DOI:10.13718/j.cnki.xsxb.2017.02.028

# 基于可逆矩阵加密技术的保密通信数学模型①

张新文[1], 王 佳[2]

1. 广州商学院 思想政治理论课教学部 数学教研室, 广州 511363;
2. 广州大学华软软件学院 基础部 数学教研室, 广州 510990

**摘要**: 矩阵是线性代数中的一个重要组成部分, 可逆矩阵在矩阵理论与应用中都占有很重要的地位. 主要探讨可逆矩阵在保密通信中的应用, 首次建立了可逆矩阵在保密通信中加密技术的数学模型, 并给出了可逆矩阵对字符以及对图片进行加密与解密的应用实例.

**关 键 词**: 可逆矩阵; 保密通信; 加密与解密; 数学模型; 应用实例
**中图分类号**: TN918.4; O151.21 **文献标志码**: A **文章编号**: 1000-5471(2017)02-0166-05

保密通信是当今信息时代一个极其重要的课题, 无数科技工作者为此做了大量工作[1-7]. 随着科学技术的发展, 特别是互联网的迅速发展, 以及计算机、智能手机等网络工具的广泛使用, 信息安全问题日益突出, 对信息传输过程中的安全性和可靠性的要求更高, 而保密通信作为实现信息安全的有效手段, 在其中起着至关重要的作用. 采用密码技术将明文加密传递, 一直是保密通信的一种重要手段, 尤其是在军事、商业、外交等通信领域. 对于破译者而言, 在不知道密钥的情况下, 即使截获到了密文也不能获取通信信息的真实内容. 矩阵作为线性代数重要的组成部分, 是一种强而有力的数学工具, 在保密通信中发挥着重要作用[8-11]. 本文首次利用可逆矩阵加密技术建立了一种保密通信数学模型, 并给出了它的一些实际应用.

## 1 保密通信模型

保密通信过程中, 存在明文和密文两个概念. 要发送的信息称为明文, 通过某种方法进行伪装或隐藏的信息称为密文. 通信过程中, 发送方会通过某种算法对明文代码进行加密, 通过加密后转换成密文代码发送给接收方, 接收方再通过相应的某种算法, 对密文代码进行解密转换, 还原为明文代码, 这个过程就是加密与解密的过程, 其中的某种算法就是密钥. 基于加密技术的保密通信模型[10]如图 1 所示.

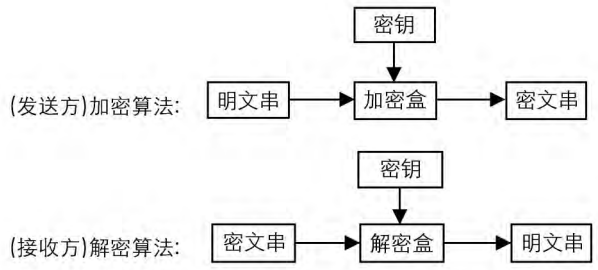


图 1 基于加密技术的保密通信模型

## 2 可逆矩阵在保密通信中的应用

利用可逆矩阵对通信信息进行编码, 即将明文转换成密文发送给接收方, 而接收方再通过相应的逆运

① 收稿日期: 2016-03-25
作者简介: 张新文(1982-), 男, 江西鄱阳人, 讲师, 硕士, 主要从事应用数学的研究.

算将密文编译成明文，就完成了重要信息的传递.

### 2.1　可逆矩阵在保密通信中加密技术的数学模型

设 $A$ 为 $n$ 阶可逆矩阵，则：

(i) 加密算法：$AY = X$；

(ii) 解密算法：$A^{-1}X = Y$.

其中 $A$ 为加密矩阵，$Y$ 为明文矩阵，$X$ 为密文矩阵，$A^{-1}$ 为解密矩阵. 加密时，发送方通过加密矩阵 $A$ 左(或右)乘明文矩阵 $Y$，将明文转换成密文 $X$；解密时，接收方则通过解密矩阵 $A^{-1}$ 左(或右)乘密文矩阵 $X$，将密文还原为明文.

由于可逆矩阵加密和解密时都用到了矩阵乘法，而矩阵乘法必须满足：左边矩阵的列数等于右边矩阵的行数，因此模型中加密矩阵 $A$ 的阶数必须等于明文矩阵 $Y$ 的行数.

### 2.2　基于可逆矩阵加密技术保密通信数学模型的应用实例

**例 1**　在某次战争中，假设总指挥部要给前线部队发送信息 FIRING，但需加密后才能发出. 双方约定用可逆矩阵

$$\boldsymbol{A} = \begin{pmatrix} 1 & -1 & 1 \\ 1 & 1 & -1 \\ -1 & 1 & 1 \end{pmatrix}$$

作为加密矩阵，且字母与数字一一对应如表 1 所示：

**表 1　字母与数字的对应**

| 字母 | $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ | $J$ | $K$ | $L$ | $M$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 对应数字 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 字母 | $N$ | $O$ | $P$ | $Q$ | $R$ | $S$ | $T$ | $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ |
| 对应数字 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

试写出总指挥部发出的密文代码，并给出前线部队收到密文后如何解密.

首先总指挥部把要发送的字母信息 FIRING 转化为明文代码 6,9,18,9,14,7. 其次根据加密矩阵的阶数把明文代码截取成明文矩阵

$$\boldsymbol{Y} = \begin{pmatrix} 6 & 9 \\ 9 & 14 \\ 18 & 7 \end{pmatrix}$$

然后通过 $AY = X$ 将明文矩阵 $Y$ 转换为密文矩阵 $X$：

$$\boldsymbol{AY} = \begin{pmatrix} 1 & -1 & 1 \\ 1 & 1 & -1 \\ -1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 6 & 9 \\ 9 & 14 \\ 18 & 7 \end{pmatrix} = \begin{pmatrix} 15 & 2 \\ -3 & 16 \\ 21 & 12 \end{pmatrix} = \boldsymbol{X}$$

最后将密文矩阵 $X$ 转换成密文代码 15，−3,21,2,16,12 发出.

前线部队收到密文后可以用解密矩阵 $A^{-1}$ 采用对应的算法进行解密得明文矩阵 $Y$：

$$\boldsymbol{A}^{-1}\boldsymbol{X} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 15 & 2 \\ -3 & 16 \\ 21 & 12 \end{pmatrix} = \begin{pmatrix} 6 & 9 \\ 9 & 14 \\ 18 & 7 \end{pmatrix} = \boldsymbol{Y}$$

再将明文矩阵 $Y$ 转换成明文代码 6,9,18,9,14,7. 对照字母表，前线部队就可以得到总部发来的信息 FIRING.

**例 2**　在商业交往中，甲乙两家公司关系非常密切，常常会相互传送商业机密. 两公司事先约定用可逆矩阵

$$\boldsymbol{A}=\begin{pmatrix}1&-1&1\\1&1&-1\\-1&1&1\end{pmatrix}$$

作为加密矩阵. 现假设甲公司收到来自乙公司的密文 F＞iBPL，请译出原信息. 其中 F＞iBPL 对应的 ASCII 代码值分别为 70,62,108,66,80,76.

首先甲公司通过 ASCII 表把 ASCII 码的密文 F＞iBPL 转换为密文数字代码 70,62,108,66,80,76. 其次由解密矩阵的阶数把密文代码截取成 3 行的密文矩阵

$$\boldsymbol{X}=\begin{pmatrix}70&66\\62&80\\108&76\end{pmatrix}$$

然后甲公司通过 $\boldsymbol{A}^{-1}\boldsymbol{X}=\boldsymbol{Y}$ 将密文矩阵 $\boldsymbol{X}$ 解密转换成明文矩阵 $\boldsymbol{Y}$：

$$\boldsymbol{A}^{-1}\boldsymbol{X}=\begin{pmatrix}\frac{1}{2}&\frac{1}{2}&0\\0&\frac{1}{2}&\frac{1}{2}\\\frac{1}{2}&0&\frac{1}{2}\end{pmatrix}\begin{pmatrix}70&66\\62&80\\108&76\end{pmatrix}=\begin{pmatrix}66&73\\85&78\\89&71\end{pmatrix}=\boldsymbol{Y}$$

最后将明文矩阵 $\boldsymbol{Y}$ 转换成明文代码 66,85,89,73,78,71，对照 ASCII 表，乙公司就可以得到甲公司发来的信息是 BUYING.

这里给出了可逆矩阵对字符进行加密与解密的应用实例. 要注意的是，在实际加密与解密过程中有时会遇到明文代码截取矩阵不满的情况，此时只需要将矩阵空缺的位置补充无意义代码即可. 另外，在实际应用中，密钥矩阵的阶数会非常大，而且十分复杂，一般可以在 MATLAB 中通过相应的程序指令：

```
n = 任意正整数;
A = rand(n, n);
s = zeros(n, 1);
for i = 1 : n
for j = 1 : n
s(i) = s(i) + A(i, j);
end
end
for i = 1 : n
for j = 1 : n
A(i, j) = A(i, j)/s(i);
end
end
det(A)
```

来构造得到，而且还可以根据要加密的信息容量的大小，选择加密矩阵的阶数.

下面给出可逆矩阵在 MATLAB 中对图片进行加密与解密的应用实例：

**例 3** 假设某高层领导人甲有一张机密的黑白图片文件资料：secret 文件.jpg（假定在甲电脑 D 盘中），要发送给另一个高层领导人乙，为防止外交通信过程中文件信息被第三方截获，发送方甲必须对图片进行加密后才能发出. 事先双方约定好了加密矩阵，接收方乙收到密文(假定存放在乙的电脑 E 盘中)后可用相应的逆矩阵在 MATLAB 中解密得到原图片.

发送方甲在 MATLAB 中对图片加密操作如下：首先甲通过 Y=imread('D:\secret 文件.jpg')程序读取 D 盘中的图片，得到明文矩阵，记为 $\boldsymbol{Y}$；再通过 imshow(Y)在 MATLAB 中显示明文图片，截图见图 2. 然后通过 $\boldsymbol{A}$=xlsread('D:\加密矩阵.xls')程序读取 D 盘中的加密矩阵 $\boldsymbol{A}$；由于得到明文矩阵 $\boldsymbol{Y}$ 里面的数

型是 unit8 无符号的整型数，而 $A$ 里面的数型是 double 实型数，两者不能进行运算，所以先通过 $Y1=$ im2double(Y)程序把 $Y$ 的数型转换成 double 实型数的明文矩阵 $Y1$，接着通过 $X=A*Y1$ 程序把明文矩阵 $Y1$ 加密为密文矩阵 $X$，再通过 imshow(X)显示密文图片，截图见图 3.

图 2　加密前的明文图片

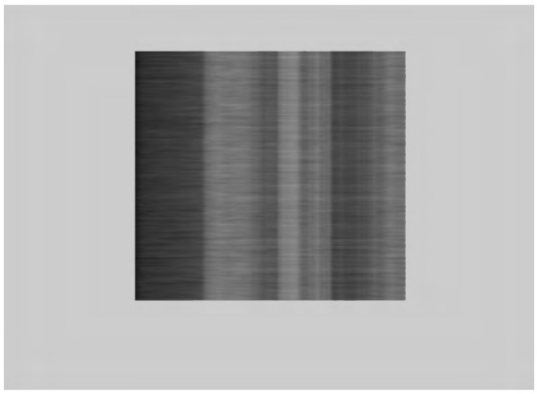

图 3　加密后的密文图片

甲加密成功后，通过 xlswrite('D：\密文矩阵. xls'，X)程序把密文矩阵写到 D 盘，最后把密文矩阵 $X$ 发送给接收方乙. 此时，假如密文被第三方截获，在不知晓解密矩阵的情况下，是不可能获取原图片信息的，甚至连密文 X 是什么都不能轻易地辨别出来.

接收方乙收到密文矩阵 $X$ 后，首先通过 $X=$xlsread('E：\密文矩阵. xls')程序读取 E 盘中的密文矩阵 $X$，然后通过 $A=$xlsread('E：\加密矩阵. xls')程序读取 E 盘中的加密矩阵 $A$，接着通过 $Y=$inv(A)$*$X 程序把密文矩阵 $X$ 还原为明文矩阵 $Y$，最后通过 imshow(Y)程序显示明文矩阵 $Y$，得到明文图片资料信息，乙解密成功. 截图见图 4.

图 4　解密后的明文图片

由于任意一个可逆矩阵，只有唯一的一个可逆矩阵与其互为逆矩阵，所以在可逆矩阵作为加密密钥矩阵未知的情况下，求得解密密钥矩阵的概率几乎为 0. 该加密算法还可以利用密钥矩阵空间无穷大的特性，在不同的通信中对密钥矩阵进行更换或者用多个密钥矩阵进行多层加密，以确保通信数据信息的安全.

## 3　结　　语

本文基于可逆矩阵加密技术保密通信的数学模型，利用可逆矩阵对字符以及对图片进行了加密与解密，这是信息编码算法的一种非常实用的技巧. 相信随着科学技术的不断发展与进步，包括可逆矩阵在内的许多数学工具将发挥越来越大的作用.

**参考文献：**

[1]　颜森林，迟泽英，陈文建. 激光混沌同步及其在光纤保密通信中的应用 [J]. 中国科学，2004，34(4)：467－480.

[2] 李文林，沈志萍，陈秀琴. 统一混沌系统同步及在保密通信中的应用[J]. 信息与控制，2008，37(6)：757－761.
[3] 梅 蓉，吴庆宪，陈 谋，等. 时滞Lorenz混沌系统的同步电路实现及在保密通信中的应用[J]. 应用基础与工程科学学报，2011，19(5)：830－841.
[4] 刘玉金，张胜海，杨 华，等. 光反馈垂直腔面发射半导体激光器的混沌驱动同步在保密通信中的应用[J]. 中国激光，2012，39(9)：88－94.
[5] 刘乐柱，张季谦，许贵霞，等. 一种基于混沌系统部分序列参数辨识的混沌保密通信方法[J]. 物理学报，2013，63(1)：24－29.
[6] 李震波，唐驾时. 参数扰动下的混沌同步控制及其保密通信方案[J]. 控制理论与应用，2014，31(5)：592－600.
[7] 朱艳平. 基于CNN超混沌的视频加密新算法[J]. 西南师范大学学报(自然科学版)，2016，41(9)：113－119.
[8] 徐景实，谭 利. 矩阵加密与解密的一些方法[J]. 长沙电力学院学报(自然科学版)，2003，18(1)：1－3.
[9] 龙新科. 图像的矩阵加密解析[J]. 岳阳职业技术学院学报，2006，21(4)：65－67.
[10] 熊小兵. 可逆矩阵在保密通信中的应用[J]. 大学数学，2007，23(3)：108－112.
[11] 单侠芹，潘 洋，赵 华，等. 基于贪心算法构成的正交矩阵及保密通信[J]. 电子设计工程，2011，19(6)：95－97.

# On Mathematical Model of Secure Communication Based on Inverse Matrix Encryption Technique

ZHANG Xin-wen[1], WANG Jia[2]

1. *Mathematics Teaching and Research Section, Department of Ideological and Political Theroy, Guangzhou College of Commerce, Guangzhou 511363, China;*
2. *Mathematics Teaching and Research Section, Basic Department, South China Institute of Software Engineering of Guangzhou University, Guangzhou 510990, China*

**Abstract**: Matrix is one of the important parts of linear algebra, and the reversible matrix is a very important role in the theory and application of it. In this paper, the application of the reversible matrix in the secure communication has been discussed, the mathematical model of the encryption technology of the reversible matrix in secure communication established for the first time, and application examples of the reversible matrix to the character and the image encryption and decryption been given.

**Key words**: reversible matrix; secure communication; encryption and decryption; mathematical model; application examples

责任编辑 廖 坤