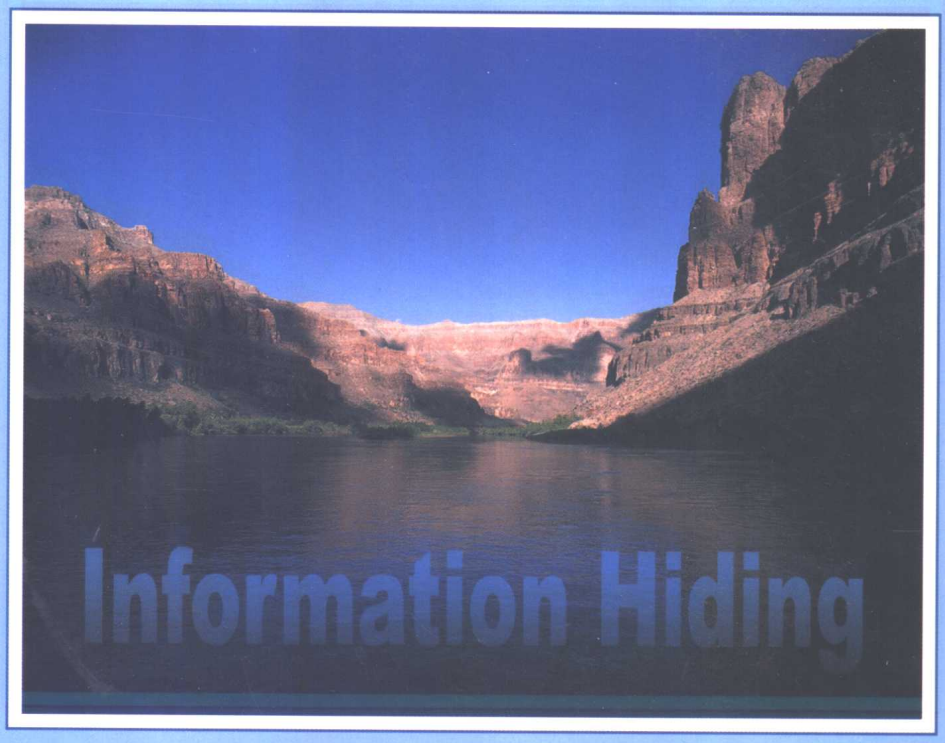
信息安全的新领域

信息隐藏

全国学术研讨会(CIHW2000/2001)论文集

北京电子技术应用研究所 主编



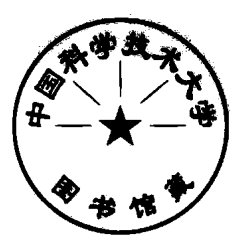
西电出版社
西安电子科技大学出版社
http://www.xduph.com

信息隐藏全国学术研讨会

(CIHW2000/2001)

论　文　集

北京电子技术应用研究所　主编



西安电子科技大学出版社

内 容 简 介

信息隐藏作为信息安全技术中的一个新领域，已经吸引了众多的科研人员。我国的信息隐藏学术研讨会（China Information Hiding Workshop）始于 1999 年，至今已成功举行了三届。

本书收录了国内第三届研讨会的学术论文 26 篇，第二届研讨会的学术论文 23 篇，较为全面地介绍了信息隐藏的基本概念与原理、隐藏通信与检测、版权保护与攻击等领域的最新理论探讨与实践。

本书作为国内第一部信息隐藏领域的专著，内容全面、新颖、实用，可作为信息安全学科的教学及科研之参考用书。

信息隐藏全国学术研讨会（CIHW2000/2001）论文集

北京电子技术应用研究所　主编

责任编辑　夏大平

出版发行　西安电子科技大学出版社（西安市太白南路 2 号）

电　　话　（029）8227828　　邮　编　710071

http://www.xdup.com　　E-mail: xdupfxb@pub.xaonline.com

经　　销　西安文化彩印厂

版　　次　2001 年 9 月第 1 版　　2001 年 9 月第 1 次印刷

开　　本　787 毫米×1092 毫米　　1/16　　印张 23.25

字　　数　552 千字

印　　数　1～300 册

定　　价　200.00 元

ISBN 7-5606-0432-3 / TN・0186

前　言

随着计算机、网络和通信技术的飞速发展，信息安全显得越来越重要，而信息隐藏技术作为信息安全技术的一个新的研究领域，已经吸引了众多的科学研究人员。在信息时代，信息隐藏技术的两个最大的应用领域是：版权保护和隐蔽通信。

国外的信息隐藏学术研讨会开始于 1996 年，至今已经举行了四届国际信息隐藏学术研讨会（International Information Hiding Workshop），第一届在英国的剑桥（Cambridge，IHW1996），第二届在美国的波特兰（Portland，IHW1998），第三届在德国的德雷斯顿（Dresden，IHW1999），第四届在美国的皮茨堡（Pittsburgh，IHW2001）。

我国的信息隐藏学术研讨会是由我国信息科学领域的何德全、周仲义、蔡吉人三位院士与有关研究单位联合发起的。1999 年，在北京电子技术应用研究所举行了第一次学术会议，参加会议的有何德全院士、周仲义院士、蔡吉人院士，还有来自北方工业大学、北京电子技术应用研究所、北京邮电大学、清华大学、中国科技大学、中国科学院计算技术研究所、中国科学院自动化研究所等高等院校或科研机构的专家*，其中有戴一奇教授、冯正和教授、林代茂研究员、吕述望教授、齐东旭教授、谭铁牛研究员、徐光佑教授、杨义先教授、尤新刚研究员等。2000 年 1 月，863 计划智能计算机系统专家组在北京主持召开了“数字水印技术研讨会”。2000 年 6 月，全国第二届信息隐藏学术研讨会（CIHW2000）在北京举行，参加研讨会的学者来自全国各地从事信息隐藏研究的二十四个高等院校或科研机构。周仲义院士、蔡吉人院士全程出席了全国第二届信息隐藏学术研讨会，何德全院士在百忙之中致电关心研讨会的召开。

2001 年，全国第三届信息隐藏学术研讨会（CIHW2001）在古城西安举行。为了进一步促进我国信息隐藏学术研究水平的提高，本届研讨会编辑出版了信息隐藏学术论文集。在此，特别感谢李荣才教授（总编辑）、王育民教授为西安电子科技大学出版社出版本论文集所做的努力。

本论文集收录了第三届研讨会的学术论文 26 篇、第二届研讨会的学术论文 23 篇。

到目前为止，参加信息隐藏学术研讨会的学者来自北方工业大学、北方交通大学、北京大学、北京电子技术应用研究所、北京工业大学、北京科技大学、北京理工大学、北京邮电大学、重庆大学、重庆通信学院、大连理工大学、复旦大学、国防科技大学、国家自然科学基金委员会、哈尔滨工业大学、河北工业大学、吉林大学、解放军理工大学、计算机世界报、南京理工大学、清华大学、汕头大学、上海大学、上海交通大学、深圳大学、四川大学、天津大学、西安电子科技大学、西安理工大学、云南大学、浙江大学、郑州信息工程大学、中国科技大学、中国科学院计算技术研究所、中国科学院自动化研究所、中

---

* 本前言中的单位及姓名以汉语拼音字母为序，本论文集的论文以所在单位汉语拼音字母为序。

国矿业大学、中国信息安全测评认证中心、中山大学、装备指挥技术学院等单位。

第三届信息隐藏学术研讨会得到了北京电子技术应用研究所、西安电子科技大学等单位的大力支持，北京电子技术应用研究所、西安电子科技大学出版社的有关人员为本论文集的编辑出版付出了辛勤的劳动，本人在此一并表示感谢。

特别感谢来国柱教授以及中国电子学会通信学分会对我国信息隐藏学术工作的理解和支持。

全国信息隐藏学术研讨会纳入中国电子学会通信学分会的学术活动范畴，将会更好地汇集信息隐藏研究与应用领域的各界人士，以学术研讨会的组织形式开展学术活动。本人作为全国信息隐藏学术研讨会最早的倡导者之一，愿意继续为全国信息隐藏学术研讨会尽微薄之力。

最后，衷心感谢何德全院士、周仲义院士、蔡吉人院士对我国信息隐藏学术研讨会的关心和支持。感谢国家重点基础研究发展规划项目(课题编号：G1999035805) 对本论文集的支持。

尤新刚

2001 年 9 月于北京　昆明湖畔

目　录

全国第三届信息隐藏学术研讨会（2001 年）论文

全国第二届信息隐藏学术研讨会（2000 年）论文

正交拉丁变换的周期性及其在数字图像置乱中的应用

李国富

（北方工业大学基础学院，北京，100041）

【摘　要】 本文以图像信息安全问题为背景，介绍了正交拉丁方用于图像置乱的理论基础，以及变换的周期性，并给出了进行具体运算的方法和实验结果。

【关键词】 典信息安全，拉丁方，正交拉丁方，数字图像置乱，周期性

随着计算机技术、通信技术、信息处理技术和智能化网络技术的飞速发展和广泛应用，人们处理信息的方式日趋多元化，从早期的语言传递信息，到出现文字，再到活字印刷，以致发展到今天的智能化网络传递信息，人们之间的距离逐步拉近，以致出现了“地球村”的概念。然而，相应的问题也显示出来，由于大量的信息(包括公共的、个人的、军事的、商业的等)在网上传播，使得信息的有效性、安全性倍受关注，在信息安全中，往日因存储量大而让人望而却步的数字图像也由于存储设备容量的增大及成本的降低而成为了人们关注的热点。

对于图像信息的安全性，传统的保密学尚缺少足够的研究，这主要是由于经典的密码学主要对一维数据流提供了较好的算法，而对数字图像却忽视了其固有的一些特殊性质，如二维的自相似性、相关性、大数据量等。随着计算机技术的发展，人们在这方面做了许多有益的探索，并取得了很多有意义的成果。

针对数字图像的安全保密问题，信息隐藏与伪装技术是其主要手段，其中包括如下几个重要课题：(1) 数字图像的置乱技术；(2) 数字图像的分存技术；(3) 数字图像的隐藏技术；(4) 数字图像的水印技术。

数字图像的置乱技术主要用于数字图像的预处理和后处理，在这方面也有许多有效的方法，如基于 Arnold 变换、幻方、Hilbert 曲线、Conway 游戏、Tangram 算法、IFS 模型、Gray 码变换、广义 Gray 码变换、仿射模变换[1~7,9,10]等方法。本文则提出了一种新的数字图像变换方法，即基于正交拉丁方的数字图像变换方法，并给出了变换的周期及其在数字图像上的应用。

1 基本概念

定义 1 由元素 1，2，3，…，n 构成一个 $n\times n$ 的方阵 $(a_{ij})_{n\times n}$，使得每行、每列中各元素恰好只出现一次，这样的方阵叫做 n 阶拉丁方。

定义 2 设 $A=(a_{ij})_{n\times n}$，$B=(b_{ij})_{n\times n}$ 是两个 $n\times n$ 的拉丁方，若方阵 $((a_{ij},b_{ij}))_{n\times n}$ 中的 n^2 个偶对 (a_{ij},b_{ij}) 互不相同，$i,j=1,2,\cdots,n$，则称 A 与 B 为互相正交拉丁方，或称 A 与 B 为 n 阶正交拉丁方。如

$$A=\begin{bmatrix}1&2&3\\2&3&1\\3&1&2\end{bmatrix},\quad B=\begin{bmatrix}1&3&2\\2&1&3\\3&2&1\end{bmatrix}$$

则由 A、B 构成的 3×3 的偶对方阵

$$\begin{bmatrix}(1,1)&(2,3)&(3,2)\\(2,2)&(3,1)&(1,3)\\(3,3)&(1,2)&(2,1)\end{bmatrix}$$

中没有相同的元素，故 A 与 B 是三阶正交拉丁方。

定义 3 如果 M 是含有 n 个元素的有限集，集 M 的可逆变换就是 M 到自身的 1－1 变换，称作集 M 上的置换，记作

$$A=\begin{pmatrix}i_1&i_2&\cdots&i_n\\j_1&j_2&\cdots&j_n\end{pmatrix}$$

这里表示变换 A 将元素 i_k 变为 j_k。

定义 4 形如

$$A=\begin{pmatrix}i_1&i_2&\cdots&i_k&i_{k+1}&i_{k+2}&\cdots&i_n\\j_1&j_2&\cdots&i_1&i_{k+1}&i_{k+2}&\cdots&i_n\end{pmatrix}$$

的置换称为循环置换。

定义 5 A 是有限集 M 上的置换，若存在自然数 m，使得 $A^m=I$，其中 I 为单位变换，则称变换 A 有周期性，最小的 m 称为变换 A 的周期。

2 几个定理

定理 1[8] 互相正交的 n 阶拉丁方的个数不超过 $n-1$ 个。即若 $A_1,A_2\cdots\cdots A_k$ 是两两正交的 n 阶拉丁方，则 $k\leq n-1$。

定理 2[8] 设 $n \geq 3$，且 $n = p^{\alpha}$，p 为一个素数，a 是一个正整数，则存在 $n-1$ 个正交的 n 阶拉丁方 $A_1, A_2 \cdots \cdots A_{n-1}$。且若设

$$A_k = (a_{ij}^{(k)})_{n\times n} \qquad k = 1,2,\cdots,n-1$$

$$t_i = i \qquad i = 0,1,2\cdots,n-1$$

则 $$a_{ij}^{(k)} = t_k \cdot t_{i-1} + t_{j-1} \qquad i,j = 1,2,\cdots n;\ k = 1,2,\cdots,n-1$$

其中"+"和"·"是 GF（P^{α}）域的加法和乘法运算。

定理 3 若 $A_1, A_2 \cdots, A_m$ 为两两正交的拉丁方组，且设

$$A_k = (a_{ij}^{(k)}) \qquad i,j = 1,2\cdots n;\quad k = 1,2\cdots m$$

则方阵

$$((a_{ij}^{(l_1)}, a_{ij}^{(l_2)}, a_{ij}^{(l_3)}))_{n\times n} \qquad l_1 \neq l_2 \neq l_3, l_1, l_2, l_3 = 1,2,\cdots,m$$

中的元素互不相同。

定理 4 任一含有有限个元素的置换都可以分解为有限个互相没有共同元素的循环置换的乘积，且此种分解是唯一的。

定理 5 设 $A=A_1A_2\cdots A_k$，其中 A_1，A_2，…，A_k 为变换 A 分解的有限个互相没有共同元素的循环置换的乘积，且 A_1，A_2，…，A_k所含有的元素个数分别为 n_1，n_2，… n_k，则变换 A 的周期 m 为 n_1，n_2，…，n_k的最小公倍数。

3 正交拉丁变换的周期性

设 $A=(a_{ij})_{n\times n}$，$B=(b_{ij})_{n\times n}$为互相正交的拉丁方，定义变换 $f(i,j)\rightarrow(a_{ij}, b_{ij})$，$(i,j=1,2,\cdots,n)$，称为正交拉丁变换。显然变换 f 是 1–1 映射，故其构成一个含有 n^2 个元素的置换。由定理 4 及定理 5 知，对于給定的正交拉丁方 A 与 B 以及固定的 n，由定理 2 中的公式易算出变换 f 的周期。例如：

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

数字图像矩阵为

$$x = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \xrightarrow{f} \begin{bmatrix} a & f & h \\ e & g & c \\ i & b & d \end{bmatrix} \xrightarrow{f} \begin{bmatrix} a & c & b \\ g & i & h \\ d & f & e \end{bmatrix}$$

$$\xrightarrow{f} \begin{bmatrix} a & h & f \\ i & d & b \\ e & c & g \end{bmatrix} \xrightarrow{f} \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$

即在上述拉丁方 A, B 及 $n=3$ 时的周期为 4。

下面是利用计算机编程得到的部分结果。

表 1　不同阶数下的相同参数的正交拉丁方变换的周期

A_k	2	2	2	2	2	2	2	2	2	2	2
A_j	3	3	3	3	3	3	3	3	3	3	3
阶数	4	5	7	8	9	11	13	16	17	19	22
周期	6	12	16	12	6	8	52	24	16	40	24

表 2　不同阶数下的相同参数的正交拉丁方变换的周期

A_k	2	2	2	2	2	2	2	2	2	2	2
A_j	3	3	3	3	3	3	3	3	3	3	3
阶数	23	25	27	29	31	32	37	41	43	47	49
周期	22	60	18	28	64	48	76	28	42	96	112

表 3　相同阶数下的不同参数的正交拉丁方变换的周期

A_k	2	2	2	2	2	2	2	2	2	2	2
A_j	4	5	6	7	8	9	10	11	12	13	14
阶数	31	31	31	31	31	31	31	31	31	31	31
周期	320	480	10	192	30	960	30	30	30	120	480

表 4　相同阶数下的不同参数的正交拉丁方变换的周期

A_k	15	16	17	18	20	23	25	26	28	29	30
A_j	2	2	2	2	2	2	2	2	2	2	2
阶数	31	31	31	31	31	31	31	31	31	31	31
周期	480	960	30	320	30	930	15	480	30	80	30

表 5　不同阶数下的不同参数的正交拉丁方变换的周期

A_k	2	2	3	5	4	7	7	6	9	12	18
A_j	1	3	1	2	5	8	10	9	12	13	14
阶数	3	4	5	7	8	9	11	13	16	17	19
周期	4	6	24	48	12	24	120	12	16	12	36

表 6　不同阶数下的不同参数的正交拉丁方变换的周期

A_k	15	3	6	18	20	23	5	8	28	29	3
A_j	12	8	9	3	37	14	10	9	99	212	18
阶数	25	27	32	64	81	125	128	243	151	256	512
周期	20	54	24	96	108	500	128	54	75	256	342

4　在数字图像处理中的应用

数字图像可以看作一个矩阵，矩阵元素所在的行与列就是图像显示在计算机屏幕上的诸像素点的坐标，元素的数值就是像素点的灰度。数字图像的置乱有基于位置空间、色彩空间和频率空间的置乱变换。即改变像素的位置或色彩而置乱图像。但要恢复原始图像必须保证原始图像与变换图像之间的变换是 1－1 映射(双射)，而正交拉丁方正好具备该性质。具体方法是：

设数字图像的矩阵为

$$A=(a_{ij})_{n\times n}$$

其中，$n=p^{\alpha}$ (≥ 3, 且p为素数,α为整数)。由定理 2 知存在含有 $n-1$ 个拉丁方的互相正交的拉丁方组 $A_1, A_2, \cdots A_{n-1}$，在该组中任取两个互相正交的拉丁方设为：

$$A_i, A_j \quad 1 \leq i, j \leq n-1, \ i \neq j$$

构造矩阵

$$b = ((a_{ij}^{(i)}, a_{ij}^{(j)}))_{n\times n}$$

则 B 中的元素 $(a_{ij}^{(i)}, a_{ij}^{(j)})$ 遍历(1,1), (1,2), (1,3), $\cdots$ (1,n), (2,1), (2,2), $\cdots$(2,n), (n,1), (n,2), $\cdots$ (n,n)，因此，将 B 中的元素 $(a_{ij}^{(i)}, a_{ij}^{(j)})$ 看作数字图像 $a_{a_{ij}^{(i)}, a_{ij}^{(j)}}$ 的坐标，

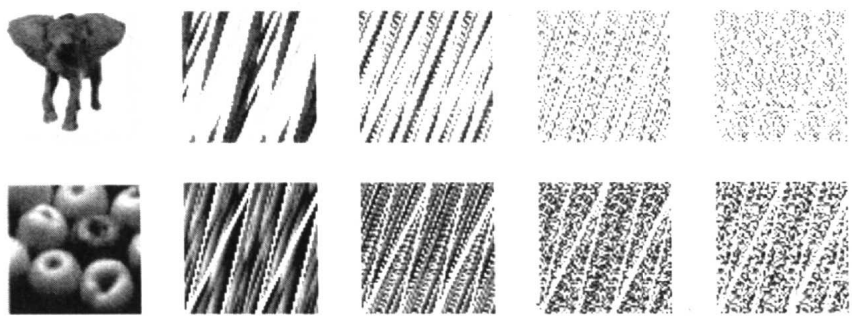
而将其灰度值 $A = (a_{ij})$ 放于(i,j)点，则得变换后的数字图像矩阵 $C = (a_{a_{ij}^{(i)}, a_{ij}^{(j)}})$

从而达到置乱图像的目的。

对于三维空间中的图像，由定理 3 知利用正交拉丁方同样能达到数字图像置乱的目的，在此不再赘述。

由于正交拉丁方组中含有 $n-1$ 个互相正交的拉丁方，故这种图像置乱方法有$(n-1)(n-2)$种，而对于三维图像则有$(n-1)(n-2)(n-3)$种。

下面是利用该法进行图像置乱变换的实例，所用拉丁方为定理 2 中 $k=2$ 和 $k=4$ 的结果。



原图　　变换一次图　　变换二次图　　变换三次图　　变换四次图

5 总结

数字图像信息处理是近年来新兴起来的研究课题，人们已作过许多有益的探索，得到了一些有趣的结果。本文提出的算法本质上是二维 Arnold 变换的推广，但由于其中含有两个参数，且这些方法可混合使用，因此增加了解密的难度。从上述实验结果来看，其用作图像的预处理或后处理还是非常有效的。另外，同 Arnold 变换类似，该算法的周期性问题也有待进一步探讨。

在完成此文的过程中，得到齐东旭教授的精心指导和鼓励，邹建成博士也提出许多宝贵意见，在此向他们表示衷心的感谢。

参 考 文 献

[1] 齐东旭. 分形及其计算机生成. 北京：科学出版社，1994

[2] 孙伟. 关于 Arnold 变换的周期性. 北方工业大学学报，1999，11（1）：29－32

[3] 丁玮，齐东旭，数字图像变换及信息隐藏与伪装技术.计算机学报，1998，21（9）：838－843

[4] 邹建成，铁小匀，数字图像的二维 Arnold 变换及其周期性. 北方工业大学学报，2000 年第 1 期，10－14

[5] Ding Wei, Yan Wei-Qi and Qi DongXu. Digital Image Scrambling Technology Based on Gray Code. Proc. Of International Conference on CAD/CG, 1999

[6] 李国富，邹建成，齐东旭. 广义 Gray 码及其在数字图像置乱中的应用. 全国第二届信息隐藏学术研讨会论文集，1－6，北京，2000，6

[7] Qi DongXu, Ding Wei and Li HuaShan. Tangram Algorithm: Image Transformation for Storing and Transmitting Visual Secrets. Proceedings of the 9'st International Conference of CAD/CG, Vol. 1, 1997, 135-139

[8] 杨振生. 组合数学及其算法. 合肥: 中国科技大学出版社，1997

[9] 李国富，宋瑞霞，赵慧. 椭圆曲线在数字图像隐藏中的作用. 北方工业大学学报，2000 年第 3 期，17－20

[10] 邹建成，唐旭晖，李国富. 数字图像的仿射模变换及其周期性. 北方工业大学学报，2000 年第 3 期，13－17

一种基于 Frobenius 问题的数字图像分存方法*

邹建成[1]　孙　伟[2]

[1]（北方工业大学基础学院，北京市石景山区，100041）

[2]（北方工业大学 CAD 研究中心，北京，100041）

【摘　要】 介绍了组合数学中的一次不定方程的 Frobenius 问题，给出了利用一次不定方程进行数字图像分存的数学理论基础、算法和应用例子。

【关键词】 Frobenius 问题，信息安全，计算机密码学，图像分存

1　引言

随着多媒体技术和国际互联网的飞速发展，大量国家、团体和个人信息在国际互联网和各种不同类型的局域网上传播，人们可以很方便地对信息进行编辑、修改和复制，甚至恶意者对信息进行破坏。信息安全问题显然是倍受关注和重视的问题[1~12]。而图像信息安全是其中特别重要的一个研究领域。目前人们对图像信息安全的研究主要集中在数字水印研究领域。数字图像分存技术是图像信息安全研究的一个重要课题，已有的方法主要是基于动直线的图像分存技术、基于 Lagrange 插值的分存技术和基于中国剩余定理的分存技术[10~12]。图像分存可以避免由于少数几分图像信息的丢失而造成严重的事故。其好处是个别图像信息的泄露不会引起整个图像信息的丢失。本文首先介绍一次不定方程的 Frobenius 问题，然后给出利用一次不定方程进行数字图像分存的数学理论基础、算法和应用例子。

2　组合数学中的 Frobenius 问题

对 s（≥2）个互素的正整数 a_1，a_2，…，a_s，是否存在一个仅与 a_1，a_2，…，a_s 有关的整数 $\phi(a_1, a_2, \cdots, a_s)$，使得对任何不小于 $\phi(a_1, a_2, \cdots, a_s)$ 的整数 x 都能够表示成 $a_1x_1 + a_2x_2 + \cdots + a_sx_s$，其中 $x_i \geq 0, i = 1, \cdots, s$，而 $\phi(a_1, a_2, \cdots, a_s) - 1$ 不能表示成 $a_1x_1 + a_2x_2 + \cdots + a_sx_s$，其中 $x_i \geq 0, i = 1, \cdots, s$。求 $\phi(a_1, a_2, \cdots, a_s)$ 的问题称为 Frobenius 问题。$\phi(a_1, a_2, \cdots, a_s)$ 称为 Frobenius 数。

*得到国家 973 项目、北京市自然科学基金、北京市科技新星计划项目资助。

Frobenius 问题是组合数学中一次不定方程研究中的重要问题，它与布尔方阵的幂序列的周期和幂敛指数的研究有关。在此我们不做过多阐述，只给出几个我们将要用到的结果。

定理 1（Schur）[13]：设 $s \geq 2$，如果 x 和 $a_i\ (i=1,\cdots,s)$ 都是正整数，且 $(a_1,\cdots,a_s)=1$，则存在仅与 a_1，a_2，…，a_s 有关的整数 $\phi(a_1, a_2, \cdots, a_s)$，使得下列方程：

$$a_1x_1 + a_2x_2 + \cdots + a_sx_s = x$$

有非负整数解 $x_i \geq 0, i = 1,\cdots,s$。

对 $s=3$ 的情形，Frobenius 问题已完全解决。对 $s \geq 3$，一般地只能找到 $\phi(a_1, a_2, \cdots, a_s)$ 的一些算法，求 $\phi(a_1, a_2, \cdots, a_s)$的一般表达式仍然是一个未解决的问题。下面是一些已知的结果。

定理 2 [13]：设 $(a_1,a_2)=1$，a_1，a_2 为正整数，则

$$\phi(a_1,a_2) = (a_1-1)(a_2-1)$$

定理 3（柯召 1955）[13]：设 $(a_1,a_2,a_3)=1$，a_1，a_2，a_3 为正整数，则

$$\phi(a_1,a_2,a_3) \leq \frac{a_1a_2}{(a_1,a_2)} + a_3(a_1,a_2)$$

定理 4（Vitek 1975）[13]：设 $a_1 > a_2 > \cdots > a_s$，$s \geq 3$，$(a_1,a_2,\cdots,a_s)=1$，则

$$\phi(a_1,a_2,\cdots a_s) \leq \left[\frac{1}{2}(a_{s-1}-1)(a_1-2)\right]$$

其中[x]表示不大于 x 的最大整数。

3 基于 Frobenius 问题的数字图像分存算法

我们知道图像像素的灰度值介于 0 ~ 255 之间。所以我们可以选取适当的两个、三个甚至多个互素的正整数，利用由 Frobenius 问题给出的算法，把图像的每个点的像素分解为两个、三个甚至多个分量，从而把一幅图像分存为两幅、三幅甚至多幅，达到隐蔽传输图像信息的目的。下面举例说明。

3.1 分存为两幅图像

取 $a_1=2$，$a_2=3$，则由定理 2 知 $\phi(2,3)=2$。也就是说，对任何大于或者等于 2 的

正整数x，都存在两个正整数x_1和x_2，使得$x=2x_1+3x_2$。例如$8=2\times4+3\times0$，或者$8=2\times1+3\times2$。事实上对于任意大于或等于2的x，我们有如下非常简单的算法：

(1) 如果$x\equiv0(\mathrm{mod}\,2)$，则可取$x_1=\dfrac{x}{2}$，$x_2=0$；

(2) 如果$x\equiv1(\mathrm{mod}\,2)$，则可取$x_1=\dfrac{x-1}{2}$，$x_2=1$。

当然可以预见按这种算法得到的两幅图像，一幅与原始图像相差无几，另外一幅则是黑白图像。所以在实际对图像进行分存时，我们不仅要利用以上算法的多种变体，还要对原始图像进行预处理和对分存得到的图像进行后处理。预处理和后处理可以利用数字图像的置乱变换，如Arnold变换和Gray码变换等。

3.2 分存为三幅图像

取$a_1=2$，$a_2=3$，$a_3=5$，则由定理2知$\phi(2,3,5)\le3$。也就是说对任何大于或者等于3的正整数x，都存在三个正整数x_1、x_2和x_3，使得$x=2x_1+3x_2+5x_3$。例如：

$17=2\times1+3\times0+5\times3$，$17=2\times2+3\times1+5\times2$，$17=2\times3+3\times2+5\times1$
$17=2\times0+3\times4+5\times1$，$17=2\times3+3\times2+5\times1$，$17=2\times6+3\times0+5\times1$
$17=2\times1+3\times5+5\times0$，$17=2\times4+3\times3+5\times0$，$17=2\times7+3\times1+5\times0$

与分存为两幅图像类似，我们可以把图像的每个像素的灰度值分解为三个分量，从而把一幅图像分存为三幅图像。事实上对于任意大于或等于3的x，我们有如下非常简单的算法：

(1) 如果$x\equiv0(\mathrm{mod}\,5)$，则可取$x_1=0$，$x_2=0$；$x_3=\dfrac{x}{5}$；

(2) 如果$x\equiv1(\mathrm{mod}5)$，则可取$x_1=0$，$x_2=2$，$x_3=\dfrac{x-1}{5}-1$；

(3) 如果$x\equiv2(\mathrm{mod}5)$，则可取$x=1$，$x_2=0$，$x_3=\dfrac{x-2}{5}$；

(4) 如果$x\equiv3(\mathrm{mod}5)$，则可取$x_1=0$，$x_2=1$，$x_3=\dfrac{x-3}{5}$；

(5) 如果$x\equiv4(\mathrm{mod}5)$，则可取$x_1=2$，$x_2=0$，$x_3=\dfrac{x-4}{5}$。

具体分存时我们不仅要利用以上算法的多种变体，还要对原始图像进行预处理和对分存得到的图像进行后处理。例如可以结合数字图像置乱技术中的Arnold变换、Gray玛变换、仿射模变换等。还可以利用数字图像的信息隐藏技术，使分存的几个图像都有意义，从而使分存的信息更加保密。