

一种基于背包问题的图像加密算法

崔艳 张永红¹

(西安财经学院统计学院, 西安 710048; 渭南师范学院数学系¹, 渭南 714000)

摘要 提出了一种基于背包问题的数字图像公开密钥加密算法, 利用该算法可以实现对图像的快速、安全加密。实验证明, 该算法对图像加密效果良好。

关键词 超递增序列 背包问题 图像加密

中图法分类号 TP391.41; **文献标识码** A

随着计算机网络的发展, 数字图像数据越来越多地在网上传输、交流, 数字信息与网络给人们带来方便的同时, 也带来了安全问题, 信息的安全与保密显得尤为重要。保证图像数据的方法分为两类: 数字水印技术和图像加密技术, 前者能为数字图像提供有效的版权保护, 后者能保证数字图像不被未经授权的人使用。图像加密算法根据密钥性质分为私钥密码和公钥密码。目前, 公钥加密算法由于受加密速度、安全性等的限制, 通常用于加密少量数据和慢速数据加密的场合。然而, 公钥加密算法使用公开密钥来对数据进行加密, 使用私人密钥来解密, 而且加密密钥是可以公开的, 使得利用公钥加密算法, 不仅可以对图像数据加密, 还可以进行数字签名^[1], 从而为图像数据的存储和传输提供了方便。一般地, 公钥加密算法都是基于某些数学难解问题而设计的, 本文所研究的加密算法就利用了背包难题(knapsack problem)。

1 算法原理

背包问题是^[2, 3]已知一个长度为 b 的背包及长度分别为 $a_1, a_2, \dots, a_n$ 的 n 个物品, 假定这些物品

的半径和背包相同, 若从这 n 个物品中选出若干个正好装满这个背包, 现在反过来求解究竟是哪些物品。 $x_i = 0$ 或 $1, i = 1, 2, \dots, n$, 使满足:

$$\sum_{i=1}^n a_i x_i = b。$$

其中 $a_1, a_2, \dots, a_n$ 和 b 都是整数。

背包问题属于 NP 类问题(nondeterministic polynomial time-problem), 而且是 NP 类问题中难度最大的 NP 完备类(NP-complete problem), 目前求解这一类问题还没有有效的多项式算法, 所以一般的背包问题在计算上是安全的。但并非所有的背包问题都没有有效的多项式算法, 如若序列 $a_1, a_2, \dots, a_n$ 满足条件: $\sum_{j=1}^{i-1} a_j \leq a_i; i = 2, 3, \dots, n$ 时, 则有多项式解法, 这样的序列称为超递增序列(Super-increasing sequence)。由该序列可以生成相应的背包序列, 具体过程如下:

$$b_k \equiv \omega a_k \pmod{m} \quad k = 1, 2, \dots, n。$$

其中 $m > 2a_n$, ω 和 m 互素, $\omega\omega \equiv 1 \pmod{m}$ 。以上过程称为 Merkle-Hellman 变换。这样, 就可以从超递增背包序列 $a_1, a_2, \dots, a_n$ 得到相应的背包序列 $b_1, b_2, \dots, b_n$ 。一般来说, $b_1, b_2, \dots, b_n$ 不再具有超递增性, 是非超递增背包序列。背包公钥密码体制便是以非超递增背包序列作为公钥, 而以超递增背包序列作为私钥的。

假定已知:

$$c = b_1 m_1 + b_2 m_2 + \dots + b_n m_n。$$

其中 $m_1, m_2, \dots, m_n \in \{0, 1\}$, c 为 $m = m_1 m_2 \dots m_n$ 的密文,则解密过程为:

$$\varpi c = \varpi b_1 m_1 + \varpi b_2 m_2 + \dots + \varpi b_n m_n = a_1 m_1 + a_2 m_2 + \dots + a_n m_n \pmod{m}.$$

这样,根据 $a_1, a_2, \dots, a_n$ 是超递增序列的条件,可以解出唯一的 $m = m_1 m_2 \dots m_n$ 。这样的公钥加密体制相应称为背包公钥密码体制。

2 加密和解密算法

根据以上背包公钥密码体制的思想,结合图像的数据特点,可以构造基于公钥密码体制的数字图像公钥加密算法^[4, 5]。

设 $a_1, a_2, \dots, a_8$ 满足: $0 < a_i < 256, i = 1, 2, \dots, 8$ 是一个超递增序列,根据背包公钥密码的思想,我们取 $m = 512, \omega$ 和 m 互素, ϖ 满足 $\omega \cdot \varpi \equiv 1 \pmod{512}$ 。根据已有的超递增序列 $a_1, a_2, \dots, a_8$,我们可以生成相应的背包序列为:

$$b_k \equiv \omega a_k \pmod{512}; k = 1, 2, \dots, 8 \quad (1)$$

这样,得到用于公钥加密的背包序列: $b_1, b_2, \dots, b_8$ 。相应可得到以下关系:

$$a_k \equiv \varpi b_k \pmod{512}; k = 1, 2, \dots, 8 \quad (2)$$

根据以上的背包序列,我们给出加密解密算法分别如下^[6]:

算法 1: 基于背包公钥密码的数字图像加密算法

Step1: 根据已知的超递增序列 $a_1, a_2, \dots, a_8$ 和 ω 的值,由公式(1)生成相应的用于加密过程的公钥 $b_1, b_2, \dots, b_8$ 。

Step2: 输入需要加密的图像 $Image$, 对图像的像素灰度值 $Image(i, j)$ 进行以下运算。

Step3: 将像素灰度值转化为相应的二进制表示,得到的 $\{0, 1\}$ 序列记为: $c_1 c_2 \dots c_8$ 。

Step4: 根据得到的 $c_1 c_2 \dots c_8$ 进行以下计算: $c = c_1 b_1 + c_2 b_2 + \dots + c_8 b_8 \pmod{512}$, 得到相应的加密图像 $Enimage$ 的相应像素灰度值为: $Enimage(i, j) = \lfloor c/2 \rfloor$ 。

Step5: 当计算完所有像素的值以后,循环结束,

得到相应的加密图像 $Enimage$ 。

相应的解密算法为:

算法 2: 基于背包公钥密码的数字图像解密算法

Step1: 输入需要解密的图像 $Enimage$ 和解密的密钥 $a_1, a_2, \dots, a_n$ 和 ϖ 。

Step2: 对解密图像的像素灰度值 $Enimage(i, j)$ 进行计算: $c' = \varpi (2 \times c) \pmod{512}$, 根据加密过程可知: $c' = \varpi b_1 c_1 + \varpi b_2 c_2 + \dots + \varpi b_8 c_8$ 。

Step3: 根据公式(2)计算: $c' = a_1 c_1 + a_2 c_2 + \dots + a_8 c_8$, 由于 $a_1, a_2, \dots, a_8$ 是超递增序列,所以可以唯一确定 $\{0, 1\}$ 序列 $c_1 c_2 \dots c_8$ 的值。

Step4: 将 $\{0, 1\}$ 序列 $c_1 c_2 \dots c_8$ 转化为灰度值 k , 即为解密图像的灰度值 $Deimage(i, j)$ 。

Step5: 当计算完所有的像素时,循环结束,得到的就是解密图像 $Deimage$ 。

3 图例

根据算法,实验的结果如下图所示:图 1 中 $\omega = 171$, 超递增序列为: 1, 3, 5, 10, 20, 40, 80, 160, 相应的 $\varpi = 3$, 背包序列为: 171, 1, 343, 174, 348, 184, 368, 224。

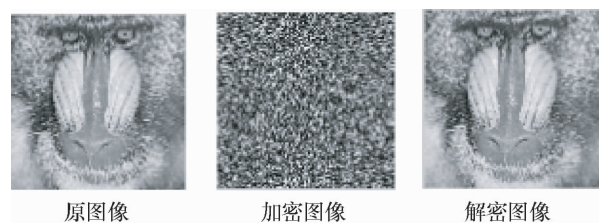


图 1 加密图像和解密图像

图 2 中 $\omega = 171$, 超递增序列为: 3, 5, 8, 16, 32, 64, 128, 256, 相应的 $\varpi = 3$, 背包序列为: 1, 343, 344, 176, 352, 192, 384, 256。

4 算法分析

基于背包公钥密码的数字图像加密算法,通过比较加密算法和解密算法可知,对于解密图像和原

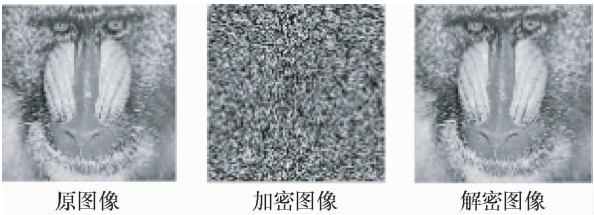


图 2 加密图像和解密图像

图像进行比较,相应像素的灰度值相差不会超过 1,这是因为可能出现的误差是由 $|c/2|$ 引起的,在恢复过程中可能影响到 $\{0,1\}$ 序列 $c_1c_2\cdots c_8$ 的最末位,该位对应的灰度值影响为 1。所以,通过实验可以发现,解密图像与原图像比较,差别是很小的,说明算法恢复效果良好。

对于算法的安全性,根据背包公钥密码体制的结论可知,是由背包序列的安全性决定的,所以,该算法也具有较好的安全性。

5 结论

本文给出了一种基于背包公钥密码的数字图像加密算法,实验证明,该算法的加密效果和解密效

果理想,而且,该算法适用于对数字图像进行公钥加密,从而保证了算法具有较大的适用范围。但是,算法的安全性还有待于进一步提高,当然,可以通过扩大算法中取模运算的范围,或者引入概率加密的方法来增加算法的安全性^[7],但这样将会使算法的解密效果受到影响,如何解决这些问题,还需要做很多工作。

参 考 文 献

1 Stallings W. Cryptography and network security: principles and practice. 北京:清华大学出版社,2002

2 卢开澄. 计算机密码学. 北京:清华大学出版社,2000

3 李肯立,李庆华,戴光明,等. 背包问题的一种自适应算法. 计算机研究与发展,2004;41(7):1292—1297

4 李文卿. 数论及其应用. 北京:北京大学出版社,2001

5 Dang P P, Chau P M. Image encryption for secure internet multimedia applications. IEEE Transactions on Consumer Electronics,2000;46(8):395—403

6 李昌刚,韩正之. 图像加密技术新进展. 信息与控制,2003;32(4):339—343

7 Blum M, Goldwasser S. An efficient probabilistic public-key encryption scheme which hides all partial information. In: Advances in Cryptology: Proceedings of CRYPTO84, Springer-Verlag,1985;289—299

Digital Image Encryption Algorithm Based on Knapsack Problem

CUI Yan, ZHANG Yong-hong¹

(School of Statistics, Xi'an University of Finance and Economics, Xi'an 710100, P. R. China;

Department of Mathematics, Weinan Teacher's College¹, Weinan 714000, P. R. China)

[Abstract] An image encryption algorithm is presented based on knapsack problem, and can encrypt image safely and quickly by using this algorithm. The experimental results indicate the algorithm has good encryption results.

[Key words] ultra-greater sequences knapsack problem image encryption