软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2016,27(6):1592−1601 [doi: 10.13328/j.cnki.jos.005007]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

同态公钥加密系统的图像可逆信息隐藏算法*

项世军, 罗欣荣

(暨南大学 信息科学技术学院 电子工程系,广东 广州 510632)

通信作者: 项世军, E-mail: Shijun_Xiang@qq.com

摘 要: 同态加密技术在加密信息、对信息进行隐私保护的同时,还允许密文数据进行相应的算术运算(如云端可直接对同态加密后的企业经营数据进行统计分析),已成为云计算领域的研究热点之一.然而,由于云存在多种安全威胁,加密后信息的安全保护和完整性认证问题仍然突出.另外,信息在加密后丢失了很多特性,密文检索成为了云计算需要攻克的关键技术.为了实现对加密图像的有效管理及其安全保护,提出了一种基于同态加密系统的图像可逆信息隐藏算法.该算法首先在加密前根据密钥选择目标像素,并利用差分扩展 DE(difference expansion)的方法将目标像素的各比特数据嵌入到其他像素中.然后,利用 Paillier 同态加密系统对图像进行加密得到密文图像.在加密域中,利用待嵌入信息组成伪像素,加密后替换目标像素,完成额外信息的嵌入.当拥有相应的密钥时,接收方可以分别在密文图像或明文图像中提取出已嵌入的信息.当图像解密后,通过提取出自嵌入目标像素的各比特数据来恢复原始图像.仿真实验结果表明,该算法能够在数据量保持不变的前提下完成同态加密域中额外信息的嵌入,信息嵌入快速高效,并可分别从加密域和明文域中提取出嵌入的信息.

关键词: 可逆信息隐藏;图像加密;同态加密系统;图像安全保护;云计算

中图法分类号: TP309

中文引用格式: 项世军,罗欣荣.同态公钥加密系统的图像可逆信息隐藏算法.软件学报,2016,27(6):1592−1601. http://www.jos.org.cn/1000-9825/5007.htm

英文引用格式: Xiang SJ, Luo XR. Reversible data hiding in encrypted image based on homomorphic public key cryptosystem. Ruan Jian Xue Bao/Journal of Software, 2016,27(6):1592−1601 (in Chinese). http://www.jos.org.cn/1000-9825/5007.htm

Reversible Data Hiding in Encrypted Image Based on Homomorphic Public Key Cryptosystem

XIANG Shi-Jun, LUO Xin-Rong

(Department of Electronic Engineering, School of Information Science and Technology, Ji'nan University, Guangzhou 510632, China)

Abstract: Homomorphic encryption, which protects privacy effectively and allows algebraic operations directly in the ciphertext, has been a active topic in the study of cloud computing. Due to security threats in cloud computing, the security protection and integrity authentication of encrypted data remain critical problems. The challenge lies in how to retrieve the encrypted data. To achieve more effective management and security protection of encrypted images on-line, this paper proposes a reversible data hiding scheme for ciphertext based on the public key cryptosystems with homomorphic and probabilistic properties. In the proposed scheme, partial pixels are selected as target pixels by a secret key and all bits of the target pixels are embedded into the other pixels with difference expansion (DE) to vacate room before encryption. As a bonus, secret data can be embedded directly in homomorphic encrypted domain by altering the target pixels with the fake pixels which are comprised of secret data. With the legal key, the receiver can extract the embedded data from the encrypted image and the directly decrypted image. Furthermore, user can accurately recover the original image after decryption

* 基金项目: 国家自然科学基金(61272414)
Foundation item: National Natural Science Foundation of China (61272414)
收稿时间: 2015-08-15; 修改时间: 2015-10-09; 采用时间: 2015-12-05; jos 在线出版时间: 2016-01-21
CNKI 网络优先出版: 2016-01-22 11:20:08, http://www.cnki.net/kcms/detail/11.2560.TP.20160122.1120.017.html

and data extraction. Finally, experimental results show that extra data can be embedded more efficiently in homomorphic encrypted domain while keeping the quantity of data unchanged. Besides, the embedded data can be extracted in both ciphertext and plaintext.

Key words: reversible data-hiding; image encryption; homomorphic cryptosystem; image security protection; cloud computing

随着互联网技术及云计算技术的快速发展,人们将更多的资料和数据上传到远程服务器或者云端进行存储,从而节省了购买实际物理储存设备的开支[1−3].用户可随时随地通过联网下载已上传的资料、利用网络中的其他资源以及享受第三方提供的数据处理等服务[4].这些技术在方便人们生活的同时,也引发了数据安全和隐私保护的问题.上传的数据可能涉及用户的隐私内容,如个人照片、企业的用户资料、电子票据等,用户应先对数据进行加密后再上传,以降低内容泄露的风险[5].然而,数据在加密后失去了许多的特性,随着用户和上传数据量的爆炸式增长,海量密文数据的检索及管理成为了急需攻克的关键技术[6].另外,由于存在安全漏洞或内部人员的非法操作,密文被非法访问后会受到篡改、替换等攻击,用户加密数据的完整性、可靠性保护尤为重要.

加密域中的可逆信息隐藏技术是在不知道明文内容的情况下,直接将额外信息嵌入到密文载体中,并在解密及信息提取后能够百分之百地恢复出原始载体的技术.该技术有着很好的应用前景,例如,患者的医学图像加密后上传到医院的服务器或云中[7],管理者可将图像的相关信息,如所有者信息、拍摄时间、拍摄部位等嵌入到对应的密文中,通过提取嵌入信息和比对相应的关键词,可实现对密文图像的快速检索;再有,设计师将作品加密后上传到数据库,再通过嵌入与密文相关的特征信息及版权信息,从而实现对加密数据的完整性认证和版权保护[8].加密域中的可逆信息隐藏技术较好地解决了密文检索及其安全保护的问题,并可在解密及数据提取后,恢复原始载体,近年来已成为了信息安全领域的一个研究热点.文献[7]提出一种基于流密码的可逆信息隐藏算法,该算法对图像进行分块后,通过翻转每个图像块中相应的LSB(least significant bit)来嵌入1比特数据,并在解密后利用相邻像素的相关性恢复出原始图像.随后,Hong 等人通过改进平滑函数[9]及非均匀翻转的方法[10]对文献[7]中的方法进行改进,减少了图像恢复时的错误率,提高了算法的嵌入率.文献[7,9,10]的算法中,信息提取及原图像恢复只能在解密后同时进行.因此,Zhang 提出了一种可分离的可逆信息隐藏算法[11],以实现加密域中的信息提取.该算法利用边信息及信源编码对加密图像的低几位数据进行压缩,以腾出额外信息的嵌入空间.为实现更好的性能,Ma 等人提出了一种加密前预留空间的算法[12],其核心思想是利用明文域的可逆信息隐藏算法将部分信息自嵌入到其他部分,该算法具有较大的嵌入容量及低失真的特点.

上述算法使用对称加密系统,密钥管理难度较大,利用流密码进行加密,不能对密文进行处理.而同态公钥加密系统为非对称加密系统,安全性更高,明文值与密文值一一对应,且允许对密文进行算术运算,更适用于云计算等第三方数据处理,如云端可直接计算出利用加性同态系统加密的企业经营数据、个人账单等数据的差 $E[x_i-x_j]$、和 $E[\sum x_i]$(解密后除以数据 x 的个数 n,可得到均值),从而为用户提供数据的统计分析服务.因此,Chen 等人提出了一种基于同态公钥加密系统的可逆信息隐藏算法[13].该算法先将明文图像中的每个像素分成两部分:LSB 和其余的整数部分,并用 Paillier 加密系统[14]进行加密.然后利用加密系统的同态特性,通过改变相邻两像素 LSB 的相对大小嵌入1比特数据.在接收端,解密后通过比较两相邻 LSB 的相对大小提取出嵌入信息.该算法将数据分成两部分后再加密,使得数据量成倍增长,且只能在解密后提取嵌入信息.2015 年,Zhang 等人提出了能分别在加密域及明文域中提取嵌入信息的可逆信息隐藏算法[15].该算法首先对明文进行直方图平移,对明文进行约束,再结合纠错码及密文域像素值平移的方法嵌入额外信息,使得嵌入的信息能够在明文域中提取出来;根据同态加密特性,利用 WPC(wet paper code)[16],将信息无损地嵌入到加密图像中,使得嵌入信息能够在密文域中提取.由于该算法利用 WPC 进行嵌入,信息隐藏者需要利用高斯消元法求解一个含有 k 个未知数的线性方程组,其中,k 为嵌入容量,该算法的计算复杂度为 $O(k^3)$.对于大嵌入容量的情况如 k=10^5,该算法嵌入过程耗时较长,不适用于云中加密图像的实时处理.针对上述算法的不足,本文提出了一种新的图像可逆信息隐藏算法,该算法首先根据密钥选出目标像素,并利用 DE 算法将目标像素嵌入到其他像素中,加密自嵌入后的图像得到加密图像,嵌入过程并没有造成数据量的增大.在加密域中,根据嵌入密钥将待嵌入的额外信息组成伪像素,加密后替换目标像素,实现信息嵌入的快速嵌入.只要拥有相应的密钥,接收者可计算出伪像素值的范围及其对应的密文,通过比对相应的密文,得到相应伪像素的值,完成加密域中的信息提取.此外,接收者还可以在解密后,提取自

嵌入的目标像素的数据,重组目标像素,从而恢复原图像,实现加密域中的可逆信息隐藏.本文算法传输数据量较小,计算复杂度较低,且具有足够的嵌入容量来嵌入加密图像相关标签信息、版权信息或图像特征信息等,更适用于云中加密图像的快速检索、版权保护及完整性认证.

1 Paillier 同态加密系统

同态加密系统首先由 Rivest 等人提出[17].在同态加密系统中,可直接对密文进行算术运算,得到的结果与明文域中对应运算的结果一致.为实现语义安全,Goldwasser 等人提出了一种具有概率特性的公钥加密系统[18].该系统的概率特性为:对于相同的明文,可通过不同的加密过程得到不同的密文,因此,加密密钥可以是公开的.同时具有同态特性和概率特性的加密技术已广泛应用于加密信号处理或第三方数据处理领域当中[19−21],如 Paillier 加密技术.Paillier 加密系统[14]是一种加性同态公钥加密系统,其加密和解密机制如下:

密钥生成.随机选择两个大的质数 p 和 q,计算他们的乘积 N 以及 $p-1$、$q-1$ 的最小公倍数 λ.然后再随机选取一个整数 $g\in Z_{N^2}^*$, 且 g 满足:

$$gcd\left(L\left(g^{\lambda} \bmod N^2\right), N\right)=1 \tag{1}$$

其中,函数 $L(u)=(u-1)/N$, $Z_{N^2}^*$ 为 Z_{N^2} 中与 N^2 互质的整数的集合,而 Z_{N^2} 为小于 N^2 的整数的集合.(N,g)和 λ 分别为公钥和私钥.

加密过程.再随机选取一个整数 $r\in Z_N^*$, 对于明文 $m\in Z_N$,可通过公式(1)得到对应的密文 c:

$$c=g^m\cdot r^N \bmod N^2 \tag{2}$$

其中, $c\in Z_{N^2}^*$, 记公式(2)为 $c=E[m,r]$.因此,利用相同的公钥进行加密时,由于 r 的选取是随机的,对于同一个明文 m,可得到不同的密文 c,从而保证了密文的语义安全.

解密过程.对密文 c 的解密过程为

$$m=D[c]=\frac{L\left(c^{\lambda} \bmod N^2\right)}{L\left(g^{\lambda} \bmod N^2\right)} \bmod N \tag{3}$$

另外,文献[14]给出了定理 1.

定理 1. 若 g 的阶为 N 的非零整数倍,则 $c=E[m,r]$是双射的.

即当 g 满足上述要求时, $\forall(m,r)\,|\,m\in Z_N, r\in Z_N^*$ 都有唯一的 $c=E[m,r]$与之一一对应.本文算法将利用该定理实现在加密域中嵌入信息的提取.

2 基于同态加密的图像可逆信息隐藏算法

本文提出的图像可逆信息隐藏算法的框架如图 1 所示.

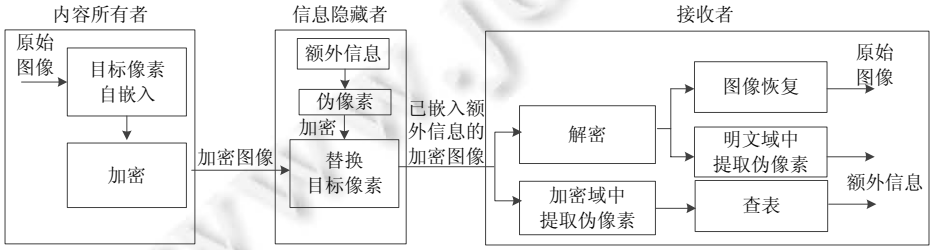

Fig.1 Sketch of the reversible data hiding scheme in encrypted image based on homomorphic cryptosystem

图 1 基于同态加密系统的图像可逆信息隐藏算法框架

内容所有者首先根据密钥选取目标像素,并利用 DE 算法将目标像素的每一比特数据嵌入到其他像素中,预留出嵌入空间.然后将完成自嵌入的图像加密后传递给信息隐藏者.信息隐藏者将待嵌入的额外信息组成伪像素,加密后替换目标像素,完成加密域中的信息嵌入.接收方拥有相应的密钥时,可分别在加密域和明文域中

完成信息的提取:(1) 从加密图像中提取加密后的伪像素,根据密钥计算出伪像素可能取值与对应密文的映射表,通过查表的方法确定伪像素的值,再提取出额外信息;(2) 根据密钥直接从解密后的图像中提取伪像素原值,提取出嵌入信息.此外,接收者对图像进行解密后,提取出自嵌入数据,重组目标像素,可百分之百地恢复出原图像.

2.1 预留嵌入空间

1) 图像的分块和分组.首先将原始图像 I 分成大小为 $l\times l$ 的图像块,不妨设 I 的大小为 $M\times N$,M 和 N 都是 l 的整数倍.然后以每 4 个像素为一组将图像块分成多个 T 型像素组.每个像素组由一个中心像素 R 和 3 个边缘像素 s 组成.图 2 为 l=8 时图像块分组示意图.

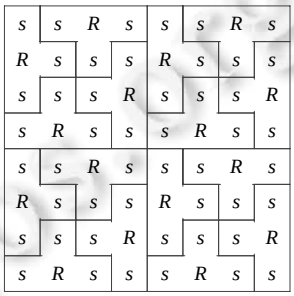

Fig.2 Patch division for a pixel block sized 8×8

图 2 8×8 图像块的分组示意图

2) 目标像素自嵌入.内容所有者利用自嵌入密钥 k_{se1},选取部分边缘像素作为目标像素,记为 $S_{i,j}^T$. 取出 $S_{i,j}^T$ 的各比特数据 $b=\{b_{i,j}(k)\,|\,i,j\in I,k=0,1,...,7\}$, 其中,

$$b_{i,j}(k)=\left\lfloor \frac{S_{i,j}^T}{2^k} \right\rfloor \bmod 2,\ k=0,1,2,...,7 \tag{4}$$

根据自嵌入密钥 k_{se2},在每个图像块中选取另外的边缘像素用于 b 的自嵌入,记为嵌入像素 $S_{i,j}^e$. 对于每个像素组,保持中心像素 R 的值不变,对 $S_{i,j}^e$ 进行差分扩展 DE,得到扩展后的嵌入像素 $S_{i,j}^E$.

$$S_{i,j}^E=R+(S_{i,j}^e-R)\times 2 \tag{5}$$

然而,差分扩展及信息嵌入后可能会引起数据的溢出,即 $S_{i,j}^E$ 满足:

$$\begin{cases} S_{i,j}^E+1\geqslant 255 \\ S_{i,j}^E\leqslant 0 \end{cases} \tag{6}$$

当公式(7)成立,称对应的 $S_{i,j}^E$ 为溢出像素,用辅助信息 a_o 记录溢出的部分:

$$a_o=\begin{cases} S_{i,j}^E-254, & \text{if } S_{i,j}^E+1\geqslant 255 \\ 0-S_{i,j}^E, & \text{if } S_{i,j}^E\leqslant 0 \end{cases} \tag{7}$$

记 a_o 中的最大值 $\max(a_o)$,并将其转换成二进制数表示,记该二进制数的最小长度为 L_1,然后将 a_o 的每个数据转换成长度为 L_1 的二进制数,得到 a.

然后对扩展后的像素 $S_{i,j}^E$ 进行修正,得到修正后的扩展像素 $S_{i,j}^M$.

$$S_{i,j}^M=\begin{cases} 255, & \text{if } S_{i,j}^E+1\geqslant 255 \\ 0, & \text{if } S_{i,j}^E\leqslant 0 \\ S_{i,j}^E, & \text{else} \end{cases} \tag{8}$$

为了保证原图像能够无损恢复,目标像素数据 b 和辅助信息 a 都要自嵌入到图像中,记 $w_0=\{a,b\}$,则自嵌入过程为

$$S_{i,j}^{\sim}=\begin{cases}S_{i,j}^{M}, & \text{if } S_{i,j}^{M}=0 \text{ or } S_{i,j}^{M}=255\\ S_{i,j}^{M}+w_0, & \text{else}\end{cases} \tag{9}$$

其中, $S_{i,j}^{\sim}$ 为自嵌入后的像素值,这样就完成的目标像素的自嵌入,除此之外,其他像素保持不变,得到自嵌入后的图像 $I^{\sim}$.

2.2 图像加密

在完成自嵌入后,内容所有者按照第 1 节 Paillier 加密系统中描述的加密过程,对 $I^{\sim}$ 中的每个像素值 m 随机选取一个整数 $r_m\in Z_n^*$, 记 $r_0=\{r_m\mid r_m\in Z_n^*, m\in I^{\sim}\}$, 再利用公钥$(N,g)$进行加密,加密过程记为 $E[\cdot]$,则有:

$$c=E[m,r_m]=g^m\cdot r_m^N \bmod N^2 \tag{10}$$

其中,c 为密文数据.内容所有者将加密后的图像及自嵌入密钥 k_{se1} 传递给信息隐藏者,将自嵌入密钥 k_{se1}、k_{se2}、L_1 传递给接收者.

2.3 信息嵌入

由于目标像素的数据已自嵌入到图像中,可直接用待嵌入数据组成伪像素,加密后替换目标像素完成嵌入.考虑到直接解密后图像的质量,需要限制伪像素的值的范围.图像的质量用 PSNR(peak signal to noise ratio)来衡量,其计算公式为

$$PSNR=10lg\frac{Num\times 255^2}{\sum_{m=1}^{Num1}\left(S_m^T-F\right)^2+\sum_{n=1}^{Num2}\left(S_n^e-S_n^E\right)^2} \tag{11}$$

其中,Num 为像素的总的个数,$Num1$ 为目标像素 S^T 的个数,$Num2$ 为嵌入像素的 S^e 个数,F 为伪像素.对于自然图像,像素的灰度值集中于[25,230]的范围内.为了提高 PSNR,本文把 F 的均值定为 128.信息隐藏者将待嵌入数据 d 按每 n 比特为一组进行分组(n=1,2,…,8),分别为 $d_0,...,d_{n-1}$, 按公式(11)计算得到 F_1,再加上相应的偏移量得到伪像素 F.

$$F_1=\sum_{m=0}^{n-1}2^m\cdot d_m \tag{12}$$

$$F=F_1+128-2^{n-1} \tag{13}$$

因此,F 的取值范围为$[128-2^{n-1},128+2^{n-1}-1]$与 F_1 的值$[0,2^n-1]$一一对应.

信息隐藏者选取一个整数 $r_1\in Z_N^*$, 根据第 1 节提及的加密过程,利用公钥(N,g)对伪像素进行加密,得到 $E[F,r_1]$,再利用自嵌入密钥 k_{se1},确定目标像素的位置,用加密后的伪像素替换目标像素,完成加密域中的信息嵌入.这里,(r_1,n)为信息隐藏密钥.

2.4 信息提取

2.4.1 加密域中的信息提取

当拥有公钥(N,g)、自嵌入密钥 k_{se1} 和信息隐藏密钥(r_1,n)时,接收者可根据以下 5 个步骤,直接从密文图像中直接提取已嵌入的信息.

第 1 步.首先利用自嵌入密钥 k_{se1},提取出加密后的伪像素 $E[F,r_1]$.

第 2 步.根据 n,求得伪像素的取值范围:$[128-2^{n-1},128+2^{n-1}-1]$.

第3步.利用公钥(N,g)和 r_1,求得伪像素的每一个可能值$F_p=128-2^{n-1},\ldots,0,\ldots,128+2^{n-1}-1$ 对应的密文 $E[F,r_1]$,由第 1 节定理 1 可知, $\forall(m,r)\mid m\in Z_N, r\in Z_N^*$ 都有唯一的 $c=E[m,r]$与之对应.F_p 与 $E[F_p,r_1]$的映射表如图 3 所示.

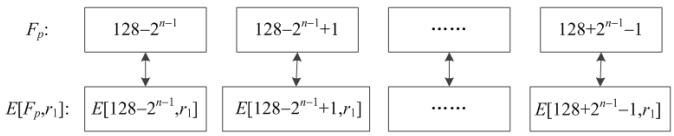

Fig.3 One-to-One match between F_p and $E[F_p,r_1]$

图 3 F_p 与 $E[F_p,r_1]$的映射表

第 4 步.因为伪像素的值只能为 F_p,则对应的密文只能取 $E[F_p,r_1]$的值.因此,伪像素 $E[F,r_1]$与 $E[F_p,r_1]$进行比对,再通过上述映射表得到的 F_p,即为伪像素的原值 F(可先对 $E[F_p,r_1]$进行排序,再利用二分查找等方法进行快速查找),然后减去相应的偏移量 $128-2^{n-1}$,得到由额外信息组成的 F_1.

第 5 步.通过公式(14)取出 F_1 的低 n 位数据 $d_0,...,d_{n-1}$,提取出嵌入的信息.

$$d_m=\left\lfloor \frac{F_1}{2^m} \right\rfloor \bmod 2, m=0,1,...,n-1 \tag{14}$$

2.4.2 明文域中的信息提取

当拥有自嵌入密钥 k_{se1}、信息隐藏密钥 n 以及私钥λ时,接收者可从含额外信息的明文图像中提取出嵌入的额外信息.接收者首先根据第 1 节提及的加密过程,利用私钥λ对密文图像进行解密,得到已嵌入信息的明文图像.然后利用自嵌入密钥 k_{se1} 取出伪像素 F,直接减去相应的偏移量 $128-2^{n-1}$,得到由额外信息组成的 F_1.最后按照公式(14)提取出嵌入的信息.

2.5 原图像恢复

图像恢复的具体步骤如下:

1) 图像解密.首先利用私钥λ,根据第 1 节中的解密过程对图像进行解密.

2) 图像分块和分组.按照与发送端同样的方式对图像进行分块和分组.

3) 自嵌入信息提取.根据自嵌入密钥 k_{se2},找到自嵌入像素 $S_{\tilde{i},j}$,对于 $S_{\tilde{i},j}$ 满足[1,254],可取出对应自嵌入信息 w_0.

$$w_0=(S_{\tilde{i},j}-R) \bmod 2 \tag{15}$$

其中,R 为 $S_{\tilde{i},j}$ 所在像素组的中心像素.

4) 自嵌入像素恢复.接收者统计溢出像素 $S_{\tilde{i},j}\in\{0,255\}$ 的个数 $Num3$,计算出 a 的长度 $L_2=L_1\times Num3$,根据 L_1,L_2 从 w_0 中提取出 a 和 b,并对 a 进行分组,每组有 L_1 比特.利用形如公式(18)的方式,重组 a_o,从而计算出溢出像素对应的扩展后的值 $S_{i,j}^E$.

$$S_{i,j}^E=\begin{cases} S_{\tilde{i},j}+a_o, & S_{\tilde{i},j}=255 \\ -a_o, & S_{\tilde{i},j}=0 \end{cases} \tag{16}$$

接收者可根据公式(17)恢复出自嵌入像素的原值 $s_{i,j}$.

$$s_{i,j}=\begin{cases} \left\lfloor \dfrac{S_{i,j}^E+R}{2} \right\rfloor, & \text{if } S_{\tilde{i},j}=0 \text{ or } 255 \\ \left\lfloor \dfrac{S_{\tilde{i},j}+R}{2} \right\rfloor, & \text{else} \end{cases} \tag{17}$$

5) 目标像素恢复.接收者将 b 进行分组,每 8 比特为一组,记为 $b_0,b_1,...,b_7$.按公式(18)重组目标像素 $S_{i,j}^T$.

$$S_{i,j}^T=\sum_{k=0}^{7} b_k\cdot 2^k \tag{18}$$

最后根据嵌入密钥 k_{se1},按顺序将由上式求得的 $S_{i,j}^T$ 替换伪像素,实现原图像的恢复.

3 实验结果及分析

本文首先给出以 Lena 为载体的实验结果,验证本文算法的可行性.该实验选取 8 比特灰度图像,图像大小为

512×512,取分块大小 l=32,每个伪像素嵌入比特数 n=4,即在每个大小为 32×32 的图像块中选择一个目标像素,用一个含 4 比特额外信息伪像素替换该目标像素进行嵌入,具体实验结果如图 4 所示.内容所有者根据自嵌入密钥,从原始图像图 4(a)中选取目标像素,并将目标像素的各比特信息嵌入到其他边缘像素,得到自嵌入后的图像图 4(b),该图像的 PSNR 为 42.9dB.然后,利用 Paillier 加密系统对图 4(b)进行加密,得到加密图像.信息隐藏者根据信息隐藏密钥将 1 024 比特额外信息直接嵌入到加密图像中,得到含额外信息的加密图像,其对应的直接解密后的图像如图 4(c)所示,其 PSNR 为 40.61dB,图像质量较好.而在接收端,接收者可根据相应的密钥对图像解密,然后提取出自嵌入的目标像素的数据,得到恢复后的图像如图 4(d)所示.该图像对应的 PSNR 为+∞,表明恢复出来的图像与原图像完全相同,恢复了原始图像,实现了加密域中的可逆信息隐藏.

(a) 原始图像 (b) 自嵌入后的图像(42.9dB)

(c) 直接解密后图像(40.61dB) (d) 恢复后的图像(+∞)

Fig.4 Experiment results with cover Lena

图 4 以 Lena 为对象的实验结果

然后以 Man 等 8 幅灰度图像为载体,对本文算法进行的性能测试,在不同的分块大小 l 及每个伪像素嵌入信息的比特数 n 下,PSNR 值及其对应嵌入容量见表 1.当 l=32 时,嵌入 512、1 024、1 536、1 792、2 048 比特额外信息时,对应于在每个大小为 32×32 的图像块中选取一个目标像素,每个目标像素嵌入分别嵌入 n=2,4,6,7,8 比特.由表 1 可知,当 $n\leqslant 6$ 时,对应的 PSNR 相差不大,但 n=7,8 时,PSNR 值分别出现约 1dB、3dB 的衰减.而随着 l 的减小,保持每个块中选取一个目标像素,需要进行扩展、用于目标像素自嵌入的边缘像素增加,伪像素的个数也随之增加,使得对应的 PSNR 明显下降.

Table 1 Embedding rate-PSNR performance of the proposed scheme on different cover images (dB)

表1 不同嵌入容量下的 PSNR 值(dB)

Capacity (bit)	*l*=32					*l*=16		*l*=8	
	512	1 024	1 536	1 792	2 048	4 096	7 168	16 384	28 672
Lena	40.617	40.612	40.411	39.751	37.73	34.685	33.895	28.741	27.816
Plane	38.443	38.44	38.319	37.896	36.472	32.661	31.979	26.638	26.026
Lake	37.685	37.687	37.605	37.271	36.052	31.834	31.346	25.717	25.224
Baboon	34.606	34.604	34.545	34.354	33.652	28.65	28.389	22.544	22.292
Camera	39.696	39.684	39.511	38.949	37.184	33.79	33.079	27.82	27.059
Man	39.306	39.287	39.082	38.52	36.826	33.315	32.64	27.381	26.698
Pens	38.336	38.327	38.178	37.74	36.316	32.407	31.827	26.396	25.834
Pepper	39.843	39.845	39.69	39.141	37.357	33.729	33.101	27.475	26.795
Average (dB)	38.566	38.561	38.418	37.953	36.449	32.634	32.032	26.589	25.968

图 5 为以 Lena 和 Man 两幅标准测试图像为载体,本文算法与文献[7,9]在 PSNR 及嵌入容量两方面的性能对比.文献[7,9]均采用流密码进行加密,在保持数据量不变的前提下直接对加密图像嵌入额外信息,计算复杂度较低.如图所示,在相同的嵌入率下,本文算法的 PSNR 值要比文献[7,9]的高.这是因为 Lena 和 Man 两幅图像相对平滑,且灰度值相对较集中于[92,160],使得差分扩展及信息嵌入对图像质量的影响变小,因而算法性能较优,而对于纹理较丰富的图像如 Baboon,或灰度值并不集中于 128 的图像如 Lake,算法性能会有所下降.对于嵌入容量,由于要利用像素间的相关性无损恢复图像,文献[7,9]中算法的嵌入容量较低,对于上述两幅图像,最大嵌入率仅为 0.003 9bpp 和 0.006 9bpp,在直接解密图像的 PSNR 为 32dB 的情况下,本文算法的嵌入率可达 0.015 6bpp,容量相对较大.此外,本文利用同态加密系统进行加密,更适用于云计算等第三方信号处理领域,扩展性好、实用价值高.

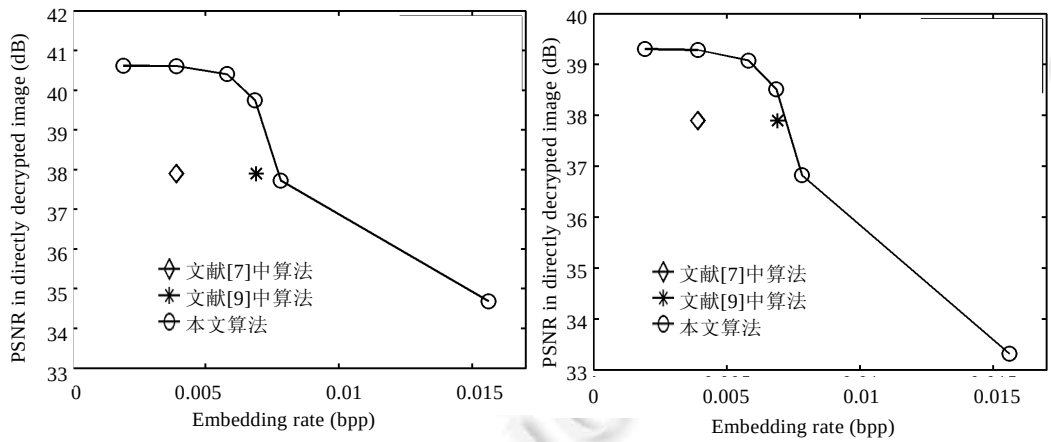

Fig.5 Comparision of embedding rate-PSNR with previous methods encrypted by stream cipher

图 5 与经典流加密算法的嵌入容量-PSNR 性能比较

文献[13,15]是两个典型的同态加密域中的图像可逆信息隐藏算法,且具有较大的嵌入容量及较好的图像质量.表 2 为本文算法与文献[13,15]在数据量、信息提取对象及计算复杂度的对比.

Table 2 Comparision of data quantity,object of data extraction and computation complexty with previous methods using homomorphic cryptosystem

表2 与现有同态加密算法的数据量、数据提取对象及计算复杂度对比

	传输数据量	信息提取对象	计算复杂度
文献[13]	加密图像的 2 倍	明文图像	$O(k)$
文献[15]	加密后的图像	加密图像、明文图像	$O(k^3)$
本文算法	加密后的图像	加密图像、明文图像	$O(k)$

文献[13]中,内容所有者将明文像素值分成 LSB 和余下的整数,加密后需要将这两路数据传给信息隐藏者,因此,传输的数据为原加密图像的两倍.另外,信息隐藏者利用同态特性改变相邻 LSB 的相对大小来嵌入信息,而利用同态加密系统加密后的数据无法判别对应明文的大小,因此只能从解密图像中提取信息;该算法的计算复杂度为 $O(k)$,其中 k 为嵌入容量.而文献[15]首先对明文像素值进行约束,加密后通过两次嵌入确保嵌入信息能够在嵌入后的加密图像和直接解密图像进行提取:(1) 利用 WPC 进行嵌入,使得信息可在加密域中提取;(2) 利用直方图平移嵌入信息,使得信息可在明文域提取.该算法传输的数据量保持不变,但由于利用 WPC,该算法在嵌入时需要求解含 k 个未知数的线性方程,计算复杂度为 $O(k^3)$,对于容量较高如 $k=10^5$,计算耗时过长,并不适用于云中存储的对加密图像进行实时处理.而本文算法首先将目标像素嵌入到原图像中,加密后利用由额外信息组成的伪像素替换目标像素完成信息的嵌入.伪像素的值的范围受限于嵌入密钥,接收者可在加密域或明文域中,根据密钥求出伪像素的可能值,通过比对便可提取信息.因此,相比文献[13,15],本文算法所要传输的数据量较低,计算复杂度仅为 $O(k)$,能够快速地嵌入和提取信息,且能够在加密域和明文域中完成信息的提取,更适用于云中加密图像的快速检索、完整性认证等.虽然,本文算法相对于文献[13,15]嵌入容量较低,但对于大小为 512×512 的图像,PSNR 为 32dB 时,嵌入容量为 7 168 比特,这对于在云中进行图像相关关键词索引、特性信息等嵌入操作来说,是足够的.

4 总 结

本文提出了一种基于同态公钥加密系统的图像可逆信息隐藏算法,该算法首先根据嵌入密钥选取目标像素,然后利用 DE 算法将目标像素嵌入到明文图像中,再利用 Paillier 加密系统进行加密,得到加密图像.信息隐藏者利用待嵌入信息组成伪像素,加密后替换目标像素完成信息嵌入.在接收端,可根据密钥计算出伪像素的明文值范围与其密文值的映射表,从密文图像中提取出加密后的伪像素后,通过比对和查表,得到伪像素的值,或在解密后根据密钥提取伪像素,最后从伪像素中提取已嵌入的信息.此外,接收者在解密后提取出自嵌入信息,恢复自嵌入像素和目标像素,从而恢复出原始图像.本文算法能够在数据量保持不变的前提下完成同态加密域中额外信息的嵌入;计算复杂度较低,信息的嵌入和提取快速高效,并可分别从加密域和明文域中提取出嵌入的信息.利用本文算法,管理者可向云或服务器中的加密图像嵌入相应的标签、版权信息或图像的特征信息,实现对加密图像的快速检索、版权认证及内容安全保护.因此,本文所提出的同态加密域信息隐藏算法对云计算中加密图像的管理和保护具有重要意义.

References:

[1] Hsu CY, Lu CS, Pei SC. Image feature extraction in encrypted domain with privacy-preserving SIFT. IEEE Trans. on Image Processing, 2012,21(11):4593−4607. [doi: 10.1109/TIP.2012.2204272]

[2] Creeger M. Cloud computing: An overview. ACM Queue, 2009,7(5):1−5. [doi: 10.1145/1551644.1551646]

[3] Hurwitz J, Bloor R, Kaufman M, Halper F, Cloud Computing for Dummies. Wiley Publishing Inc., 2009.

[4] Chow R, Golle P, Jakobsson M, Shi E, Staddon.J, Masuoka R, Molina J. Controlling data in the cloud: Outsourcing computation without outsourcing control. In: Proc. of the 2009 ACM Workshop on Cloud Computing Security (CCSW 2009). 2009. 85–90. [doi: 10.1145/1655008.1655020]

[5] Lagendijk RL, Zekeriya E, Barni M. Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation. IEEE Signal Processing, 2013,30(1):82−105. [doi: 10.1109/MSP.2012.2219653]

[6] Feng DG, Zhang M, Zhang Y, Xu Z. Study on cloud computing security. Ruan Jian Xue Bao/Journal of Software, 2011,22(1): 71−83 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3958.htm [doi: 10.3724/SP.J.1001.2011.03958]

[7] Zhang XP. Reversible data hiding in encrypted image. IEEE Signal Processing Letters, 2011,18(4):255−258. [doi: 10.1109/LSP.2011.2114651]

[8] Zheng HY, Gao Z, Xiao D. Novel reversible data embedding algorithm for encrypted image. Computer Engineering and Applications, 2014,50(7):186−189 (in Chinese with English abstract).

[9] Hong W, Chen TS, Wu HY. An improved reversible data hiding in encrypted image using side match. IEEE Signal Processing Letters, 2012,19(4):199−202. [doi: 10.1109/LSP.2012.2187334]

[10] Hong W, Chen TS, Kao YH. Reversible data embedment for encrypted cartoon images using unbalanced bit flipping. Advances on Swarm Intelligence Lecture Notes in Computer Science, 2013,7929:208−214. [doi: 10.1007/978-3-642-38715-9_25]

[11] Zhang XP. Separable reversible data hiding in encrypted image. IEEE Trans. on Information Forensics and Security, 2012,7(2): 826−832. [doi: 10.1109/TIFS.2011.2176120]

[12] Ma KD, Zhang WM, Zhao XF, Yu NH, Li FH. Reversible data hiding in encrypted images by reserving room before encryption. IEEE Trans. on Information Forensics and Security, 2013,8(3):553−562. [doi: 10.1109/TIFS.2013.2248725]

[13] Chen YC, Shiu CW, Horng G. Encrypted signal-based reversible data hiding with public key cryptosystem. Journal of Visual Communication and Image Representation, 2014,25:1164−1170. [doi: 10.1016/j.jvcir.2014.04.003]

[14] Paillier P. Public-Key cryptosystems based on composite degree residuosity classes. In: Proc. of the Int'l Conf. on the Theory and Application of Cryptographic Techniques Prague. Czech Republic, 1999. 223−238. [doi: 10.1007/3-540-48910-X_16]

[15] Zhang XP, Loong J, Wang Z, Cheng H. Lossless and reversible data hiding in encrypted images with public key cryptography. IEEE Trans. on Circuits and Systems for Video Technology. [doi: 10.1109/TCSVT.2015.2433194]

[16] Fridrich J, Goljan M, Lisonek P, Soukal D. Writing on wet paper. IEEE Trans. on Signal Processing, 2005,53(10):3923−3935. [doi: 10.1109/TSP.2005.855393]

[17] Rivest R, Adleman L, Dertouzos M. On data banks and privacy homomorphisms. In: Foundations of Secure Computation. Cambridge: MIT Press, 1978. 169−178.

[18] Goldwasser S, Micali S. Probabilistic encryption. Journal of Computer and System Sciences. 1984,28(2):270−299. [doi: 10.1016/0022-0000(84)90070-9]

[19] Bianchi T, Piva A, Barni M. On the implementation of the discrete Fourier transform in the encrypted domain. IEEE Trans. on Information Forensics and Security, 2009,4(1):86−97. [doi: 10.1109/TIFS.2008.2011087]

[20] Bianchi T, Piva A, Barni M. Composite signal representation for fast and storage-efficient processing of encrypted signals. IEEE Trans. on Information Forensics and Security, 2010,5(1):180−187. [doi: 10.1109/TIFS.2009.2036230]

[21] Zheng PJ, Huang JW. Discrete wavelet transform and data expansion reduction in homomorphic encrypted domain. IEEE Trans. on Image Processing, 2013,22(6):2455−2468. [doi: 10.1109/TIP.2013.2253474]

附中文参考文献:

[6] 冯登国,张敏,张妍,徐震,云计算安全研究,软件学报,2011,22(1):71−83. http://www.jos.org.cn/1000-9825/3958.htm [doi: 10.3724/SP.J.1001.2011.03958]

[8] 郑洪英,高真,肖迪,密文图像中的可逆信息隐藏算法,计算机工程与应用,2014,50(7):186−189.

项世军(1974−),男,贵州普定人,博士,教授,CCF 高级会员,主要研究领域为信息隐藏,多媒体技术与信息安全,加密域信号处理.

罗欣荣(1990−),男,硕士,主要研究领域为多媒体技术与信息安全,加密域可逆信息隐藏.