·图形图像处理· 文章编号：1000-3428(2018)10-0215-06 文献标志码：A 中图分类号：TP391

基于矩阵编码的大容量密文域可逆信息隐藏算法

刘 宇，杨百龙，赵文强，袁志华

（火箭军工程大学 信息与通信工程系，西安 710025）

摘 要：针对当前密文域可逆信息隐藏技术中容量不足的缺陷，提出一种完全可分离的大容量可逆信息隐藏算法。将猫脸变换后的密文图像按照像素值划分区间，对特定区间内的像素定位，按矩阵编码的方式嵌入信息。接收方利用位置信息并根据隐写密钥解码提取秘密信息，经简单计算复原密文图像，解密后即可恢复原始图像。实验结果表明，该算法能够准确地提取秘密信息，无损恢复载体图像，实现 2 种操作的完全分离。

关键词：矩阵编码；密文域；可分离性；可逆信息隐藏；隐藏容量

中文引用格式：刘 宇，杨百龙，赵文强，等. 基于矩阵编码的大容量密文域可逆信息隐藏算法[J]. 计算机工程，2018，44(10)：215-220.

英文引用格式：LIU Yu，YANG Bailong，ZHAO Wenqiang，et al. Large capacity reversible information hiding algorithm in encryption domain based on matrix coding[J]. Computer Engineering，2018，44(10)：215-220.

Large Capacity Reversible Information Hiding Algorithm in Encryption Domain Based on Matrix Coding

LIU Yu，YANG Bailong，ZHAO Wenqiang，YUAN Zhihua

（Department of Information and Communication Engineering，Rocket Force University of Engineering，Xi'an 710025，China）

【Abstract】 Aiming at the shortcomings of insufficient capacity in the current encrypted domain reversible information hiding technique，a completely separable large capacity reversible information hiding algorithm is proposed. Arnold transform is used to encrypt original image，and pixel values of the encrypted image are divided into different intervals according to Most Significant Bit(MSB)，so each pixel belongs to a specific interval. Secret messages are embedded into the encrypted image by matrix-encoding. At the receive end，the secret messages are extracted accurately with the help of the location map and the steganalysis key. The encrypted image can be restored by simple calculation，and then the original image can be obtained by decrypting the encrypted image without error. The correctness of the scheme is demonstrated by derivation. Experimental results show that the method can extract the secret information accurately and restore the carrier image without loss，and realize the complete separation of these two operations.

【Key words】 matrix coding；encryption domain；separability；reversible information hiding；hiding capacity

DOI：10.19678/j.issn.1000-3428.0048388

0 概述

可逆信息隐藏技术能够在明文载体中嵌入隐秘信息但不会对图像造成永久失真，在军事、医疗领域应用广泛。为保障图像在传输过程中的内容隐私，用于嵌入信息的载体图像一般会预先加密。因此，信息隐藏者需要能够针对密文域特性处理信息的专用可逆信息隐藏算法。作为典型的加密域信号处理方法，密文域可逆信息隐藏可应用于许多领域，如用户信息标识、隐私保护、密文数据管理等。目前已经提出了一些实用的算法。

文献[1]使用异或操作加密图像，数据隐藏者翻转数据块内像素的 3 个最低有效位(Least Significant Bit，LSB)来嵌入秘密信息。但该方法利用像素空间相关性恢复载体图像，会产生误差。文献[2]利用平滑度函数和边界匹配技术改进此方案，提升了隐藏容量和提取信息的准确率。文献[3]也提出了一种改进方案，通过考虑多个邻近像素来降低提取信息的平均错误率。但是以上方案均不能完全准确地提取秘密信息和恢复载体图像，不是完全可逆的算法。同时，秘密信息的提取必须要在图像解密之后完成。

为解决以上问题，文献[4]提出一种可分离的密

作者简介：刘 宇(1993—)，男，硕士研究生，主研方向为图像处理、信息隐藏；杨百龙，教授、博士生导师；赵文强，博士研究生；袁志华，硕士研究生。

收稿日期：2017-08-17 **修回日期：**2017-10-11 **E-mail：**lauyu_18@163.com

文域可逆信息隐藏算法。文献[5]在图像加密后对密文图像进行嵌入,接收端秘密信息的提取和图像解密完全独立,合法的接收者可根据不同权限执行相应操作。文献[6]基于像素预测提出了一种新的可分离方案,在信息隐藏阶段,使用伪随机密钥选择多个像素,在两个最高比特位中隐藏秘密信息,有效提升了算法的性能。然而随着嵌入率的增加,误码率会增大。文献[7]给出一种直方图修正的可分离密文域可逆信息隐藏算法,然而在嵌入的同时引入了椒盐噪声,影响了图像质量。文献[8]结合 LWE 公钥密码算法设计了一种新的可分离方案,适用于各类载体。文献[9]提出了新的可分离的信息隐藏框架,在密文图像中使用直方图平移的方法嵌入秘密信息,获得了较高的嵌入率和可逆性,但在隐藏容量上仍不理想。此外,文献[10]描述了基像素排序定位的方法。文献[11]利用双峰值多零点嵌入信息,有效提升了隐藏容量。文献[12]采用双层直方图嵌入,减小了信息隐藏造成的图像失真。

为提高密文域可逆信息隐藏算法的隐藏容量,本文根据矩阵编码思想,将密文图像像素组按照要求分为不同的区间,在特定区间内使用矩阵编码嵌入信息,保留可嵌入像素的位置图以便接收端能够可逆地解码和恢复载体图像。

1 矩阵编码

为提升算法隐藏容量,许多信息隐藏算法引入隐写编码嵌入信息。文献[13]融合方向编码与湿纸编码,在不同类型的载体上均具备较高的隐藏容量。文献[14]结合视觉模型与菱形编码,有效提升了信息隐藏算法的隐藏容量,且具备抗隐写分析的能力。

矩阵编码也是一种高效的隐写编码方式,由文献[15]首先提出,后被应用于 JEPG 图像隐写的著名的 F5[16]算法中,在同等嵌入率的情况下大幅减小载体图像的修改率,极大地提升了算法的嵌入效率。矩阵编码的表示形式为一个有序元组$[d_{\max},n,k]$,其含义是将载体信息按照码字长度 n 分组,最多修改其中的 $d_{\max}$ 个比特即可嵌入 k bit 的数据,从而提升嵌入效率。定义每次修改对像素的改变量为 $C(k)$,嵌入率为 $R(k)$,计算方式如式(1)、式(2)所示。

$$C(k)=\frac{d_{\max}}{n+1}=\frac{d_{\max}}{2^k} \tag{1}$$

$$R(k)=\frac{k}{n}=\frac{k}{2^k-1} \tag{2}$$

因此,矩阵编码的嵌入效率表示为:

$$P(k)=\frac{R(k)}{C(k)}=\frac{2^k\times k}{2^k-1} \tag{3}$$

当 $d_{\max}=1$ 时,矩阵编码的改变量、嵌入量和嵌入效率之间的对应关系如表 1 所示。

表 1 矩阵编码改变量、嵌入率、嵌入效率之间的关系

k	n	改变量	嵌入量	嵌入效率
1	1	50.00	100.00	2.00
2	3	25.00	66.67	2.67
3	7	12.50	42.86	3.43
4	15	6.25	26.67	4.27
5	31	3.12	16.13	5.16
6	63	1.56	9.52	6.09
7	127	0.78	5.51	7.06
8	255	0.39	3.14	8.03
9	511	0.20	1.76	9.02

在 F5 算法中 $d_{\max}=1$,以 $n=3,k=2$ 为例演示矩阵编码的原理。

设读取的 3 bit 载体信息为 a_1、a_2、a_3,需要嵌入的 2 bit 秘密数据为 x_1、x_2,判断秘密数据与载体信息之间的数学关系,对载体信息中的某一个比特进行修改。判断标准和修改方式如下:

1)$x_1=a_1\oplus a_3$,$x_2=a_2\oplus a_3$,不做修改;

2)$x_1\neq a_1\oplus a_3$,$x_2=a_2\oplus a_3$,翻转 a_1;

3)$x_1=a_1\oplus a_3$,$x_2\neq a_2\oplus a_3$,翻转 a_2;

4)$x_1\neq a_1\oplus a_3$,$x_2\neq a_2\oplus a_3$,翻转 a_3。

在此 4 类情况中,对 3 bit 的载体信息进行矩阵编码后嵌入了 2 bit 秘密数据,但对于载体信息的修改最大只有 1 位。

在一般情况下,若 $a=a_1a_2\cdots a_n$ 表示 n 个可以修改的码字,$x=(x_1,x_2,\cdots,x_k)$ 表示需要嵌入的 k bit 秘密信息,则 a'表示将秘密信息 x 嵌入到 a 之后的码字。

1)按照式(4)定义散列函数 f,可以从码字 a'中提取嵌入的信息 x,使得 $x=f(a')$,有:

$$f(a)=\bigoplus_{i=1}^{n}a_i\cdot i \tag{4}$$

2)通过散列函数和秘密信息异或找到需要修改的数据位置,如式(5)所示。

$$s=f(a)\oplus x \tag{5}$$

3)按照上一步找到的位置,修改特定的码元,规则如式(6)所示。

$$a'=\begin{cases}(a_1,a_2,\cdots,a_i,\cdots,a_n),\ s=i\\ a,s=0\end{cases} \tag{6}$$

4)重复以上步骤直至嵌入所有秘密信息。

2 算法流程

本文算法执行过程如图 1 所示。

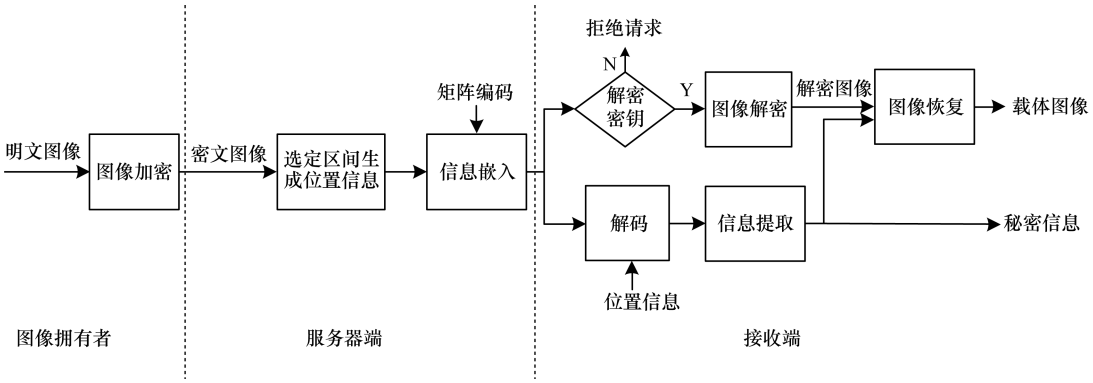

图 1　本文算法流程

如图 1 所示,明文图像经加密后选定特殊区间生成位置信息,利用矩阵编码嵌入信息,接收端根据权限解码提取所嵌入的信息或解密复原图像内容,图像质量的完全恢复需要两部分协同完成。

本文算法以增大算法的隐藏容量为核心,兼顾算法的可逆性与可分离性。引入矩阵编码嵌入信息旨在提高隐藏容量,但是矩阵编码对于载体的修改不可逆,因此,利用位置图记录矩阵编码位置,以确保信息隐藏算法的可逆性。同时为确保矩阵编码正确解码,编码后的码字顺序不能在解码前发生变化,因此,不能在图像解密之后再提取信息,需要算法接收端具有灵活的操作选择。本文采取位置置乱加密,矩阵编码嵌入与提取过程均对像素值进行操作,不会影响解密正确性,从而确保了算法的可分离性。

2.1　图像加密

为保护在信息传输过程中图像内容的隐私性,图像拥有者在上传图像前需要对明文图像进行加密。本文采取 Arnold 变换加密图像。Arnold 变换可以把图像中各像素点的位置进行置换,使其达到加密的目的。当输入图像为正方形时,Arnold 映射的表达式如式(7)所示。

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod(N) \tag{7}$$

其中,a、b、N 为正整数,(x,y) 表示输入图像矩阵中各个像素的坐标,N 表示矩阵的宽度,mod 是求余函数。

对于灰度图像而言,位置坐标移动实际上是对应点的灰度值的移动,即将原来点(x,y)处像素对应的灰度值移动至变换后的点(x',y')处。对一个数字图像迭代地使用离散化的 Arnold 变换,即将上一次变换输出的(x',y')作为下一次 Arnold 变换的输入,循环执行迭代直到图像内容无法辨识,图像加密完成。以 Lena 灰度图像为测试,分别执行 1 次、5 次、10 次、20 次 Arnold 变换,加密效果如图 2所示。经 20 次变换后,图像内容已经完全被掩盖,达到了保护隐私内容的需求。

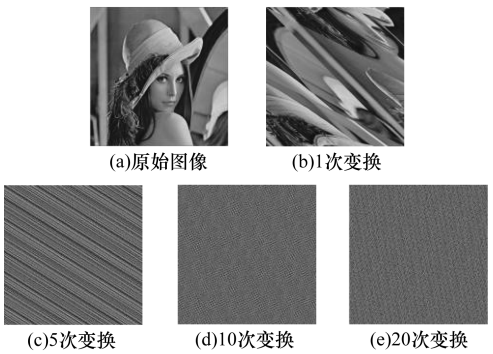

图 2　猫脸变换加密效果

2.2　位置信息的生成

灰度图像像素区间为[0,255],每个像素值可以用 8 位二进制数表示。将像素按照 3 个最高有效位(Most Significant Bit,MSB)的差异把[0,255]的像素范围均分为 8 个区间,$s_0=[0,31]$,$s_1=[32,63]$,$s_2=[64,95]$,$s_3=[96,127]$,$s_4=[128,159]$,$s_5=[160,191]$,$s_6=[192,223]$,$s_7=[224,255]$,对应的区间内像素的 3 位 MSB 分别为 000、001、010、011、100、101、110、111。每个区间内所有像素的 3 位 MSB 恰好等于所在区间编号的二进制表示。为确保接收端能够准确提取和恢复载体图像,选定一个像素区间作为嵌入区间,保留嵌入区域所有像素的位置信息和所在的区间编号。如图 3 所示,经 20 次猫脸变换的密文域 Lena 图像中,白色区域为可嵌入区域,此位置图为二值图像,需要压缩后嵌入密文图像。

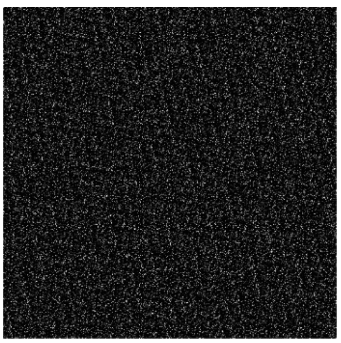

图 3　密文图像中可嵌入位置示意图

2.3 秘密信息嵌入及提取

服务器端接收到密文图像后,将秘密信息转化为二进制比特流,进入嵌入序列。为尽量减少对于载体密文图像的修改,在使用矩阵编码嵌入信息时选择与 F5 算法相同的有序元组$[l,n,k]=[1,3,2]$,表示最多只需修改 1 位数据,在密文图像的每个可嵌入像素的 3 位 MSB 上嵌入 2 bit 秘密信息。迭代执行编码过程,直到嵌入所有的秘密信息。嵌密完成后,将含有秘密数据的密文图像和位置图一起发送至接收端。此时,为保证信息隐藏过程的安全性,减少传输次数,由于位置图为二值图像,占用空间很小,可压缩后嵌入密文图像。

接收方得到含有秘密信息的加密图像时,需要首先提取位置图,根据位置图找到所嵌入像素的位置,使用散列函数对指定位置的像素逐一进行解码操作即可提取秘密信息。

2.4 图像恢复及解密

恢复载体图像时,由于在嵌入操作时选定的像素均属于同一区间,所有像素的 3 位 MSB 相同,且该 3 位 MSB 所对应的十进制数就是所在的区间编号,因此可以根据如下方法计算得出被修改像素的原始 3 位 MSB。

在 3 位二进制数中,由于每次嵌入操作只修改最多 1 位数据,则每个 3 位二进制数对应 4 种不同的修改结果。恢复操作同样只需修改 1 位数据。具体对应关系如表 2 所示。

表 2 数据修改及恢复关系对应结果

原始(修改后)数据	修改(恢复)结果
000	000,001,010,100
001	001,000,011,101
010	010,000,011,110
011	011,010,001,111
100	100,000,101,110
101	101,100,001,111
110	110,111,100,010
111	111,110,011,101

接收方根据位置图找到被修改的像素后,需要恢复指定位置的所有像素的 3 位 MSB,根据嵌入规则可知,这些像素的 3 位 MSB 相同。由表 2 可知,接收方对每个像素的 3 位 MSB 执行恢复操作时,可能出现的恢复结果中必有一个是原始的 MSB,其余均为错误的恢复结果,同一错误不会在每次恢复过程中都出现。因此,只需对特定位置的少量像素的 3 位MSB 执行预判断,统计所有可能恢复的 3 位二进制数据,找到重复最多的恢复结果就是被修改的原始 MSB。替换特定像素的 3 位 MSB 即可无损地恢复密文图像,将密文图像执行 Arnold 逆变换,得到与原始图像完全相同的解密图像。

2.5 算法执行示例

下面以一个实例来说明算法的执行过程。

若密文图像中选定区间为$s_4=[128,159]$,读取 4 个可嵌入像素值$p_1=155$,$p_2=133$,$p_3=149$,$p_4=137$,假设待嵌入的秘密信息比特为$x=(10110001)$。p_1 对应二进制数为 10011011,取出 3 位 MSB 作为矩阵编码的码字$a_1a_2a_3=100$,按顺序嵌入的秘密信息为$x_1=1$,$x_2=0$。因此,该码字对应的所有修改结果只有 4 种情况:100,101,110,000,按照式(4)计算:$f(a)=\bigoplus_{i=1}^{n}a_i\cdot i=1\times1\oplus0\times2\oplus0\times3=01$,根据式(5)计算需要修改的码字位置,$s=f(a)\oplus x=01\oplus10=11$,翻转 a_3 完成嵌入得到码字$a_1'a_2'a_3'=101$,修改后的二进制序列为 10111011 = 187 = p'_1。同理计算出其余像素嵌入秘密信息后的结果分别为 11000101 = 197 = p'_2,00010101 = 21 = p'_3,10001001 = 137 = p'_4。

接收方提取秘密信息时,根据位置图找到 p'_1、p'_2、p'_3、p'_4。按照散列函数直接计算出 p'_1 中所嵌入的秘密信息为$x_1x_2=1\times1\oplus0\times2\oplus1\times3=10$,$p'_2$、$p'_3$、$p'_4$ 中所嵌入的秘密信息分别为$x_3x_4=1\times1\oplus1\times2\oplus0\times3=11$,$x_5x_6=0\times1\oplus0\times2\oplus0\times3=00$,$x_7x_8=1\times1\oplus0\times2\oplus0\times3=01$,组合可得秘密信息为$x=x_1x_2x_3x_4x_5x_6x_7x_8=10110001$;恢复载体图像时,接收方不能直接找到被修改的像素中具体哪一位数据被翻转,但是可以通过表 2 进行预计算,得到如表 3 所示的结果。

表 3 接收端高位数据恢复结果预计

高位数据	预恢复结果
101	101,100,001,111
110	110,111,100,010
000	000,001,010,100
100	100,000,101,110

从表 3 可以看出,在所有恢复结果中,只有 100 这一种结果在每个高位 MSB 数据可能恢复的结果中均出现,重复次数最多。因此,原始像素的 3 位 MSB 为 100,用其替换被修改像素的 3 位 MSB 即可恢复原始像素。

3 实验与结果分析

本文基于 Matlab2014a 实验仿真平台,以图 4 所示标准灰度测试图像为例,从可逆性、隐藏容量两方面分析算法性能。

图 4　标准灰度测试图像

3.1　可逆性分析

在算法嵌入过程中,矩阵编码的编码过程对于可嵌入像素的 MSB 的修改最大为 1,对于像素值的改变最大为 128。在对图像质量要求不是很苛刻的情况下接收端可以直接解密图像。接收端直接进行 Arnold 逆变换获得的解密图像如图 5(a)所示。

从图 5(a)中可以看出,直接解密后图像大部分内容已经可以获得,但是由于选定区间的像素值发生了最大为 128 的变化,而图像的空间相关性又使得该部分像素集中于原始图像的某个区域,因此图像中许多细节部分呈现出杂乱无章的噪声。为了改善直接解密图像的图像质量,采用 3×3 的模板对图像进行中值滤波,得到图 5(b)。可以看出,图像质量大大改善,许多杂乱的细节被恢复,但是仍存在一些噪声块。另外,秘密信息的嵌入率也会影响图像直接解密的质量,嵌入率越高,直接解密图像质量越差。

本文算法采用散列函数计算秘密信息,可以 100% 正确地恢复秘密信息。而在恢复载体图像时,若要完全无损地恢复载体图像,只需按照位置图找到选定的嵌入像素的具体位置,按照前文的计算方法得出被修改的 MSB,替换指定位置上所有像素的 MSB 即可恢复到嵌密操作前的密文图像,执行 Arnold 逆变换即可获得无损的原始图像,如图 5(c)所示。以 Lena 图像为例,计算不同嵌入率时恢复图像、直接解密图像、中值滤波图像与原始图像对比的峰值信噪比,如表 4 所示。

图 5　图像恢复效果对比

表 4　不同嵌入率下图像的恢复质量

嵌入率	直接解密/dB	中值滤波/dB	恢复图像
0.14	23.58	28.63	∞
0.28	21.19	25.21	∞
0.42	19.90	23.47	∞
0.56	19.26	22.67	∞

从表 4 中的数据得知,在嵌入率不断增加时,直接解密图像的质量迅速降低,即使经过中值滤波也无法很好地改善图像质量,但按照 2.4 节中的方法恢复图像,可以获得与原始图像质量相同的恢复图像。对比文献[6,9]中恢复图像的质量如表 5 所示。

表 5　不同算法的图像峰值信噪比　　dB

图像	文献[6]算法	文献[9]算法	本文算法
Lena	31.10	55.19	∞
Jet	33.10	51.95	∞
Baboon	30.49	54.58	∞
Goldhill	34.27	53.56	∞
Peppers	31.98	54.15	∞

从表 5 可以看出,在恢复图像时,本文算法是真正可逆的恢复载体图像,文献[6]采取预测误差的方式,恢复效果不佳。文献[9]虽然获得了较高的峰值信噪比,但不是真正可逆的恢复图像。

3.2　隐藏容量分析

在本文算法中,每个可嵌入像素均可嵌入 2 bit 秘密信息,因此,隐藏容量与选定嵌入区间像素数量正相关。按照第 2 节中的区间划分方式,统计测试图像中各个区间像素的数量,如图 6 所示。

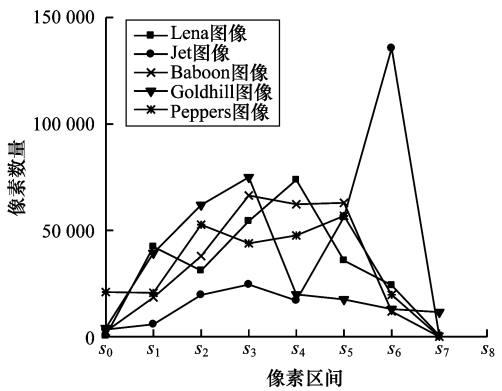

图 6　像素值区间分布情况

图像的像素数值区间分布与图像的内容特性相关,而像素数值也决定了算法的隐藏容量。从图中可以看出,除 JET 图像外,大部分图像像素最集中的区间在 s_3、s_4、s_5 区间,同时该折线图也反映了选定不同的区间为嵌入区域时,各测试图像的隐藏容量的变化趋势。为了最大限度地提升算法隐藏容量选取图像中像素数量最多的区间作为嵌入区域,不同测试图像下算法隐藏容量与嵌入率的关系如表 6 所示。

表 6 隐藏容量与嵌入率对应关系

图像	隐藏容量/bit	嵌入率/bpp
Lena 图像	147 442	0.56
Jet 图像	271 232	1.03
Baboon 图像	132 742	0.51
Goldhill 图像	149 936	0.57
Peppers 图像	113 574	0.43

将本文算法与文献[1,9]算法进行对比,3 种算法的嵌入率统计如表 7 所示。

表 7 不同算法嵌入率对比

算法	最大嵌入率	平均嵌入率
本文算法	1.030	0.62
文献[1]算法	0.015	0.01
文献[9]算法	0.510	0.13

如表 7 所示,引入矩阵编码后,本文算法平均嵌入率为 0.62,最高嵌入率甚至超过了 1,平均嵌入效率高出文献[1]算法 1 个数量级,高出文献[9]算法 5 倍。文献[1]算法对图像分块,而每块中只能嵌入 1 bit 秘密信息,同时该算法恢复秘密信息时需要借助图像的空间相关性,分块数不能太小,这极大限制了算法的隐藏容量。文献[9]利用直方图平移的方法,嵌入率受直方图峰值点的约束,较本文算法稍有逊色。

综上,本文虽然只在图像局部进行嵌入,但图像依然具有较高的隐藏容量。在矩阵编码对载体进行修改后,接收方可以提取信息,但若要恢复载体图像,必须得知载体中哪一位被翻转,这是制约矩阵编码在可逆信息隐藏中应用的关键。因此,本文根据最高3 位MSB 的区别划分像素区间,在同一区间内对3 位MSB 执行矩阵编码后,不需要了解具体哪一位比特被翻转,直接恢复为该区间对应的 3 位 MSB。由此可实现载体的完全可逆恢复。

而发送方采取的位置置乱加密方法与服务器端矩阵编码的操作互不影响,确保了接收端实现解密与信息提取的可分离,实现了不同权限的灵活操作。

4 结束语

本文提出一种新的密文域可逆信息隐藏算法,通过在密文图像的部分 MSB 上执行矩阵编码,使得算法嵌入容量大幅提升。而使用位置图则可以准确找到被修改的像素进行完全可逆的载体图像恢复,同时准确无误地恢复秘密信息。针对接收端的载体图像解密与信息提取没有次序的问题,可依据不同的权限可分离地进行操作。实验结果证明,本文算法具有完全可逆性、和可分离性,同时具有较高的隐藏容量。

参考文献

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

[2] 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.

[3] LIAO Xin, SHU Changwen. 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.

[4] MA Kede, ZHANG Weiming, ZHAO Xianfeng, 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.

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

[6] WU Xiaotian, SUN Wei. High-capacity reversible data hiding in encrypted images by prediction error[J]. Signal Processing, 2014, 104(6):387-400.

[7] QIAN Zhenxing, HAN Xiyu, ZHANG Xinpeng. Separable reversible data hiding in encrypted images by n-nary histogram modification[C]//Proceedings of the 3rd International Conference on Multimedia Technology. Washington D. C., USA:IEEE Press, 2013:869-876.

[8] 柯 彦,张敏情,张英男. 可分离的密文域可逆信息隐藏[J]. 计算机应用研究,2016,33(11):3476-3479.

[9] YIN Zhaoxia, ABEL A, ZHANG Xinpeng, et al. Reversible data hiding in encrypted image based on block histogram shifting[C]//Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing. Washington D. C., USA:IEEE Press, 2016:2129-2133.

[10] 项洪印,苑津莎,侯思祖. 基于平滑分块基像素定位的可逆信息隐藏方法[J]. 计算机工程,2016,42(9): 116-120.

[11] 刘 俊,杨任尔,万旭东. 基于不同扫描顺序差值的可逆信息隐藏算法[J]. 计算机工程,2015,41(3): 269-272.

[12] 熊祥光,韦 立. 基于直方图平移和互补嵌入的可逆水印方案[J]. 计算机工程,2015,41(8):180-185.

[13] 张新鹏,刘 焕,张颖春,等. 融合方向编码和湿纸编码的高效信息隐藏[J]. 上海大学学报(自然科学版), 2010,16(1):1-4.

[14] 陈涨胜,杨任尔,陈贞佐,等. 基于视觉模型与菱形编码的图像隐写算法[J]. 宁波大学学报(理工版), 2017,30(4):68-73.

[15] CRANDALL R. Some notes on steganography[EB/OL]. [2017-08-17]. http://os.inf.tu-dresden.de/~westfeld/crandall.pdf.

[16] WESTFELD A. F5——A steganographic algorithm[C]// Proceedings of International Workshop on Information Hiding. Washington D. C., USA: IEEE Press, 2001: 289-302.

编辑 顾逸斐