一种基于Arnold置乱和优化大素数选取方案的RSA数字图像加密算法

杨 洋 杨 洁 冯久超

(华南理工大学电子与信息学院 广州 510641)

摘 要 提出了一种优化大素数选取方案的RSA算法和Arnold置乱结合的数字图像加密算法,该算法包括图像置乱加密和RSA加密。在传统RSA算法的基础上,针对大素数选取方案的优化,提出了一种以时间的流逝作为seed的随机大素数选取方案,提高了加密的安全性。实验结果表明,该方法有较强的安全性,密文图像对加性噪声的攻击也有一定的鲁棒性。

关键词 RSA,Arnold,大素数选取方案,图像加密

中图法分类号 TN957.52 **文献标识码** A

Algorithm Based on Arnold and RSA for Optimal Selection of Large Prime Numbers in Image Encryption

YANG Yang YANG Jie FENG Jiu-chao

(School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510641, China)

Abstract An algorithm based on Arnold and RSA for optimal selection of large prime numbers in image encryption is proposed, including the Arnold transform and the RSA encryption algorithm. On the basis of the traditional RSA algorithm, this method proposed a scheme of the random selection of large prime numbers using the passage of time as the seed. Experimental results show that this method has high security, the decrypted image has a certain degree of robustness to additive noise attack.

Keywords RSA, Arnold, Selection of large prime numbers, Image encryption

近年来,随着科学技术的进步,信息安全问题越来越成为人们关注的焦点。人们不得不产生一种意识:信息的传送一定要安全,特别是秘密信息。基于这种意识,现代社会出现了很多关于信息安全的新发明,学术界也出现了很多关于信息安全的讨论和研究。其中图像加密就是一个不容忽视的领域。

在图像加密领域目前已经有多种方法[11,12],例如可以将图像数据当作普通的二进制数据来加密,其中对称加解密算法DES、AES等等就属于这类算法。又如像素置乱算法,最典型的是Arnold置乱算法[1-3]。它将图像的像素信息按照一定规律打乱,从而实现图像的加密。不过这种算法安全性很差,目前已经能够被轻易破解,除此之外还有针对数字图像的时域加密算法、频域加密算法等等。

本文提出一种将优化大素数选取方案的RSA非对称加解密算法[6]和Arnold置乱算法相结合的数字图像加解密算法,其将广泛应用于IC及Internet加密领域中的RSA非对称加解密算法和广泛应用于数字图像加密的Arnold置乱算法相结合,并在此基础上优化了RSA算法关键的大素数选取方案,使之安全性显著增强并具有很好的鲁棒性。

本文首先介绍Arnold置乱算法,然后介绍传统的RSA非对称加解密算法,接着对RSA算法进行优化,最后,将这两种算法结合起来应用于数字图像加解密中。

实验表明,RSA加密过的图像由于经过归一化之后可能丢失个别像素信息,故没有较好的图像信息熵。但是一次一密的特征使其加密效果优越,并能够无差别地恢复原始图像。在优化大素数选取方案和Arnold置乱算法结合之后加密安全性进一步加强。

1 Arnold置乱算法

1.1 算法概述

Arnold置乱算法又称为"猫脸"变换,是俄国数学家Vladimir I Arnold提出的一种算法。针对一幅$N\times N$的数字图像I,离散化的二维Arnold置乱定义如下[13]:

$$\begin{bmatrix}x'\\y'\end{bmatrix}=\begin{bmatrix}1&1\\1&2\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}(\mathrm{mod}\ N) \tag{1}$$

式中,x,y为原始图像的像素位置坐标,x',y'为经过置乱变换之后的像素位置坐标。即

$$x,y,x',y'\in\{0,1,2,\cdots,N-1\} \tag{2}$$

经过一次置乱变换之后,原始图像的像素点会根据新的像素坐标重新分布,从而形成杂乱无章的图像。但是随着迭代次数的增加,经过一定次数的置乱之后又会恢复到原始图像,因此该算法的安全性较差。其中,恢复周期因图像大小不

本文受国家自然科学基金(60872123),国家-广东省自然科学基金联合基金(U0835001)资助。

杨 洋(1991-),男,硕士,主要研究方向为信息安全、数字图像处理,E-mail:fighting_yang@foxmail.com;冯久超(1966-),男,教授,主要研究方向为非线性电路、混沌信号与信息处理,E-mail:fengjc@scut.edu.cn(通信作者)。

同而不同。

1.2 算法应用

例如对于图像大小为 128×128、256×256、512×512 的图像，恢复周期分别为 96、192、384。

对于一幅 256×256 的二维图像，运用 Arnold 置乱算法效果如图 1 所示。

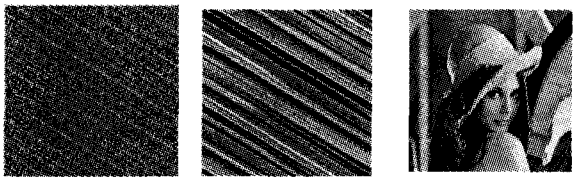


图 1　3 次、100 次、192 次置乱结果

可以看到，原始图像在经过 3 次、100 次置乱之后图像变得杂乱无章，初步达到了加密的效果。但是经过 192 次置乱之后恢复了原始图像。可见，只要获得了该图像的图像大小，就可以很轻易地通过迭代进行解密，故如果仅仅使用这种算法进行加密，安全性是很差的。

2 RSA 算法

2.1 算法概述

RSA 算法又称为 RSA 非对称算法，是区别于传统的对称算法的一种公钥加密算法。它是 1977 年由 Ron Rivest、Adi Shamirh 和 Len Adleman 开发的，它的核心思想是基于大数分解的困难性。

该算法之所以成为非对称算法，是因为在加密和解密的过程中所使用的密钥是不同的。加解密过程如图 2 所示。

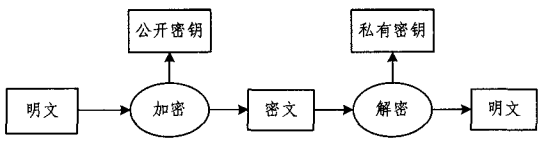


图 2　非对称加解密算法过程

从图 2 我们可以知道整个非对称加解密算法的过程。首先，我们将明文数据使用公开密钥进行加密，公开密钥也就是发送节点和接收节点都知晓的密钥。然后将加密后的数据通过信道传送给接收节点，然后接收节点用自己的私钥对密文进行解密得到明文数据。该私钥只有接收节点自己知晓。

2.2 算法实现

2.2.1 公钥与私钥的产生

- 随机选取两个大的素数 p 和 q，并且 $p \neq q$。
- 计算 $n=p\times q$。
- 计算 $f=(p-1)\times(q-1)$。
- 选择一个整数 e，使其与 f 互素 $a^2+b^2=c^2$，并且 $e<f$，得到公钥 e。
- 计算 $(d\times e)=1(\mathrm{mod}(f))$ 得到私钥 d。
- 将 p 和 q 的记录销毁。

这样，我们得到了两个密钥对：(n,e) 和 (n,d)。其中，密钥对 (n,e) 是公开密钥对，(n,d) 是私有密钥对。

2.2.2 加密过程

我们假设发送节点是 A，接收节点是 B，A 要发送消息 m 给 B，因为 A 已经知道 B 的公钥 e 和大数 n，所以 A 可以用该公开密钥对 (n,e) 对 m 进行加密。加密时，A 使用原先与 B 约定好的格式将明文 m 转化为一个小于 n 的整数，比如 n_1，又比如 A 也可以将明文里的每一个字转换成这个字的 Unicode 码，然后将这些数字连在一起组成一个数字。又假如 A 要发送的明文 m 非常长，那么它可以将信息分段，将每一段的 n 算出来，逐个加密后发送给接收节点 B。

加密公式如下：

$$m^e=c(\mathrm{mod}\ n) \tag{3}$$

式中，c 就是得到的密文。

2.2.3 解密过程

接收节点 B 在收到密文 m 后，就可以用自己的私钥 d 将密文解密。解密公式如下：

$$c^d=m'(\mathrm{mod}\ n) \tag{4}$$

解密完成后，$m'=m$。

3 优化大素数选取方案

3.1 想法提出

我们知道，两个大数相乘的运算很容易实现，但是将一个已知大数分解成两个数这样的逆运算却很难或者需要相当长的时间。即：

$p\times q\rightarrow n$(容易)

$n\rightarrow p\times q$(困难)

从前文对传统 RSA 算法的叙述可以知道，公钥私钥的产生都是依赖于两个大素数 p 和 q。也就是说，只要知道了 p 和 q，就可以破解密文。因此，随机数的选取问题就尤为关键了。

3.2 解决方案

针对这个问题，本文提出了一种“以时间的流逝作为 seed 产生随机数”的思想。

为什么产生随机数要用时间的流逝作为种子呢？这是因为所谓的随机数，例如使用 random 函数产生随机数，其实并不能完全称作随机，理论上它的产生是有规律的。比如 srand(1)到 srand(1000)里面有 1000 个种子，也就是说有 1000 种选择，所以称为“随机”。但其实关键是种子的选择不是接近随机。

所以，我们将时间的流逝作为这个种子，因为时间的数值会随着时间的流逝而变化。也就是说，使用这个思想之后，用来产生随机数的函数连续运行两次，一般不会出现前一次和后一次产生的随机数相同的情况。这样一来，数字的产生就接近随机了，当然因此进行的 RSA 加解密的安全性也有了提高。利用 C 语言实现该思想，我们来看这个函数：

```
int random(a)
{
int d;
srand((unsigned)time(0) * a);
d=(rand()%(200-100))+100;
return d;
}
```

该函数旨在产生一个 100 到 200 之间的随机数。在 srand 函数里面有个因子 a，通过设置不同的值，时间数值将会发生不同快慢的变化，可以将 a 设置得大一些以保证产生理想的随机数。

4 Arnold 置乱及优化的 RSA 算法在数字图像加解密的结合使用

4.1 实现过程

为了提升加密的安全性，本文将 Arnold 置乱和优化的 RSA 算法进行结合，思路如图 3 所示。

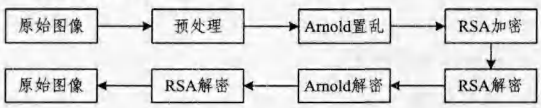


图 3 Arnold 置乱与 RSA 算法相结合

将 Arnold 置乱和 RSA 应用到数字图像加密方案中，流程如图 3 所示。步骤为：

4.1.1 Arnold 置乱

对于一幅 $N\times N$ 的 256 级灰度图像 I，先设定 Arnold 置乱轮数，并进行 Arnold 置乱。置乱后的图像像素点坐标(x', y')为：

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\ N) \tag{5}$$

式中，只要 $a_1a_4 - a_2a_3 = 1$，在 mod N 的意义下，它对平面的坐标变换就可以视为置乱，且易于计算逆矩阵用以还原置乱。

4.1.2 RSA 加密

将置乱后的图像利用已知公钥进行优化的 RSA 加密。

4.1.3 RSA 解密

将经过 RSA 加密后的图像利用私钥进行 RSA 解密。

4.1.4 Arnold 解密

将经过 RSA 解密后的图像进行 Arnold 反置乱，得到原始图像。

4.2 算法分析

我们知道 RSA 算法的优势在于密钥管理的便捷性，发送方只需知道双方的公开密钥即可对数据进行加密，而接受方在接收到加密数据后使用自己的私有密钥可以很方便地对数据解密。本文提出的将 Arnold 置乱算法和经过优化的大素数选取方案的 RSA 算法相结合的方案，更进一步提升了加解密的安全性。加密后的图像有理想的统计直方图和较低的熵，并能无差别恢复原始图像。

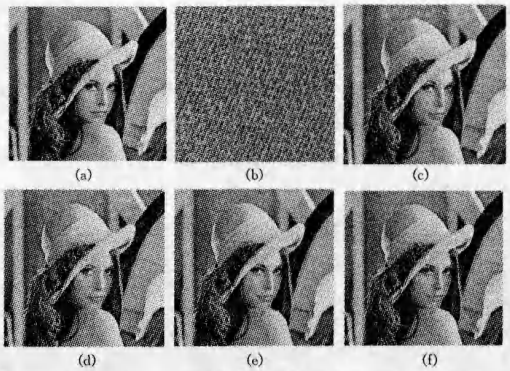
4.3 抗干扰分析

为了获得该算法在数字图像加密上的抗干扰性能，我们分别在原始图像和经过 Arnold 置乱后的图像上进行高斯噪声攻击。我们在 MATLAB7.0 环境下使用 Lena 图像，对该图像加密方法进行分析，所使用图像灰度级别为 256，大小是 256×256。

首先，我们在经过了 20 次 Arnold 置乱后的图像上加上均值为 0、方差为 0.001 的高斯噪声(如图 4(b)所示)，解密后的图像如图 4(c)所示。

然后，我们在原始 lena 图像上加上均值为 0、方差为 0.001的高斯噪声(如图 4(d)所示)，解密后的图像如图 4(e)所示。

最后，我们在原始 lena 图像和经过 20 次 Arnold 置乱之后的图像上同时加上均值为 0、方差为 0.001 的高斯噪声，解密后的图像如图 4(f)所示。



(a) 原始图像；(b) 在 0.001 高斯噪声攻击下的 Arnold 置乱图像；(c) Arnold 置乱图像在 0.001 高斯噪声攻击下的解密图像；(d) 在 0.001 高斯噪声攻击下的原始图像；(e) 原始图像在 0.001 高斯噪声攻击下的解密图像；(f) 原始图像和 Arnold 置乱图像均在 0.001 高斯噪声攻击下的解密图像

图 4 加性噪声干扰后的密文图像及解密图像

结束语 针对 RSA 算法密钥管理的便捷性和信息安全领域里数字图像加密的特点，本文结合了 RSA 算法和基于像素点坐标变换的 Arnold 置乱的思想，并在此基础上优化了传统 RSA 算法的随机大素数的选取方案，巧妙地应用于数字图像加密。实验结果表明，在加性高斯噪声攻击下，通过该加密方法能较好地恢复原始图像。本文从理论上证实了思想的可行性，从实验结果证明了算法的安全性和鲁棒性。

参 考 文 献

[1] 丁玮，闫伟齐，齐东旭. 基于 Arnold 变换的数字图像置乱技术[J]. 计算机辅助设计与图形学学报，2001，13(4)：338-341

[2] 邹建成，铁小匀. 数字图像的二维 Arnold 变换及周期性[J]. 北方工业大学学报，2000，12(1)：10-14

[3] 马丁. 一种改进 Arnold 变换的数字图像加密算法[C]//第五届图像图形技术与应用学术会议. 2010：209-213

[4] 李云飞，柳青，郝林，等. 一种有效的 RSA 算法改进方案[J]. 计算机应用，2010，30(9)：2393-2397

[5] 曹建国，王丹，王威. 基于 RSA 公钥密码安全性的研究[J]. 计算机技术与发展，2007，17(1)：172-176

[6] 王茜，倪建伟. 一种基于 RSA 的加密算法[J]. 重庆大学学报，2005，28(1)：68-72

[7] 陈诚，周玉洁. RSA 加密算法及其安全性研究[J]. 信息技术，2005，23(10)：98-100

[8] 任远芳，刘志杰，高玉明，等. 浅析 RSA 加密算法[J]. 电脑知识与技术，2013，9(9)：2062-2064

[9] 任洪娥，尚振伟，张健. 一种基于 Arnold 变换的数字图像加密算法[J]. 光学技术，2009，35(3)：384-390

[10] 张云鹏，左飞，翟正军. 基于混沌的数字图像加密综述[J]. 计算机工程与设计，2011，32(2)：463-466

[11] 李兴华，高飞. 一种基于混沌序列的数字图像加密算法[J]. 电讯技术，2006：99-104

[12] 文昌辞，王沁，苗晓宁，等. 数字图像加密综述[J]. 计算机科学，2012，39(12)：6-9

[13] 徐光宪，吴巍. 基于为随机序列的 Arnold 加密算法[J]. 计算机科学，2012，39(12)：79-82