图像插值空间完全可逆可分离密文域信息隐藏算法

王继军[1],李国祥[2],夏国恩[2],孙泽锐[2]
(1. 广西财经学院信息与统计学院,广西南宁 530003; 2. 广西财经学院教务处,广西南宁 530003)

摘 要: 密文域可逆信息隐藏技术在医学、云服务、军事、商业等众多领域有着广泛应用,针对现有密文域信息隐藏算法的可逆性不能完全保证、嵌入率低、不能完全分离等不足,提出一种完全可逆可分离密文域信息隐藏算法,首先,给出了适合图像加密遍历矩阵所需满足的条件和构造方法,载体图像拥有者设置密钥 1 构造遍历矩阵,并对明文图像进行加密,然后将加密图像传送给信息嵌入者,信息嵌入者设置密钥 2,以期望插值为目标,根据插值区间大小确定嵌入位数,再由差值修正因子和秘密信息共同确定最终插值,使最终插值最大限度接近期望插值,确保载密图像高质量,整个过程无附加信息、无数据溢出、且均可保证可逆性,密钥 1 拥有者和密钥 2 拥有者两种权限互不干涉,是完全可逆可分离算法,平均嵌入率可达到 3 bit/pixel,通过与 8 种优秀算法的实验比较,表明算法在嵌入容量、可逆性、可分离性率等方面相比于对比算法均有一定优势.

关键词: 信息安全; 可逆信息隐藏; 密文域; 图像插值; 遍历矩阵
中图分类号: TP391 **文献标识码:** A **文章编号:** 0372-2112 (2020)01-0092-09
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.01.011

A Separable and Reversible Data Hiding Algorithm in Encrypted Domain Based on Image Interpolation Space

WANG Ji-jun[1], LI Guo-xiang[2], XIA Guo-en[2], SUN Ze-rui[2]
(1. *Department of Information and Statistics, Guangxi University of Finance and Economics, Nanning, Guangxi* 530003, *China*;
2. *Office of Academic Affairs, Guangxi University of Finance and Economics, Nanning, Guangxi* 530003, *China*)

Abstract: Reversible steganography in encrypted domain is widely used in medical, cloud services, military, commercial and other fields. Aiming at the problems of encrypted domain information hiding algorithm, such as incomplete guarantee of reversibility, low embedding rate and incomplete separation, this paper proposed a separable and reversible steganography in encrypted domain. Firstly, the conditions and construction methods for the ergodic matrix of image encryption are given. The carrier image owner sets the key1 to construct the ergodic matrix and encrypts the plaintext image, the information embedder sets the key2, in order to achieve the goal of expectation interpolation, the number of embedding bits is determined according to the size of interpolation interval, and then the final interpolation is determined by the difference correction factor and secret information together, so that the final interpolation is close to the expectation interpolation to the maximum extent, ensuring the high quality of the encrypted image. There is no additional information, no data overflow and reversibility is guaranteed in the whole process, the two permissions do not interfere with each other, and the algorithm is completely reversible and separable, and the average embedding rate can reach 3 bit/pixel. The experimental results show that the algorithm is better than the other eight excellent algorithms in terms of embedding capacity, reversibility and separability.

Key words: information security; reversible data hiding; encrypted domain; image interpolation; ergodic matrix

收稿日期:2018-10-18;修回日期:2019-03-22;责任编辑:李勇锋
基金项目:国家自然科学基金(No. 71862003);广西多源信息挖掘与安全重点实验室(No. MIMS18-05);广西高校中青年教师能力提升项目(No. 2018KY0518);广西应用经济学一流学科(培育)开放性课题(No. 2018YB01);广西(东盟)财经研究中心开放性课题(No. 2018DMCJYB10);广西高校中青年教师能力提升项目(No. 2018KY0520);广西财经学院科研项目(No. 2016B033);广西财经学院青年发展基金(No. 2018QNB18)

1 引言

信息隐藏技术作为信息安全的重要组成部分,近几年得到了长足发展,但一些新需求的不断出现,使得传统信息隐藏不再能完全满足现实的需要,如在医学领域,为保护病人隐私,医学图像通常需要加密,而管理图片的第三方人员并不关注明文图像具体内容,而是需要在不解密图像的前提下,直接在加密后的图像中嵌入病人相关隐私信息,还要保证秘密信息能正确提取,原始图像能够精准恢复,否则可能造成诊断错误或重大事故;像这样的需求在军事、政治、法律、商业等众多领域均有着广泛需求,在密文上进行数据操作和处理的需求与时俱增,这就需要我们设计出性能更优的信息隐藏算法,而完全可逆可分离的密文域信息隐藏能满足很好满足上述需求,因此倍受关注.

在密文域信息隐藏方面,学者们已经提出了一些相对成熟的方案,大体可以分为两种类型:"联合型"与"可分离型".

所谓"联合型"是指:信息提取与载体恢复两个操作不可分离,不能交换,如果想提取嵌入信息,必须先解密图像再进行提取. 对于"联合型"方案:Zhang[1] 将加密图像进行分块,通过翻转每一块中特定像素的 3 个不重要位来嵌入 1 比特信息,是较早的一种方案,但信息不能准确提取;Hong[2] 等人通过加入边缘匹配技术和改进波动函数对 Zhang 的算法进行了改良,提高了信息提取的正确率;Liao[3] 等人对不同位置的像素点采取不同的波动函数,进一步提高了恢复的正确率;文献[4]将载体图像像素分为两类,并用位置图标记,对一类直接加密,另一类进行误差估计和直方图平移嵌入秘密信息再加密,算法是可逆的,但嵌入率较低;文献[5]利用传统的可逆信息隐藏方法将一部分像素的不重要位嵌入到其他像素中,然后对图像进行加密,再利用这些不重要位留出的空间嵌入信息,思路简洁,但严格来说,文献[4,5]均是加密前就预留了空间,并不是真正加密域信息隐藏方法;文献[6]使用熵编码技术,设计了一种不依赖加密方式的通用密文域加密算法,嵌入率为 0.169bpp,可逆性能够完全保证,但依然未能实现解密、提取的可分离;文献[7]基于自适应策略,通过对原始图像进行预测误差直方图构造,实现可逆隐藏,该方法的嵌入容量依赖于预测误差直方图的分布,嵌入率较低,上述方法均是不可分离型,嵌入容量也较小.

所谓"可分离型"是指:信息提取与载体恢复互相独立、可交换进行. 对于"可分离型"方案:Zhang 提出一种可分离方案[8],嵌入者通过压缩密文图像最低有效位得到冗余空间,并在该空间内嵌入秘密信息,但因为秘密信息提取和载体图像的还原均是建立在像素相关性这一统计特征上,导致该方法并非是完全可逆的;Wu 等[9] 引入预测误差实现隐藏,并且还提供了高嵌入率下恢复图像的改进方案,能准确提取秘密信息,但载体图像不能完整恢复,也不是完全可逆的;肖迪等人[10] 在加密前计算了预测误差,并使用所计算的结果构造位置图作为辅助信息,再经同态加密算法并根据位置图实现嵌入,辅助信息也不需要单独传输;Karim 等人[11] 利用加密后的图像依然存在可利用的熵空间,通过熵编码去除加密图像中的冗余空间,由此构造出可嵌入空间,该方法是完全在密文域中处理,且可逆性也有保障,但嵌入容量非常有局;文献[12]提出了一种基于 R-LWE(Ring-Learning With Errors)的密文域隐藏方案,先使用 R-LWE 算法对载体明文进行加密,再通过对单位比特明文信息在密文域空间映射区域的量化以及再编码,实现信息隐藏,能保证解密与提取过程的可分离,嵌入率最高为 0.2353bpp;文献[13]提出一种基于位平面分割的可逆信息隐藏算法,首先对高位平面信息进行定长游程编码压缩,再将压缩结果进行流加密,然后再对中位平面进行加密,低位平面翻转,实现数据嵌入,该方法在嵌入率小于 0.5bpp 时,载密图像质量好,解密与提取可分离;文献[14]利用 LWE 公钥密码算法对数据进行加密,用户直接在密文中嵌入秘密信息,接收方可有效提取隐藏信息,也可无损还原出载体,实现了提取与解密的分离,最大可嵌入率为 1bpp;文献[15]是基于公钥密码体制在加密域中应用了同态乘法来扩展图像的直方图,并用直方图移位嵌入秘密信息,且秘密信息可直接提取,载体图像也可完全恢复,平均嵌入率均可达 1bpp,性能较好.

通过分析上述方案可知,现有的密文图像可逆信息隐藏尚存在几个问题,主要表现在:(1)算法可逆性不能完全保证,并非完全可逆;(2)算法嵌入率较低,不能很好满足现实需要;(3)部分算法并不是真正的密文域信息隐藏,究其实质还是明文域可逆信息隐藏算法;(4)能完全实现可逆可分离算法较少. 本文设计一种完全可逆可分离的密文域信息隐藏算法,提出了适合图像加密遍历矩阵所需满足的条件,并给出了遍历矩阵的构造方法,首先生成加密图像,再计算生成高质量插值图像对应的期望插值,以期望插值为最终目标,引导秘密信息嵌入,由插值区间大小确定出嵌入位数,再根据待嵌入秘密信息大小,调整差值修正因子,使得最终插值最大限度接近期望值,保证载密图像高质量,可独立无损还原载体,或独立准确提取秘密信息,是完全可逆可分离算法,全过程无附加信息、无数据溢出,算法平均嵌入率达到 3bit/pixel.

2 图像加密域可逆信息隐藏算法

本文算法核心思想是:图像拥有者设置密钥 1 对原

始图像进行加密,达到隐藏原始内始的目的,然后将加密图像传送给数据嵌入者;数据嵌入者设置密钥2,并对加密图像进行插值和秘密信息嵌入,达到隐藏秘密信息的目的. 接收者如果拥有密钥1,可以无损还原出原始图像,接收者如果拥有密钥2,则可提取出秘密信息,接收者同时拥有密钥1和2,则既可无损还原出原始图像,又可提取出秘密信息,算法的总架构如图1所示.

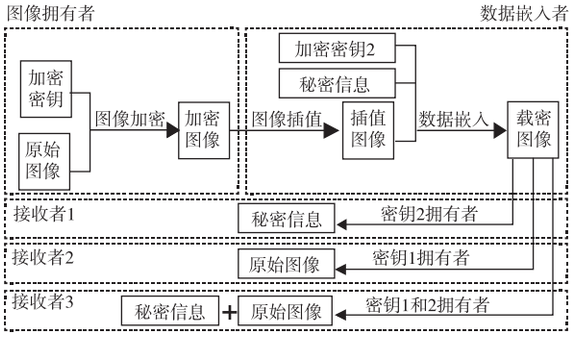


图1 本文算法框架结构图

3 本文图像加密算法

3.1 混沌伪随机数生成器

混沌系统[16]是一种复杂的非线性动力系统,而其中Logistic映射应用较为广泛,其定义为:

$$x_{k+1}=\mu x_k(1-x_k) \tag{1}$$

式中,$0\leqslant\mu\leqslant4$ 称为分支参数,当 $x_k\in(0,1)$ 且 $3.569945\leqslant\mu\leqslant4$ 时,Logistic映射处于混沌状态,为了保证序列具有更好的随机性,将去除序列前段从某一给定值开始取值,如可令:$X_i=x_{(i+300)}$.

3.2 矩阵遍历加密原理

从矩阵某一个元素开始,沿某一特定的顺序依次访问各个元素,直到最后一个元素,这种特定的访问顺序就形成一种矩阵遍历,我们以此为基础,对其进行扩展和限定,构造出适合图像加密的遍历矩阵,而适合图像加密的遍历矩阵必须同时满足两个条件:(1)遍历矩阵中各元素,必须为正整数,且在一个连续的区间内;(2)遍历矩阵中的元素无序且不重复. 为了方便描述,我们先给出如下定义.

定义1 给定一个原始矩阵 $\boldsymbol{M}$,矩阵 $\boldsymbol{E}$ 与矩阵 $\boldsymbol{M}$ 同大小,且 $\boldsymbol{E}$ 中各元素为一个连续区间$[1,m\times n]$内的正整数值,无序且不重复,那么顺次访问 $\boldsymbol{E}$ 中的元素 $\boldsymbol{E}(i,j)$,同时对应将 $\boldsymbol{M}$ 中编号为 $\boldsymbol{E}(i,j)$ 位置的值,依次读取到一个新的矩阵 $\boldsymbol{E}$ 中,我们就将矩阵 $\boldsymbol{E}$ 称为遍历矩阵,经一次遍历得到的矩阵记为:$\boldsymbol{R}_{(1)}$,称为一次遍历加密矩阵,利用同一个遍历矩阵 $\boldsymbol{E}$ 可对矩阵 $\boldsymbol{M}$ 进行 t 次遍历加密,结果记为 $\boldsymbol{R}_{(t)}$.

遍历加密原理如图2所示(以3×3为例说明).

$$\begin{pmatrix}35&66&8\\21&44&95\\16&55&76\end{pmatrix}\quad\begin{pmatrix}4&7&2\\3&8&9\\5&1&6\end{pmatrix}\quad\begin{pmatrix}21&16&66\\8&55&76\\44&35&95\end{pmatrix}$$

(a)原始矩阵$\boldsymbol{M}$ (b)遍历矩阵$\boldsymbol{E}$ (c)一次遍历加密$\boldsymbol{R}_{(1)}$

$$\begin{pmatrix}8&44&16\\66&35&95\\55&21&76\end{pmatrix}\quad\begin{pmatrix}55&8&21\\35&16&95\\66&44&76\end{pmatrix}$$

(d)二次遍历加密$\boldsymbol{R}_{(2)}$ (e)六次遍历加密$\boldsymbol{R}_{(6)}$

图2 遍历加密原理示意图

上述原理可用式(2)表示:

$$\boldsymbol{R}_{(t)}(i,j)=\boldsymbol{R}_{(t-1)}\left(\left\lceil\frac{\boldsymbol{E}(i,j)}{n}\right\rceil,\boldsymbol{E}(i,j)-\left(\left\lceil\frac{\boldsymbol{E}(i,j)}{n}\right\rceil-1\right)\times n\right) \tag{2}$$

其中,$\boldsymbol{R}_{(0)}=\boldsymbol{M}$,$\boldsymbol{M}$ 是原始矩阵,$\boldsymbol{E}$ 是遍历矩阵,$\boldsymbol{R}_{(t)}$ 是原始矩阵 $\boldsymbol{M}$ 按矩阵 $\boldsymbol{E}$ 遍历 t 次后的结果.

3.3 遍历矩阵构造方法

假定待加密图像为 $\boldsymbol{A}$,大小为 $m\times n$,首先给出混沌系统的初值(μ,x_0),可记:$key=(\mu,x_0)=(3.95,0.32578)$,用式(1)生成一个长为 $m\times n$ 的随机数列 P,如 P 中有相同元素,则去除相同元素后继续生成,直到生成一个长为 $m\times n$,且各元素互不相同的序列,记为:P_i,$1\leqslant i\leqslant m\times n$,得到的 P_i 是0到1之间的随机数,如:

$P_1=\{0.30,0.62,0.90,0.26,0.75,0.86,0.37,0.50,0.48\}$

由上述过程可知,当 $i\neq j$ 时 $P_i\neq P_j$,也就是说序列 P 中不存在相等的元素,令:$Q_k=Rank(P_i)$,$[Q,k]=Rank(P_i)$,$Rank()$ 为排序函数,用 k 返回索引序列,则 k 表示的是 P 中某一元素在 Q 中的位置,记:同一元素在序列 P 和 Q 中的位置 i 和 j 为一个二元组(i,k),$\because 1\leqslant i\leqslant m\times n$,$\therefore k\in[1,m\times n]$,将 $m\times n$ 个 k 值写为 $m\times n$ 大小的二维矩阵,记矩阵为 $\boldsymbol{E}=reshape(k,m,n)$,则 $\boldsymbol{E}$ 中各元素均为连续区间$[1,m\times n]$中的正整数,无序且不重复,完全满足适合图像加密遍历矩阵的两个条件. 如:

$$\begin{matrix}(i)&(1)&(2)&(3)&(4)&(5)&(6)&(7)&(8)&(9)\\P_1\mapsto\{&0.30,&0.62,&0.90,&0.26,&0.75,&0.86,&0.37,&0.50,&0.48\}\end{matrix}$$

$$\begin{matrix}(k)&(1)&(2)&(3)&(4)&(5)&(6)&(7)&(8)&(9)\\Q_k\mapsto\{&0.50,&0.90,&0.26,&0.30,&0.37,&0.48,&0.62,&0.75,&0.86\}\end{matrix}$$

$$(i,k)\mapsto(1,4)\ (2,7)\ (3,2)\ (4,3)\ (5,8)\ (6,9)\ (7,5)\ (9,6)$$

构造出的遍历矩阵 $\boldsymbol{E}\mapsto\begin{pmatrix}4&7&2\\3&8&9\\5&1&6\end{pmatrix}$

3.4 遍历矩阵解密原理

解密是加密的逆过程,解密时首先利用3.3中的方法生成遍历矩阵 $\boldsymbol{E}$,然后对待解密图像进行若干次遍历,便可还原出原始矩阵,如:遍历矩阵是:

$$\boldsymbol{E}\mapsto\begin{pmatrix}4&7&2\\3&8&9\\5&1&6\end{pmatrix},\boldsymbol{R}_{(2)}\mapsto\begin{pmatrix}8&44&16\\66&35&95\\55&21&76\end{pmatrix}$$

为二次加密后待解密矩阵,那么经过 5 次遍历后原始矩阵被还原,其原理如图 3 所示.

$$\begin{pmatrix}8&44&16\\66&35&95\\55&21&76\end{pmatrix}\overset{1次}{\mapsto}\begin{pmatrix}66&55&44\\16&21&76\\35&8&95\end{pmatrix}\overset{2次}{\mapsto}\begin{pmatrix}16&35&55\\44&8&95\\21&66&76\end{pmatrix}$$
$$\overset{3次}{\mapsto}\begin{pmatrix}44&21&35\\55&66&76\\8&16&95\end{pmatrix}\overset{4次}{\mapsto}\begin{pmatrix}55&8&21\\35&16&95\\66&44&76\end{pmatrix}\overset{5次}{\mapsto}\begin{pmatrix}35&66&8\\21&44&95\\16&55&76\end{pmatrix}$$

图3　遍历解密原理示意图

解密过程可用式(3)表示:

$$\boldsymbol{R}_{t'}=\boldsymbol{R}_{t'-1}\left(\left\lceil\frac{\boldsymbol{E}(i,j)}{n}\right\rceil,\boldsymbol{E}(i,j)-\left(\left\lceil\frac{\boldsymbol{E}(i,j)}{n}\right\rceil-1\right)\times n\right)\tag{3}$$

其中,$\boldsymbol{R}_{(0)}=\boldsymbol{R}$,$\boldsymbol{R}$ 为加密后矩阵.

3.5　像素扩散及还原

为了达到更好的加密效果,可对遍历得到的矩阵 $\boldsymbol{R}$ 再进行像素扩散,一方面,像素扩散可以使得离散化的混沌映射不可逆,另一面,可以更好地防御明文图像的统计特性攻击. 首先将混沌序列变换为无符号整数作为 XOR 操作数,然后与 $\boldsymbol{R}$ 进行异或运算,可用式(4)表示:

$$Y(i)=round(x(i)\times10^{k})\bmod 256\tag{4}$$

其中,$k\in\boldsymbol{Z}$ 且 $k\geqslant3$,则像素扩散后的矩阵:

$$\hat{\boldsymbol{R}}=\boldsymbol{R}\oplus Y,\oplus\text{表示异或运算}\tag{5}$$

像素扩散的还原计算方法为:

$$\boldsymbol{R}=\hat{\boldsymbol{R}}\oplus Y\tag{6}$$

4　图像加密域可逆信息隐藏算法

根据 1 中提出的算法核心思想,本文算法主要通过图像插值、可嵌入位数计算、秘密信息嵌入、差值修正、含秘插值确定、嵌入位数控制等步骤来完成,下面逐一介绍.

4.1　图像插值

文献[16]提出一种类线性插值方法,本文以此为基础,通过分析不同插值对图像质量的影响,得出生成高质量插值图对应的期望插值,以期望插值为目标,引导后续秘密信息嵌入,在保证载密图像质量的前提下,最大限度嵌入秘密信息,文献[16]是对载体图像直接插值,不便于后期算法性能准确分析比较,我们先对图像进行下采样,然后再进行后续操作,具体采样方法如下.

设原始输入图像为 $\boldsymbol{I}$,大小为 $m\times n$,$\boldsymbol{I}(i,j)$ 为各像素点灰度值,$1\leqslant i\leqslant m$,$1\leqslant j\leqslant n$,为了便于隐藏性能分析,先对输入图像 $\boldsymbol{I}$ 进行下采样,得到图像 $\boldsymbol{A}$,其大小为 $(m/2)\times(n/2)$,(实际应用中无需下采样操作,仅为便于实验对比),下采样操作为:

$$\boldsymbol{A}(i,j)=\boldsymbol{I}(2i-1,2j-1),\ 1\leqslant i\leqslant m/2,1\leqslant j\leqslant n\tag{7}$$

对图像 $\boldsymbol{A}$ 进行插值,得到图像 $\boldsymbol{B}$,其大小为 $m\times n$,图像 $\boldsymbol{B}$ 中"●"表示的像素点均是图像 $\boldsymbol{A}$ 的像素 ,而"∘"表示的像素点由其上下或左右相邻的两个像素点确定,"⊕"表示的像素点由其 45°角和 135°角上的四个像素点确定,插值示意图如下,插值的计算请参看文献[16].

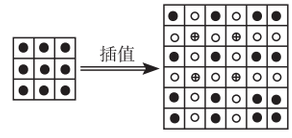


图4　图像放大4倍插值示意图

将"∘"处表示的像素点记为 $\boldsymbol{B}(\circ)$,"⊕"处表示的像素点记为 $\boldsymbol{B}(\oplus)$,在保持 $\boldsymbol{B}(\oplus)$ 不变的情形下,$\boldsymbol{B}(\circ)$ 分别取以下 7 种情形,对比不同取值下图像 PSNR 的变化情况,结果如表 1 所示.

表 1　$\boldsymbol{B}(\oplus)$ 位取值不变,$\boldsymbol{B}(\circ)$ 位取不同数值对图像 PSNR 值的影响

Image	$\boldsymbol{B}(\circ)-3$	$\boldsymbol{B}(\circ)-2$	$\boldsymbol{B}(\circ)-1$	$\boldsymbol{B}(\circ)$	$\boldsymbol{B}(\circ)+1$	$\boldsymbol{B}(\circ)+2$	$\boldsymbol{B}(\circ)+3$
Lena	33.018	33.326	33.504	33.536	33.420	33.166	32.797
Peppers	29.508	29.626	29.686	29.686	29.619	29.496	29.319
Boat	30.194	30.355	30.449	30.469	30.415	30.290	30.099
Baboon	22.967	22.999	23.018	23.024	23.017	22.996	22.962
Sailboat	28.448	28.545	28.595	28.597	28.551	28.458	28.322
Barbara	24.911	24.958	24.984	24.989	24.974	24.937	24.880

从上面实验数据可看出,插值图像"∘"处像素点的取值越接近$\boldsymbol{B}(\circ)$,图像 PSNR 值越大,插值图像质量越好;"⊕"处也得到同样结论,也就是说插值越接近$\boldsymbol{B}(\circ)$和$\boldsymbol{B}(\oplus)$,载秘图像质量就越好,本文算法以此为基础.

4.2　秘密信息的嵌入

将图像 $\boldsymbol{A}$ 中一个大小为 2×2 的图像块各像标记为 A_1,A_2,A_3,A_4,经抛物线插值并嵌入秘密信息后得到载秘图像,各像素点标记如图 5 所示.

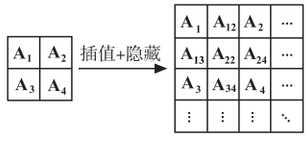


图5　图像插值和信息隐藏前后像素标识示意图

每两个相邻像素可以组成一个像素对,图 4 中可组出:A_1,A_2、A_1,A_3、A_3,A_4、A_4,A_2、A_4 四对,下面以用像素点 A_1,A_2 确定出插值 A_{12} 为例说明.

(1)可嵌入位数确定

对于像素点 A_1,A_2,由 3.1 中的实验分析可知,其期

望插值 $A'_{12}=\lfloor\frac{A_1+A_2}{2}+0.5\rfloor$,那么$[0,A'_{12}]$就是秘密信息的可嵌入区间,设在此区间内可嵌入的最大位数为 k,则有:

$$k=\begin{cases}\log_2 A'_{12}, & \text{if } A'_{12}\neq 0\\ 0, & \text{if } A'_{12}=0\end{cases}\quad k\in\mathbf{Z},0\leqslant k\leqslant 7 \tag{8}$$

如:$A_1=58$,$A_2=78$,$A'_{12}=\lfloor(58+78)/2\rfloor=68$,则 $k=\lfloor\log_2 68\rfloor=6$,最大嵌入位数为6.

(2)秘密信息嵌入

设待嵌入的秘密信息为 W,其对应的二进制为 $w_i(i=1,2,\cdots)$,我们将连续 k 位秘密信息 $w_i\sim w_{i+k-1}$转换为十进制,记为 S_k,则有:

$$S_k=\sum_{i=1}^{k}(w_i\times 2^{(k-i)}),\ 0\leqslant S_k\leqslant 255 \tag{9}$$

若将 S_k 直接当作 A_1,A_2 的最终插值 A_{12},那么 S_k 越接近 A_{12}插值效果就越好,但因 w_i 的取值不同,S_k 的波动可能较大,我们将 S_k 与 A_{12}的差值记为 Δd,即:$\Delta d=A'_{12}-S_k$,$\because S_k<A'_{12}$,$\therefore\Delta d>0$,Δd 表示最终插值与期望插值的差,Δd 越小,插值效果越好. 如:$A_1=58$,$A_2=78$,$k=6$,若 $w_i=111001$,$S_6=53$,$\Delta d_1=A'_{12}-S_6=68-53=15$,此时 Δd 的值较大,若直接嵌入秘密信息,可能会影响载密图像质量,为此我们需引入一个差值修正因子.

(3)差值修正因子

为了减小 Δd,我们引入一个差值调整因子 T,首先将 k 位连续秘密信息的最大值记为 $S_{\max}$,则有 $S_{\max}=\max\{S_k\}=2^k-1$,则差值调整因子 $T=A'_{12}-S_{\max}$,而 $A'_{12}=\lfloor(A_1+A_2)/2+0.5\rfloor$是已知的,对于给定的 k 位秘密信息,$S_{\max}$也是已知的,也就是说:对于给定的两个像素点和确定的秘密信息,差值调整因子 T 是一个常数. 如:$A_1=58$,$A_2=78$,$w_i=111001$,则:$A'_{12}=68$,$S_{\max}=2^6-1=63$,$T=5$.

(4)确定最终插值

对于像素点 A_1,A_2,以及连续 k 位秘密信息,最终的含密插值 A_{12}可表示为

$$A_{12}=\begin{cases}T+S_k=A'_{12}-S_{\max}+S_k, & \text{if } A'_{12}\neq 0\\ 0, & \text{if } A'_{12}=0\end{cases} \tag{10}$$

同样 $A_1=58$,$A_2=78$,$k=6$,$w_i=111001$,此时 $A'_{12}=68$,$S_{\max}=2^6-1=63$,$S_6=9$,$T=68-9=59$,$A_{12}=T+S_k=59+9=68$,此时 $\Delta d=A'_{12}-A_{12}=0$,效果达到最好,但如果不引入差值修正因子,则:$A_{12}=S_k=9$,此时的 $\Delta d=A'_{12}-A_{12}=68-9=59$,$\Delta d$ 较大,插值效果较差,也就是说引入插值修正因子,载密图像质量会得到进一步提高.

(5)溢出分析

$\because A_{12}=A'_{12}-S_{\max}+S_k=A'_{12}-(2^k-1)=A'_{12}+1-2^{\lfloor\log_2 A'_{12}\rfloor}$且当 $A'_{12}=255$,$w_i=1111111$ 时,A_{12}达到最大,$\max\{A_{12}\}=A'_{12}-S_{\max}+S_7=255-(2^7-1)+127=255$,而当 $A'_{12}=1$ 时,$k=0$,$\because A_{12}=A'_{12}=1$,且当 $A'_{12}=0$ 时,A_{12}的值达到最小,所以 $\min\{A_{12}\}=0$,综上分析可知,$\because 0\leqslant A_{12}\leqslant 255$,即:整个过程无数据溢出.

(6)嵌入位数控制

在上述4.2(1)中,我们确定了最大可嵌入位数 k,其中 $0\leqslant k\leqslant 7$,k 越大,可嵌入信息就越多,但随着 k 值的增大,载密图像的质量会下降,因此在实际应用中,可根据具体应用需求,合理控制 k 的最大取值,保证较高载密图像质量,具体 k 值与载密图像质量的对应关系在实验6.4中给出.

5 完全可逆可分离的密文域信息隐藏算法

5.1 图像加密与秘密信息嵌入过程

(1)设置密钥1,自动生成初值 μ 和种子 x_0,经及遍历次数 t;

(2)用3.3中的方法生成遍历矩阵 $\boldsymbol{E}$,用 $\boldsymbol{E}$ 对原始图像 $\boldsymbol{A}$ 进行 t 次遍历得到 $\boldsymbol{A}_{(t)}$,再利用式(3)~(6)进行像素扩散,得到加密图像 $\boldsymbol{R}$,将此加密图像发送给数据载入者;

(3)数据载入者先用4.1中的方法对加密图像进行插值,并用式(8)~(10)完成秘密信息的嵌入,生成加密域载密图像 $\boldsymbol{B}$.

至此,图像加密与秘密信息均已完成,整个过程,无任何附加信息,也无数据溢出.

5.2 图像还原与秘密信息提取

5.2.1 对于持有密钥1者(内容拥有者)

(1)密钥1拥有者,只需关注载密图像中"●"处的像素点,而"●"处的像素点只参与了加密运算,在秘密信息嵌入过程中未有任何改变,因此只需将"●"位置像素点,按从上到下、从左到右的顺序重新组成一幅大小为$(m/2)\times(n/2)$的图像,即得到了加密后图像;

(2)利用密钥1,生成初值 μ 和种子 x_0,便可得到遍历矩阵 $\boldsymbol{E}$,通过式(3)即可还原出原始图像,该过程是可逆的,因此还原出的图像也是无损的.

5.2.2 对于持有密钥2者(数据嵌入者)

(1)密钥2拥有者,在载密图像中以3×3大小像素块为一组,分别以插值点两侧的像素点为依据,得出期望插值 A'_{12},利用式(8)~(11)计算出最大嵌入位数 k 和差值调整因子 T,便可用式(11)计算出 S_k

$$S_k=B'_{12}-B_{12}-(2^k-1) \tag{11}$$

(2)令:$w_i=\lfloor S_k/2\rfloor\bmod 2$,$i=0,1,\cdots,k$,将 S_k 转为二进制位;

(3)依次计算所有像素对中的 S_k,并全部转换为二

进制,再按顺序连接,便可得到秘密信息.

5.2.3 对于持有密钥 1 和 2 者(接收者)

同时持有密钥 1 和 2 者,可以完成上述5.2.2和5.2.3的所有步骤,即可准确提取出秘密信息,又可无损还原出原始图像.

综上看,不同权限拥有者,可以根据自己的权限准确地获取到对应权限的信息,载体图像恢复与秘密信息提取互相独立,可交换,因此该算法是完全可逆可分离的密文域信息隐藏算法.

6 实验结果

为检验本文算法性能,我们采用 MATLAB 2016b 软件进行了仿真实验,实验图像是 USC-SIP 图库中标准图像[17],载体图像大小均为 512×512,在不同参数下对大量载体图像进行了仿真实验,受篇幅所限,在此仅列出部分主要实验结果.

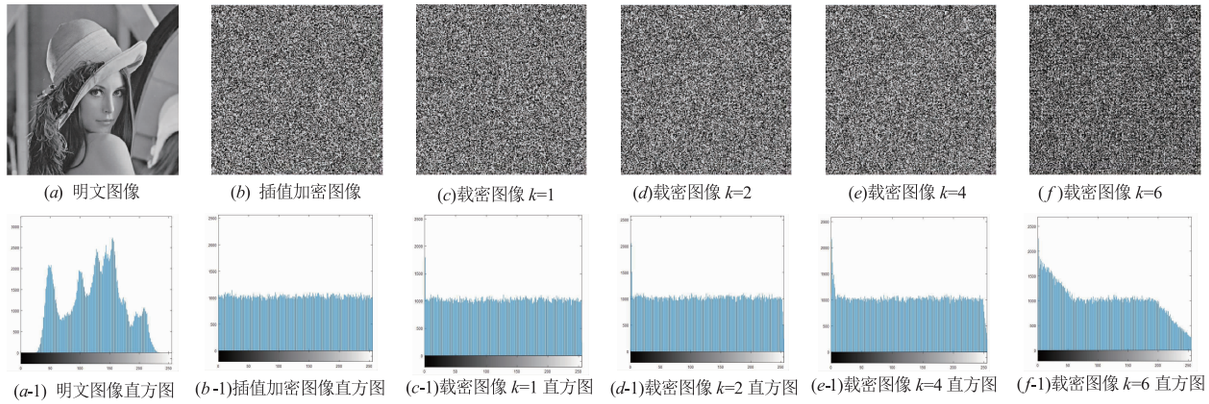
6.1 实验图像

(*a*)Lena　(*b*)Peppers　(*c*)Baboon　(*d*)Zelda

图6　实验图像

6.2 载秘图像及直方图

从图 7 可直观看出,明文图像的灰度直方图(图(*a*-1))有明显的峰值与零值,而密文图像直方图(图(*b*-1))分布基本上均匀,意味着我们的加密方法可以抵抗统计攻击,达到了较好加密效果,对于载密图像而言,当嵌入位数 k 较小时,载密图像直方图(图(*c*-1)、(图(*c*-2))与密文图像直方图(图(*b*-1))非常相似,说明秘密信息的嵌入对密文图像影响较小,嵌入效果较理想,随着 k 的增大,载密图像直方图发生变化,但即使在 $k=6$ 时与明文图像直方图分布差异依然较大,效果较好.



(*a*) 明文图像　(*b*) 插值加密图像　(*c*)载密图像 *k*=1　(*d*)载密图像 *k*=2　(*e*)载密图像 *k*=4　(*f*)载密图像 *k*=6

(*a*-1) 明文图像直方图　(*b*-1)插值加密图像直方图　(*c*-1)载密图像 *k*=1 直方图　(*d*-1)载密图像 *k*=2 直方图　(*e*-1)载密图像 *k*=4 直方图　(*f*-1)载密图像 *k*=6 直方图

图7　载秘图像及其直方图

6.3 信息熵

信息熵用来描述信源的不确定性,一个系统越是有序信息熵就越低,越是混乱信息熵就越高,如果图像中各灰度值出现的概率符合均匀分布,即每个灰度值出现的的概率均为 1/256,此时的理论熵为 8,信息不容易泄露,但在实际应用中,各灰度值不可能完全均匀分布,但性能好的图像加密方法应尽可能让图像信息接近 8,信息熵计算公式如下:

$$H(S)=\sum_{s}P(s_i)\log_2 P(s_i)^{-1} \tag{12}$$

其中,$P(s_i)$ 表示灰度值 s_i 出现的概率,因不同载体图像测试出的实验结果极为相似,在此仅给出 lena 图的结果,如表 2 所示. 从实验结果可看出,本文密文图像的信息熵达到 7.9992,非常接近理想值 8,有较好抗熵攻击性,伴随嵌入位数不断增大,信息熵逐步减小,但均保持在较高值,效果较理想.

表 2　不同嵌入率下密文图像及载秘图像的信息熵

测试图像	明文图像	加密图像	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$
Lena	7.4492	7.9992	7.9956	7.9931	7.9881	7.9795	7.9573	7.9211

6.4 嵌入容量

目前查阅文献中较大的嵌入率是 1bpp,从上面的实验可看出,本文算法有较大嵌入容量,当 $k=1$ 时,嵌入率就超过文献[1 ~ 13],当 $k=2$ 时,嵌入率达到 1.482bpp,也超过 1bpp,伴随着 k 的增大,嵌入率不断增加,最大嵌入率可达到 4.5bpp,当然在寻求大嵌入率时也要兼顾考虑图像的质量,一般认为图像的 PSNR 应保持在 30dB 以上,结合表 3 和图 7 可看出,当 $k=4$ 时,图像的 PSNR 均在 30dB 以上,此时的嵌入率仍达到 3bpp,另外,载密图像本身是一种置乱后的密文图像,PSNR 值并没有像明文图像那么重要,实际应用中可根

据具体需求,确定最大可嵌入值 k.

表 3 最大嵌入位数 k 限定在不同值对应的嵌入率

Test Images	每个插值中嵌入的最大位数 k						
	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$
Lena	0.744	1.482	2.209	2.911	3.566	4.128	4.504
Peppers	0.744	1.482	2.208	2.909	3.563	4.122	4.491
Baboon	0.744	1.482	2.207	2.910	3.565	4.126	4.500
Zelda	0.744	1.482	2.208	2.910	3.563	4.122	4.487
平均	0.744	1.482	2.208	2.910	3.564	4.125	4.496

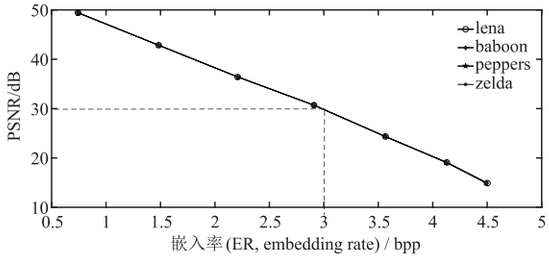


图8 不同图像在不同嵌入率下与PSNR的关系

6.5 和其他方案的比较

6.5.1 不同方案可逆可离性比较

载体图像的解密与秘密信息的提取两个操作若可分离、可交换,则算法的安全性会更高,实用性会更好,但目前完全可逆可分离的算法还比较少,文献[1~7]均是不可分离型,文献[8~10]虽然是可分离的,但载体图像不能完整还原,文献[11~15]可分离也可逆,但嵌入率较低,表4给出具体对比强果.

表 4 不同文献可逆可分离性比较

比较文献	是否可分离	是否完全可逆	最大嵌入率(bit/pixel)
文献[8]	可分离	非完全可逆	0.0625
文献[9]	可分离	非完全可逆	0.0625
文献[10]	可分离	条件下可逆	0.0660
文献[11]	可分离	完全可逆	0.1690
文献[12]	可分离	完全可逆	0.2350
文献[13]	可分离	完全可逆	0.5000
文献[14]	可分离	完全可逆	1.0000
文献[15]	可分离	完全可逆	1.0000
本文算法($k\leqslant4$)	可分离	完全可逆	3.0000
本文算法($k>4$)	可分离	完全可逆	4.5000

从表4可看出,在本文列出的15篇有代表性的文献中,有5篇是可逆可分离的,但嵌入率相对较低,在同等满足完全可逆可分离的前提下,本文算法在嵌入容量方面有优势.

6.5.2 不同方案嵌入率与载密图像质量比较

PSNR是衡量图像质量的重要指标[19],而嵌入率也是信息隐藏的主要性能衡量指标,下面给出完全可逆可分离的不同文献、在不同嵌入率下载秘图像PSNR值的变化情况,用以衡量载秘图像质量.

图9展示了本文算法与文献[12~15]对相同测试图像,在不同嵌入率下的PSNR对比,同事也能看出嵌入率的对比,从中可看出,本文算法在嵌入率及载密图像质量两个方面均有优势.

6.6 算法运行效率

算法复杂度是衡量算法性能的重要指标之一,直接影响算法的实用性,文献[12,14]是基于LWE(Learning With Errors)的算法,是一类等价于格上的一般性困难问题,算法复杂度为多项式模运算,运算效率低,关于LWE算法与其他基于大整数分解和离散对数公钥加密算法的比较可参考文献[20,21],而另一类基于同态加密的密文域信息隐藏算法,成果较多,但运算量大一直是待解决的一个难题[22],本文算法的主要运算是图像遍历加密和插值,是线性运算,算法复杂度与文献[10,13,18]相当,明显优于其他比较文献.

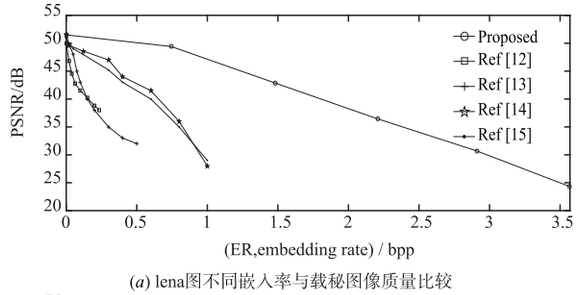
6.7 安全性分析

(1)密文图像和载秘图像直方图分布均匀、平坦,破译者不能从直方图中获得原图像和密钥信息,也不能察觉到密文图像里又嵌入了水印信息,达到了载体图像安全性和水印隐蔽性的要求;

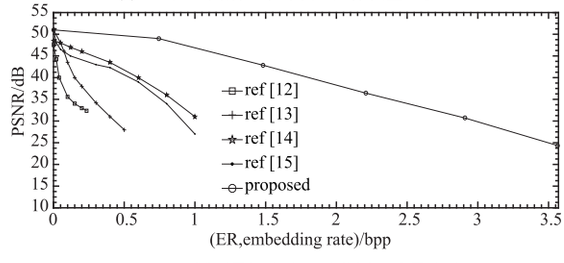
(2)水印提取和图像解密相互独立,即:水印的提取不依赖于图像解密,图像解密可直接进行,不以提取水印为前提,是完全可分离、可交换的;

(3)权限分离,不同密码持有者有不同权限,仅有嵌入密钥者只能得到秘密信息,仅有加密密钥者,只能还原出载体图像,只有同时持有嵌入密钥和加密密钥者,才能获取全部信息,保证了安全性;

(4)Logistic映射混沌系统本身是安全的,在多篇文中有过论述,在此不再赘述,那么建立在Logistic映



(*a*) lena图不同嵌入率与载秘图像质量比较



(*b*) baboon图不同嵌入率与载秘图像质量比较

图9 不同算法嵌入率与载密图像质量比较

射基础的遍历加密,也是安全的.

7 结束语

完全可逆可分离的密文域信息隐藏算法是信息安全的一个研究热点,在众多行业有着关广泛应用需求,有较好的应用价值和应用前景,本文算法的主要优势有:(1)是完全可逆可分离的信息隐藏算法;(2)在嵌入率和图像质量上均优于其他文献;(3)适用于任何载体图像,通用性较强;(4)安全性高;(5)算法简结,运行效率高,对文中不足之处,我们将做进一步深入研究,持续加以改进和完善.

参考文献

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

[2] HONG W,CHEN TS,WU HY. An improved reversible data hiding in encrypted images using side match[J]. IEEE Signal Processing Letters,2012,19(4):199 – 202.

[3] LIAO X,SHU C. 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(2):21 – 27.

[4] ZHANG W,MA K,Yu N. Reversibility improved data hiding in encrypted images[J]. Signal Processing,2014,94:118 – 127.

[5] MA K,ZHANG W,ZHAO X,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.

[6] ZHANG Xinpeng,QIAN Zei,Feng Guorui,et al. Efficient reversibledata hiding in encrypted image[J]. Journal of Visual Communicationand Image Representation,2014,25(2):322 – 328.

[7] RAD R M,WONG K S,GUO J M. Reversible data hiding by adaptive group modification on histogram of prediction errors[J]. Signal Processing,2016,125:315 – 328.

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

[9] WU X,SUN W. High-capacity reversible data hiding in encrypted images by prediction error[J]. Signal Process,2014,104:387 – 400.

[10] 肖迪,杜社,郑洪英. 基于差值域直方图平移的密文可逆水印算法[J]. 计算机应用研究,2014,31(12):3668 – 3672.
XIAO Di,DU She,ZHENG Hong-ying. Reversible watermarking algorithm for encrypted image based on histogram difference shifting[J]. Application Research of Computers,2014,31(12):3668 – 3672. (in Chinese)

[11] KARIM MSA,Wong K. Universal data embedding in encrypted domain[J]. Signal Processing,2014,94(5):174 – 182.

[12] 柯彦,张敏情,苏婷婷. 基于 R-LWE 密文域多比特可逆信息隐藏算法[J]. 计算机研究与发展,2016,53(10):2307 – 2322.
KE Yan,ZHANG Minqing,Su Tingting. A novel multiple bits reversible data hiding in encrypted domain based on RLWE[J]. Journal of Computer Research and Development,2016,53(10):2307 – 2322. (in Chinese)

[13] 李天雪,张敏情,狄富强. 基于位平面分割的密文域可逆信息隐藏算法[J]. 计算机应用研究,2018,35(9):1 – 7.
LI Tianxue,ZHANG Minqing,Di Fuqiang. Cryptographic domain reversible data hiding algorithm based on bit plane segmentation[J]. Application Research of Computers,2018,35(9):1 – 7. (in Chinese)

[14] 张敏情,柯彦,苏婷婷. 基于 LWE 的密文域可逆信息隐藏[J]. 电子与信息学报,2016,38(2):354 – 360.
ZHANG Minqing,KE Yan,SU Tingting. Reversible steganography inencrypted domain based on LWE[J]. Journal of Electronics & Information Technology,2016,38(2):354 – 360. (in Chinese)

[15] LI M,LI Y. Histogram shifting in encrypted images with public key cryptosystem for reversible data hiding[J]. Signal Processing,2017,130(7):190 – 196.

[16] 王继军. 图像插值空间大容量可逆数字数据算法[J]. 中国图象图形学报,2014,19(4):527 – 533.
WANG Ji-jun. High capacity reversible watermarking for image interpolation space[J]. Journal of Image and Graphics,2014,19(4):527 – 533. (in Chinese)

[17] USC-SIPI Image Database[OL]. http://sipi.usc.edu/database/,2018.

[18] C Yu,X ZHANG,Z TANG. Separable and error-free reversible data hiding in encrypted image based on two-layer pixel errors[J]. IEEE Access,2018,6(12):76956 – 76969.

[19] Z WANG,AC Bovik,HR Sheikh,EP Simoncelli. Image quality assessment:From error visibility to structural similarity[J]. IEEE Transactions on Image Processing,2004,13(4):600 – 612.

[20] AJTAI M. Generating hard instances of lattice problems[A]. Proceedings of 28th ACM Symposium on Theory of Computing[C]. USA:ACM,1996. 99 – 108.

[21] 吴立强. 基于格的密码体制研究[D]. 西安:武警工程大学,2012.
WU Liqiang. Research of Lattice—based public key cryptography[D]. Xi'an:Armed Police Engineering Univer-

sity,2012. (in Chinese)
[22] 李子臣,张卷美,杨亚涛. 基于 NTRU 的全同态加密方案[J]. 电子学报,2018,46(4):938 -944.
LI Zi-chen,ZHANG Juan-mei,YANG Ya-tao. A fully homomorphic encryption scheme based on NTRU[J]. Acta Electronica Sinica,2018,46(4):938 -944. (in Chinese)

作者简介

王继军 男,1981 年出生,山西吕梁人. 副教授,2008 年毕业于广西师范大学计算机应用技术专业,获硕士学位,研究方向:信息隐藏、数字水印.
E-Mail:wangjijun1209@126.com

李国祥 男,1984 年出生,山东济宁人. 副教授,2010 年毕业于广西师范大学计算机应用技术专业,获硕士学位,研究方向:人工智能、数据挖掘.