli G, Doërr G, Cox I J, et al. Detection of ±1 LSB steganography based on the amplitude of histogram local extrema [A]. Proceedings of 15th IEEE International Conference. Image Processing[C]. San Diego, CA: IEEE, 2008. 1288-1291.

[7] Pevny T, Bas P, Fridrich J. Steganalysis by subtractive pixel adjacency matrix[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(2): 215-224.

[8] Mielikainen J. LSB matching revisited[J]. IEEE Signal Processing Letters, 2006, 13(5): 285-287.

[9] Luo W, Huang F, Huang J. Edge adaptive image steganography based on LSB matching revisited[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(2): 201-214.

[10] Tan S, Li B. Targeted steganalysis of edge adaptive image steganography based on LSB matching revisited using B-Spline fitting[J]. IEEE Signal Processing Letters, 2012, 19(6): 336-339.

[11] Omoomi M, Samavi S, Dumitrescu S. An efficient high payload ±1 data embedding scheme[J]. Multimedia Tools and Applications, 2011, 54(2): 201-218.

[12] Holub V, Fridrich J. Random projections of residuals for digital image steganalysis[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(12): 1996-2006.

[13] Schaefer G, Stich M. UCID: an uncompressed color image database[A]. Proceedings of the Storage and Retrieval Methods and Applications for Multimedia[C]. San Jose, CA: SPIE, 2004. 472-480.

[14] United States Department of Agriculture. Natural Resources Conservation Service Photo Gallery. [OL]. Available: http://photogallery.nrcs.usda.gov. 2013-05-09.

作者简介

师夏阳 男,1978 年 4 月出生,河南省平顶山市人,现为华南理工大学信号与信息处理专业博士研究生,主要从事数字图像信息隐藏、隐写分析和小波分析方面的研究.
E-mail: aryang123@163.com

马赛兰 女,1989 年 8 月出生,湖北省仙桃市人,现为华南理工大学信号与信息处理专业硕士研究生,主要从事数字图像信息隐藏和隐写分析方面的研究.
E-mail: canlan818@163.com

胡永健(通信作者) 男,1962 年 12 月出生,湖北武汉人.教授、博士生导师、中国电子学会和中国计算机学会高级会员、IEEE 高级会员.1990 年和 2002 年分别在西安交通大学和华南理工大学获工学硕士和工学博士学位.主要研究方向是多媒体信息安全、信息隐藏和数字图像处理.
E-mail: eeyjhu@scut.edu.cn

周琳娜 女,1972 年 4 月出生于湖南省邵阳市,2007 年于北京邮电大学获工学博士学位,清华大学博士后,现为北京电子技术应用研究所研究员.主要研究方向为图像分析与处理、信息隐藏、多媒体信息安全.
E-mail: zhoulinna@tsinghua.edu.cn