



[12] 发明专利说明书

专利号 ZL 200610002041.X

[45] 授权公告日 2009 年 9 月 30 日

[11] 授权公告号 CN 100546239C

[22] 申请日 2006.1.24

[21] 申请号 200610002041.X

[73] 专利权人 马恒利

地址 100034 北京市西城区厂桥爱民里小区 6 号楼 10 门 201

[72] 发明人 马恒利

[56] 参考文献

CN 1547157A 2004.11.17

US 6683956B1 2004.1.27

US 6473516B1 2002.10.29

CN 1617584A 2005.5.18

US 4972481 1990.11.20

US 6745940B1 2004.6.8

US 6909783B2 2005.6.21

审查员 成 谦

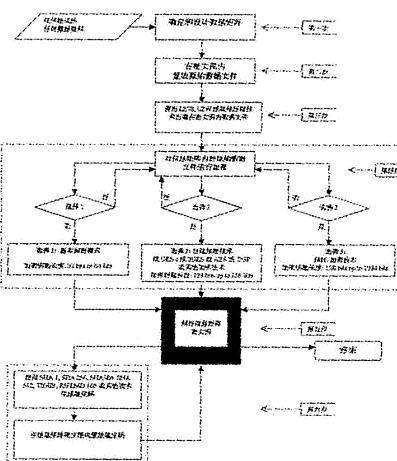
权利要求书 4 页 说明书 20 页 附图 16 页

[54] 发明名称

应用密文图技术对数据进行加密的方法

[57] 摘要

本专利发明的理念及技术是要把任何格式的数据文件无失真地转换成一种采用了信息矩阵技术、压缩技术、加密技术、数据分配技术及鉴定技术等五种技术制成的特别编码的密文图。这种带有特别鉴定编码的密文图几乎不可破解，因此可以有效地保护任何格式的文件的安全。信息矩阵密文图是防假冒、防伪造、防盗版、鉴定及验证的利器。信息矩阵密文图加密强度还可以通过一些方法提高到最强。本专利发明的理念及技术能够把任何格式、任何大小的数据文件无失真地转换成一个特别编码和全新格式的密文图。这个密文图内置几乎无法破解的特殊鉴定码。本发明专利的开放设计技术给用户多种加密方法的选择，使得数据资料得到安全而有效的保护，让用户更放心。



1. 一种对数据进行加密的方法,其特征在于,该方法包括以下步骤:

a. 设置用于储存和处理数据的信息矩阵,所述信息矩阵由数据穴(Cell)组成;

b. 将待加密的数据压缩后放入信息矩阵内的数据穴内;所述待加密数据为任何格式的数据文件;

c. 对信息矩阵内的数据进行加密;

d. 利用步骤c所述的信息矩阵生成鉴定码,并将该鉴定码放入所述信息矩阵的指定位置内,得到信息矩阵密文图,实现对数据的加密。

2. 根据权利要求1所述的方法,其特征在于,步骤b所述加密的实现方式为:采用低强度的基本加密模式,或者,采用高强度的密文图IMC加密技术;或者,采用用户设定的加密技术进行加密;

其中,所述用户设定的加密技术包括但不限于,AES(Advanced Encryption Standard)、RSA(Rivest-Shamir-Adleman Encryption System)、3DES (Triple Data Encryption Standard)、PGP(Pretty Good Privacy)。

3. 根据权利要求2所述的方法,其特征在于,所述高强度的密文图IMC加密技术包括以下步骤:

第一步,由用户或系统使用32字节数字串或256位元字符作为随机码算式的基数,以便生成随机数字;

第二步,选择随机码算式,该算式能够产生要求长度的随机数;

第三步,决定信息矩阵内的要进行交换的行和列的索引代码;

具体为,利用第一步确定的基数和第二步确定的随机码算式生成随机码,根据已设置的信息矩阵的大小,从每次产生的随机码的最后一个数字起向前选

择指定位数内的数字作为被选定为信息矩阵里的行或列的索引代码，再将该索引代码随机组合成对，作为要进行交换的行和列的索引代码；

所述向前选择指定的位数不超过5位数；

第四步，根据第三步确定的要进行交换的行和列的索引代码，选定该代码所指的行和列，把随机组合对的两个行或两个列，进行交换；所述交换次数根据加密强度的需要而确定。

4. 根据权利要求1所述的方法，其特征在于，步骤d所述利用步骤c所述的信息矩阵生成鉴定码的过程包括以下步骤：

首先生成一个制作随机鉴定码的160位元基数；该基数由系统自动生成，或由用户定义产生；

其次，利用所述160位元基数以及SHA-1算法生成一个160位元的HASH码，然后用SHA-1算法生成信息矩阵第一行的HASH码，再用XOR运算式把这两个HASH码混合，产生一个新的HASH码，称作HASH码1；

用HASH码1和用SHA-1生成的信息矩阵内第二行的HASH码，通过XOR运算式对HASH码1和信息矩阵内第二行的HASH码进行混合，生成HASH码2；用HASH码2和用SHA-1生成的信息矩阵内第三行的HASH码，通过XOR运算式对HASH码2和信息矩阵内第三行的HASH码进行混合，生成HASH码3；不断重复同样的过程，直到生成HASH码N；N代表信息矩阵的倒数第二行；

用HASH码N和用SHA-1生成的信息矩阵内最后一行的HASH码，通过XOR运算式进行混合后，最后生成信息矩阵使用的鉴定码；

所述指定位置为：信息矩阵最后一行。

5. 根据权利要求1所述的方法，其特征在于，步骤b所述压缩为无失真的压缩技术，该无失真的压缩技术包括但不限于LZ77、LZ78或LZW技术。

6. 根据权利要求1所述的方法，其特征在于，所述步骤c中对数据进行的

加密操作由预先设置的将信息矩阵里的数据文件进行加密，把信息矩阵转换成信息矩阵密文图的转码器钥匙完成，预先设置的解码器钥匙用来验证和鉴定密文图原始性和真实性，把在信息矩阵里的原始数据文件复原；

多组转码器和解码器钥匙系统包括三种钥匙系统，通用的一对多安全钥匙系统；用于高机密文件和隐私保护的一对一安全钥匙系统；用于防盗版和其他目的的联合安全钥匙系统；

所述通用的一对多安全钥匙系统有一对转码器钥匙和解码器钥匙；其转码器钥匙可以把任何格式的数据文件转换成密文图，其解码器钥匙可以把用其对称的转码器制成的密文图复原，每对转码器钥匙和解码器钥匙都是独立的，与其他对转码器钥匙和解码器钥匙互不兼容；此功能是通过给密文图文件设置不同的延伸名来实现的；

一对一安全钥匙系统是对每对转码器和解码器安全钥匙有严格的限制，每对钥匙只能对同一数据文件转码和解码，即一个数据文件只能有其唯一的转码器和解码器，使得一对一的安全钥匙系统能有效保护高度机密文件或用户隐私；

联合安全钥匙系统是转换器在把数据文件转换成密文图的同时生成一个伴随密文图的解码器，密文图只能被同时生成的解码器解码。

7. 根据权利要求6所述的方法，其特征在于，使用同一对转码器和解码器安全钥匙系统，或使用不同对的转码器和解码器安全钥匙系统对密文图进行多重加密，且使用多重加密方法的密文图需要两个或两个以上解码器安全钥匙系统才能对密文图进行解密。

8. 根据权利要求6所述的方法，其特征在于，使用隐形加密技术传送转码器钥匙和解码器钥匙及其配套的钥匙代码和密码；任何图片都可以作为隐形加密技术的隐藏转码器或解码器媒介；用隐形技术加密的转码器或解码器可以从

发送者的服务器上下载，或通过电子邮件等其他方式发送；接受者可以从隐形媒介取出转码器或解码器，然后，通过另外的方式取得钥匙代码和密码。

9. 根据权利要求6所述的方法，其特征在于，该方法进一步包括：在打开密文图之前，解码器会自动对密文图原始性和真实性进行鉴定，如果发现密文图不是原始数据文件或被改动了，系统会发出警告信息，随之，解码器系统则自动关闭。

10. 根据权利要求6所述的方法，其特征在于，该方法进一步包括：对转码器钥匙和解码器钥匙的处理数据文件的容量控制，从而限制成对的转码器和解码器的处理数据文件的能力。

应用密文图技术对数据进行加密的方法

技术领域

本发明是有关防假冒、防伪造、防盗版、鉴定及验证的技术。本专利发明的理念及技术能把任何格式和任何大小的数据文件无失真地转换成一种特别编码的密文图，从而实现对数据的加密和解密。本发明把信息矩阵技术、压缩技术、加密技术、数据分配技术、验证和鉴定技术巧妙地整合在一起，制成密文图。这种带有特别鉴定编码的密文图几乎不可破解，因此可以有效地保护任何格式的文件的安全。

背景技术

在数字时代，高速发展的数字技术就像一把双刃剑。它既能使人类的生活变得更简便，工作效率更高的有力工具。但是遗憾的是，数字技术也给犯罪分子提供了一个进行犯罪活动的有力器具。

当今，无论企事业单位还是个人都是使用电脑制作各类电子数据文件，依赖数据库和网络存储电子文件，通过内部或外部网络交换电子文件。在这些过程中，存在着这些电子文件被仿冒和被伪造的风险。犯罪分子可以利用市场上的软件和廉价的印刷技术，通过数字技术和方法对任何电子文件的内容加以修改或伪造。仿冒、伪造和盗版犯罪行为给人们生活和企业带来巨大危害和经济损失。自20世纪初以来，这些犯罪活动有增无减。据一家权威公司统计，在美国每天有超过1000的人成为身份证件被仿造和冒用的受害者。根据美国私人票据结算的统计，每天有40万个身份证件被窃，带来的经济损失高达20亿美元。除了产品仿冒外，盗版和伪造文件也是目前严重的问题。网络消费者被诈欺的案件更是有增无减。如何对付日益增长的仿冒、伪造和盗版的犯罪问题已经成为大小公司必须重视和解决的重要议题。

掌握如何保护电脑内有价值和秘密的文件要比破解和盗窃电脑内的文件要困难得多。因此发明一个能够有效地防仿冒、防伪造、防盗版和鉴定的数字技术的确是一种挑战。

目前已经有多项防仿冒、防伪造、加密和鉴定技术，如“*Ciphering and deciphering device* (密码及解码设备)，美国专利号4,972,481，1990年11月20日”、“*Encrypting conversion apparatus, decrypting conversion apparatus, cryptographic communication system, and electronic toll collection apparatus* (加密设备，解密设备，密文通信系统及电子收费设备)，美国专利号6,683,956，2004年1月27日”、“*Method for the secure handling of monetary or value units using prepaid data carriers* (使用预付数据载体传输贵重资料及安全处理金融技术)，美国专利号6,745,940，2004年1月8日”、“*Certification apparatus and method* (证书发放技术及方法) 美国专利号6,748,530，2004年6月8日”、“*Cryptographic apparatus and methods* (密码技术与方法) 美国专利号4,200,700，1980年4月29日”、“*Method and computer program product for hiding information in an indexed color image* (使用有标记的图像隐藏电脑生成的产品)，美国专利号6,519,352，2003年2月11日”、“*Large capacity steganography* (大容量隐形技术)，美国专利号6,473,516，2002年10月29日”、“*Computer system linked by using information in data objects* (使用数据对象信息连接电脑系统)，美国专利号6,553,129，2003年4月22日”和其他已经申请专利或没有申请专利的相关技术。当然各种防仿冒、防伪造、加密及鉴定技术都有自己的功能和特点。然而，这些已存在的技术和设备依然有许多问题需要解决。其中有些技术难于应用、有些技术由于要使用复杂的硬件设备导致成本太高，有些技术不够完善，因此不能达到有效地防止伪造和仿冒等犯罪的目的。

好的防仿冒、防伪造及加密的技术必须具备能够有效地保护任何格式的电子数据文件不被仿冒、伪造和盗版的性能。好的技术必须有唯一性，难于破解，不能被仿造，而且成本要低。

在防仿冒、防伪造、加密和鉴定技术之中，其中最重要的是加密技术。加

密技术在发明和制作高水准的相关技术中至关重要。理想的加密技术要包括四个技术特性：保密性、完整性、辨识性和鉴定性。传统的加密技术，如DES、RSA、AES和PGP等加密技术只有其中一两个特性。

随着电脑技术的快速发展，作为另类加密的隐形技术（Steganograph）最近也开始流行起来。但是隐形技术最大的局限性是隐藏数据的容量。多数隐形技术只能存储原来数据的15%，只有很少的隐形技术可以隐藏超过原来数据的50%。至今没有一种隐形技术有隐藏100%数据的能力。因此隐形技术无法广泛应用。如此说来，目前无论是传统的加密技术或是隐形技术都没有能提供最理想的加密措施。

发明内容

本发明的目的是找出另外一种新方法，即信息矩阵加密技术，能够有效地保护任何格式的文件不会被仿冒、被伪造或被盗版。

本发明的目的是要设计一个能够存储任何格式的文件的特别信息矩阵。信息矩阵表面看起来是一个普通的点阵影像图，但实际上它是一个特别编码的密文图。它把数据隐藏在信息矩阵内，而且无法破解。在信息矩阵内的数据格式和其原来格式完全不同。

本发明的目的是要采用其独有的数据放置方式，把原始数据放到信息矩阵内，并采用LZ77，LZ78，LZW或其他无失真压缩技术把数据压缩。这样不但可以有效地控制数据密文图的大小，而且可以不会失去数据的任何原始信息。

本发明的目的是用其独有的加密方式把数据放到特别编码的信息矩阵里。IMC加密技术把信息矩阵内的行和列用随机的方式根据用户要求的加密强度，至少交换128次，最多达到1024次。这样存储数据的矩阵会变成一个全新格式的密文图。密文图内的数据非常安全和保密。如果没有正确的解码器是无法追踪和解开密文图的。

本发明的目的是通过特殊的方法使用SHA-1或SHA-256或SHA-512或其他

任何类似技术生成唯一的鉴定码，然后把鉴定码存放在特别的信息矩阵最后一行内。这样，解码器可以辨识和鉴定密文图数据的原始性和可靠性。

本发明的目的是发明独特的，并能适用各种用途的多组对称安全钥匙系统。本发明有三种安全钥匙系统，即，一对多安全钥匙系统，为一般用途；一对一安全钥匙系统，为私人和绝密文件用途；联合安全钥匙系统，为反盗版和特殊用途。

本发明的目的是要设计一个特别的各种安全钥匙输送系统。这个系统利用特别编码的隐形技术传送解码可以转码钥匙或解码钥匙或相关的系统密码和身份证件信息。

本发明的目的是让使用信息矩阵密文图的用户可以有多种应用选择，不但可以根据各种用途制作能有效保证数据的安全各种密文图，而且使技术成本大幅度降低。

本发明是通过整合五种技术制作出一个有独一特性和功能的信息矩阵密文图系统，这个系统可以有效地保护任何格式的文件，不被访冒、不被防或盗版。信息矩阵密文图系统包括信息矩阵技术、数据压缩技术、数据加密技术、数据置放技术和数据鉴定技术。这些整合在一起的技术使得信息矩阵密文图系统有非常先进的特性和功能，可以保证文件的安全性达到最高强度。

本发明设计信息矩阵密文图的理念是能把任何格式和任何大小的文件转换成特别编码的信息矩阵密文图。在密文图里的数据格式与其原来的格式完全不一样。而且密文图里的鉴定码不但唯一，而且是通过特别方式产生的，无法破解。本发明的技术设计是开放的，允许用户在保护其数据资料安全强度和方式上有更多的选择。

本发明的信息矩阵密文图系统生成一个信息矩阵密文图需要六个步骤：1) 定义和设计信息矩阵；2) 把原始数据置放到信息矩阵中；3) 对信息矩阵里的数据进行压缩；4) 对信息矩阵里的数据进行加密；5) 把信息矩阵转

换成密文图；6) 制作和置放鉴定码。

附图说明

为了更清楚地说明本发明技术的原理，本申请书配有16张示意图。

- 图1、信息矩阵密文图系统结构
- 图2、信息矩阵密文图制作流程图
- 图3、信息矩阵尺寸样板图
- 图4-1、信息矩阵密文图中信息矩阵置放图式
- 图4-2、信息矩阵文档首注结构
- 图4-3、信息矩阵信息资料首注结构
- 图4-4、信息矩阵彩色结构和彩色索引列阵图示
- 图4-5、信息矩阵数据置放图
- 图5-1、三种加密方式选择示意图
- 图5-2、信息矩阵加密流程图
- 图5-3、信息矩阵内加密数据在重组前后的置放样板图
- 图6、多种强度加密流程图
- 图7、鉴定码生成流程图
- 图8、转码器和解码器的安全钥匙系统图
- 图9、转码器和解码器安全钥匙传送流程图
- 图10、安全钥匙工作流程图

具体实施方式

本发明的信息矩阵密文图系统具体内容将分十个部分逐一介绍。

第一部分：信息矩阵密文图系统结构

本发明可以让用户按其安全强度需要，把任何格式的数据资料转换成一个信息矩阵密文图，从而使得其数据资料不会被仿冒，或不被伪造，或被盗

版。这个信息矩阵密文图系统非常巧妙地把五种技术整合在一起，包括信息矩阵技术、数据压缩技术、数据加密技术、数据置放技术和数据鉴定技术。这些整合在一起的技术使得信息矩阵密文图系统有非常先进的特性和功能，可以使文件的安全性达到最高强度。

图 1 是信息矩阵密文图系统结构（此后简称“密文图”）示意图。密文图系统包括三个部分，即，密文图转码、密文图制作和密文图解码三个部分。密文图转码器和密文图解码器是一组对称的钥匙，总是在一起使用。密文图转码器的作用是把原始数据转换成与其原来格式完全不同的密文图。密文图解码器的功能是验证鉴定码无误后，把密文图里的数据还原。

第二部分：制作信息矩阵密文图

图 2 是信息矩阵密文图制作的流程图，它详细地说明了密文图制作的过程。密文图制作包括六个步骤，即，1. 定义和设计密文图；2. 把数据放入信息矩阵内；3. 把在信息矩阵内的数据进行压缩；4. 对在信息矩阵内的数据进行加密；5. 把信息矩阵转换成密文图；6. 在密文图内生成和置放鉴定码。

每一个步骤都有自己的特殊作用，非常重要，使得数据能按照正确的逻辑和巧妙地得到处理，从而保证信息矩阵密文图里的数据得到有效的保护。

第一步是定义和设计一个恰当的可以存储和处理的信息矩阵图。这个信息矩阵图表面看起来是一个普通的点阵图，但实际上它与普通的点阵图完全不一样。信息矩阵图由无数个数据穴（Cell）组成，用来存储数据。每个数据穴可以存储 4 位元（bit）字符。本发明使用的信息矩阵图最小的是 60×60 ，有 3600 个数据穴，可以存储 1024 个字节数据。最小的信息矩阵图要定义为 60×60 的原因是，这样大小的密文图可以才能保证规定的加密强度。

图 3 是三种不同大小的适用一般用途的信息矩阵的示意图。第一种信息矩阵有 3600 个数据穴（ 60×60 ），可以存储最多 1024 字节数据。第二种信息矩阵有 6,760,000 个数据穴（ 2600×2600 ），可以存储 3 百万字节数据。

第三种信息矩阵有 625,000,000 个数据穴（25000 x 25000），可以存储多达 3 亿字节内容。

从理论上讲，信息矩阵没有最大的尺寸限制。信息矩阵的尺寸的大小是根据要存储的数据实际容量来确定。不论信息矩阵有多大，所有信息矩阵密文图制作的过程是一样的。唯一的区别只是信息矩阵大小而已。例如，如果使用的电脑的 CPU 的速度是 2.0 GHz 和 128Mb 内存，足可以处理 25000 x 25000 信息矩阵。如果信息矩阵过大，这种配置的电脑处理起来速度就会变慢，需要的时间也多。然而，如果电脑的配备的 CPU 超过 3.8 GHz，内存超过 2.0G，任何尺寸的信息矩阵都可以很快的处理。

下面介绍信息矩阵是如何生成的。

如图 4-1 所示，每个信息矩阵都分为 4 个区（Chunk）。每个区存储的不同信息的数据。就像普通的点阵图一样，信息矩阵内也有文件首注（FILEHEADER）和信息首注（INFOHEADER）。信息矩阵第一区（14 个字节）用来存放文件首注。第二区（40 个字节）用来存储信息首注。第三区（256 个字节）用来存储彩色数据列阵表和索引。第四区（没有限制）用来存储原始数据，并在最后一行内存储鉴定码。在这个特别设计的信息矩阵里，每个数据穴只存储 4 个位元字符。

如图 4-2 所示，在第一区内文件首注内可以存储 14 个字节字符。这里信息全是关于数据矩阵本身的信息。第一组 2 字节说明数据矩阵的种类；第二组的 4 个字节说明数据矩阵的大小；第三组的 4 个字节说明数据矩阵的空间的数目，其中 2 个字节信息是保留空间信息 1（bfReserved1），2 个字节信息是保留空间信息 2（bfReserved2）初始值为 0；第四组的 4 个字节的信息是存储原始数据字符开始的缓冲区位值。

如图 4-3 所示，在第二区内信息首注内可以存储 40 个字节字符。第一

组 4 个字节说明信息矩阵尺寸结构(biSize); 第二组的 4 个字节说明信息矩阵影像点宽度(biWidth); 第三组的 4 个字节说明信息矩阵影像点的高度(biHeight); 第四组的 2 个字节说明信息矩阵的平面结构（初始值为 1）(biPlanes); 第五组的 2 个字节说明信息矩阵的深度（一种颜色为 4 个位元）(biBicount); 第六组的 4 个字节说明信息矩阵的数据被压缩后的长度(biBicompression); 第七组的 4 个字节说明在信息矩阵内的影像数据的长度（实际的影像点数）(biSizeImage); 第八组的 4 个字节和第九组的 4 个字节说明信息矩阵内每米影像点的解析度（初始值为 0）(biXPelsPerMeter)(biYPelsPerMeter); 第十组的 4 个字节说明信息矩阵内所使用的彩色列阵的彩色数目（初始值为 0）(biCirUsed); 最后一组的 4 个字节说明信息矩阵内实际使用最多的色彩（初始值为 0）(biCirImportant)。

如图 4-4 所示，第三区有 256 字节。彩色图表列阵结构在信息首注之后。彩色图表之后是彩色图表索引第二个列阵。在信息矩阵的内彩色索引列阵中的每个影像点是以索引的形式表示一种颜色。因此，彩色索引列阵的字符位元数等于影像点乘以彩色图表索引需要的字符位元数的积数。信息矩阵的色彩的多少不会影响信息矩阵密文图的功能。为了有效地控制信息矩阵的大小和显示速度，信息矩阵只用一个数据穴表示一种颜色，即，4 个字符位元一个数据穴表示一种颜色。

第四区，如图 4-5 所示，是最重要的存储原始数据的地方。这是信息矩阵的内最大的区域，它的大小由要保护的数据的大小来决定。信息矩阵的结构和普通点阵图结构在于他们存储和置放数据信息的方式完全不同。正因为如此，信息矩阵密文图是难于破解的。

在第四区，第一组 8 个数据穴存储信息矩阵的行数；第二组 8 个数据穴存储信息矩阵的列数；第三组 8 个数据穴存储信息矩阵的最后一行内的字符

数目；随其后的 4 个数据穴存储信息矩阵内文件首注使用的数据穴个数和用户电脑资料；再其后的 2 个数据穴存储信息矩阵内的文件名字母的个数；再其后的 2 个数据穴在信息矩阵存储电脑系统资料字符个数；信息矩阵内的最后一行的 40 个数据穴用来存储 160 位元长度的鉴定码。这是信息矩阵密文图的另外一个特别的功能。通过鉴定码，可以非常可靠地对信息矩阵密文图进行核证和鉴定。在第六部分将对如何生成鉴定码做详细的说明。

第三部分：信息矩阵内数据的压缩

第三步是对信息矩阵的数据进行压缩。为了控制信息矩阵密文图的大小和符合规定的大小范围内，本发明采取的重要的措施是对信息矩阵内的数据进行无失真压缩。通过压缩，密文图的尺寸会比原来的数据尺寸更小。个别数据因其内部格式复杂，经过压缩后产生的密文图会比原来数据尺寸略大，但不会超过 25%。这个压缩技术解决了数据文件转换成点阵图后，其尺寸会超大的难题。通常压缩技术可以采用目前已有的无失真技术，如，LZ77、LZ78 或 LZW 等压缩技术。这些技术都是比较好的无失真的压缩技术，可以达到本发明的要求的压缩标准。其他的可以达到本发明压缩标准的压缩技术可以应用。

使用无失真的压缩技术一是为了控制密文图的大小，二是保证原始数据信息有任何流失和改变。数据压缩是信息矩阵密文图技术必不可少的重要组成部分。

第四部分：信息矩阵内数据的加密

第四步是对信息矩阵内的数据进行加密，以便有效地保护数据的安全。信息矩阵密文图技术通过对数据位元独特的交换方式，彻底打乱了数据存放

模式，达到了加密的目的。

如图 5-1 所示，信息矩阵密文图技术有三种加密的模式。用户可以根据其需要选择加密的模式。这是本发明为方便用户所做的独特设计。它可使得采用本发明技术的用户更放心。

第一种加密选择（见图 5-1）是使用设定的基本加密方法。如果用户没有选择加密模式。本发明系统将自动选择基本加密设定模式。这种基本加密设定模式是公众可以使用的低等级加密标准。基本加密设定模式的安全钥匙长度为 64 位元字符。使用的基本加密设定模式加密的资料的加密寿命只有数天或数周。

第二种加密选择（见图 5-1）允许用户使用已存在的加密技术，如 3DES、AES、RSA、PGP 或其他的加密技术。如果用户选择了第二种模式，本发明系统的开放界面，让用户自行选择任何加密技术，或自己研发的加密技术。这样可以让用户放心地使用信息矩阵密文图，感到更安全。

第三种加密选择（见图 5-1）是使用本发明自己的加密方法。信息矩阵密文图加密技术（以下称“IMC 加密技术”）使用独特的交换方法，将信息矩阵重新格式化，这样在信息矩阵里的数据资料完全用随机的方法重新被排列，使得密文图几乎不可破解。

图 5-2 描述了 IMC 加密技术如何工作的。IMC 加密技术包括四个步骤，即 1) 生成制作随机数码的基数(Seed); 2) 选择制作随机码的公式; 3) 确定进行交换的行和列的随机代码; 4) 交换信息矩阵内的行和列

加密的第一步是生成制作随机码的基数。基数可以由本发明系统或用户

使用 32 字节个数字串或是 256 位元字符。如果用户自己没有输入随机码的基数，本发明系统将自动产生制作随机码的基数。这个基数可以视作一种增加密文图加密强度的密码。基数是产生随机码的一个数值。 X 是每次随机算式生成的随机数值。基数是让随机算式运算的初始值。本发明采用的是线性通余法 (Linear Congruential Method)，其基本模式是 $R_n = A R_{n-1} + C \bmod M$ 。其中 M 是系数值，由处理器的字元宽度而被定义，这种演算法将回传的随机数在 0 和 65,535 之间，而且不受内部的约束。 R_n 是随机数公式用来生成随机数的基数 (Seed)。这是一在 0 和 64K 之间任意常数。 A 是乘数，且为正整数。 C 是随机公式中的增值数，且为非负整数。用户输入一个初始整数作为基数。每一次随机算式运算，现在的基数值经过运算后产生的基数值，乘以 A ，加上 C ，取余数 $\bmod M$ 为结构。新的基数值是在 0 与 $M-1$ 之间的整数。这个新的基数值被转换成给用户使用的 X 值。

加密的第二步是选择随机码算式。本发明的重点是用随机算式产生给信息矩阵内的行和列的索引代码。只要能产生可靠的和正确的随机数的随机数算式，即能够产生前述所要求长度随机数的任何随机数算式都可以采用，并不限于线性通余法。

加密的第三步是决定信息矩阵内的要进行交换的行和列的索引代码。本发明需要的随机码 X 只是 1—5 位的数字，例如： $X - XXXXX$ 。根据现在信息矩阵的设计，每个信息矩阵的行和列的数目不超过 5 位数。这就是为什么 5 位数字是本系统需要的最大数值。本系统根据信息矩阵的大小从每次产生的随机码的最后一个数字起选择所需要的索引代码。

用 2600×2600 数据矩阵为例，它有 2600 列和 2600 行。行和列的代码将从 1-2600 数字范围选出。但在实际的选取号码时，1 与 2600 两个数字除外。随机码数字是在 1,000,000 至 100,000,000 范围内。本发明系统将随机选出一些数字，如，2,34; 468,78; 2100,193; 476,1200……。然后系统会把这些选出的数字再随机组合成对，例如：78 与 38 为一对；468 与 2 为一对；

2100 与 476 为一对；193 与 1200 为一对。每对数字用来作将进行交换的两个行或两个列的代码，例如：78 与 34 分别代表第 78 列和第 34 列，这表示第 78 列将与第 34 列对调在信息矩阵的位置；2100 与 476 分别代表第 2100 行和第 476 行，这表示第 2100 行将与第 476 行对调在信息矩阵的位置；根据系统需要的加密强度，这个过程将一直重复下去，直到信息矩阵里面的行和列都进行了随机对换。

加密的最后一步是交换数据矩阵内的行和列。加密实际上从这一步开始。本发明系统根据随机选出的行和列的代码，把随机组成对的行或列，进行交换。根据加密强度的需求，行或列的各自交换的次数至少 128 次，最多为 1024 次。行与列的交换次数完全取决于加密强度的需要。换句话说，行和列交换的次数越多，加密的强度也就越高。然而本发明对行和列交换的次数最高限定为 1024 次，是因为超过这个限制的交换对加密强度的提高没有太大的意义。行和列进行了 1024 次的交换后，足可以使得信息矩阵获得最大的加密强度。破解最高加密强度的密文图的概率只是 10^{77} 分之一。如果没有正确的解码器钥匙，可能花费企图破解密文图人的很长时间，甚至是终生时间。

图 5-2 展示了信息矩阵里的行和列交换前与交换后，数据置放状态。行和列每交换一次就产生一个新的信息矩阵。这样，存储在信息矩阵内的文件内资料和信息是完全随机模式存储在里面了。行和列的交换完全是随机的。密文图里的数据存储格式与其原来的格式完全不一样。任何人都无法预测密文图内每个数据穴内存储的是什么信息。然而，在现实生活中，加密的强度应该根据数据文件寿命来决定。因此要需要保护的数据文件的加密强度要根据其寿命而定。根据下表，用户可以根据数据文件的寿命来选择正确的加密钥匙的长度。加密钥匙长度越短，成本也就越低。

选择加密钥匙长度参考数据表

数据文件的性质	数据文件的寿命	建议使用的最小的加密钥匙长度及行和列需要交换的次数
一般的文件	数分钟 / 数小时	钥匙长度32位元-64位元； 行和列交换40-56次
产品信息 公司信息	数周 / 数月	钥匙长度64位元-128位元； 行和列交换56-100次
考试题目	一两个月	钥匙长度128位元； 行和列交换800次
企业计划书	数年	钥匙长度128位元； 行和列交换800次
贸易秘密	数十年	钥匙长度128位元； 行和列交换800次
财务文件	20年或更长	钥匙长度128位元； 行和列交换800次
军事文件	数年 / 20年或更长	钥匙长度128位元-256位元； 行和列交换800-1024次
高度机密文件	30年或更长	钥匙长度128位元-256位元； 行和列交换800-1024次
个人身份证明 医疗资料等	终生	钥匙长度128位元-256位元或更多； 行和列交换800-1024次或更多

说明：表内所列信息仅仅是参考资料。数据文件寿命时间要认真研究后
再确定，以便选择正确的加密钥匙的长度和行和列交换的次数。

本发明的基本加密的模式，行和列至少要各交换 40 次以上，其加密强
度可以达到 64 位元长度。

图示六描述了对密文图的进行多重加密的工作原理。这是本发明的一个
独特功能。本发明可以对储藏在密文图里的数据进行多次加密。此方法被称
为“密文图多重强度加密法”。根据特殊需要，用户可以使用此法，使得密
文图获得“双重加密强度”或“三重加密强度”或“四重加密强度”或更多
级的加密强度。而且，本发明允许用户即可以只用同一对转码器和解码器安

全钥匙系统或使用不同对的转码器和解码器安全钥匙系统对密文图进行多重加密。多重加密方法使得密文图更难破解，因为必须要使用全部正确的解码器钥匙才能解开密文图。这样可以使得密文图的获得极强的加密强度，以满足特殊需要。例如，有一些高度机密文件需要两个人或多人同时在场才能查阅，本发明的多重加密就可以完全满足这种特殊需要，确保高度机密文件安全得到彻底保证。

第五部分：制作和置放鉴定码

使用 SHA-1 或其他的类似技术制作鉴定码和置放鉴定码是完成信息矩阵密文图的最后一个步骤。SHA-1，一种安全的 HASH 算法，通过计算生成一个能代表信息或数据文件的压缩的字符串。当输入一个长度小于 2 的 64 次方 ($<2^{64}$) 的信息字符后，SHA-1 生成一个 160 位元的字符串，被称作信息文摘（message digest）。这个信息文摘是唯一的，无法被仿制。任何被传送信息，一旦被改动，信息文摘则不会认识原始信息，因此可以用来验证信息的原始性和真实性。

图 7 是鉴定码生成的流程图，介绍了如何制作用来生成一个信息矩阵的鉴定码。首先是要生成一个制作鉴定码的 160 位元基数。基数的产生有两种方式。一种是由本发明系统自动生成，一种是由用户自己产生。本发明系统或用户在电脑内输入一组字符串。字符串的长度为 20 字节。字符串可以是字母或数字，或字母与数字的混合。有了基数后，本发明系统使用 SHA-1 生成一个 160 位元的 HASH 码，然后用 SHA-1 生成信息矩阵第一行的 HASH 码，再用 XOR 运算式把这两个 HASH 码混合，产生一个新的 HASH 码，称作 HASH 码 1。用 HASH 码 1 和用 SHA-1 生成的信息矩阵内第二行的 HASH 码，通过 XOR 运算式进行混合生成 HASH 码 2。用 HASH 码 2 和用 SHA-1 生成的信息矩阵内第三行的 HASH 码，通过 XOR 运算式进行混合生成 HASH

码 3。不断重复同样的过程，直到生成 HASH 码 N。N 代表信息矩阵的倒数第二行。用 HASH 码 N 和用 SHA-1 生成的信息矩阵内最后一行的 HASH 码，通过 XOR 运算式进行混合后，最后生成一个信息矩阵使用的鉴定码。这个鉴定码将存储在信息矩阵最后一行里。有了这个鉴定码，就可以可靠和安全地鉴定一个信息矩阵的原始性和真实性了。如果鉴定不属实，解码器钥匙将无法打开密文图。本发明制作鉴定码的方法是独特的，与现在所有制作的鉴定码的方式都不一样。这样的信息矩阵密文图图的鉴定码是难于追寻和破解的，因为它不是一个用简单方法制作出的信息文摘。

第六部分：把原始数据文件转换成密文图

如图 2 所示，这是密文图技术的第六步。在完成前面的几个步骤后，本发明系统将自动把原始数据文件转换成密文图。在密文图里的原始数据文件格式与其原来的格式完全不同。

第七部分：多组转码器和解码器安全钥匙系统

本发明的另一个重要的特性是使用多组转码器和解码器安全钥匙系统。转码器和解码器钥匙是一对对称加密钥匙。转码器和解码器必须成对地在一起工作。转码器功能是定义和制作信息矩阵密文，置放信息矩阵，对在信息矩阵里的资料进行压缩和加密，把原始数据转换成密文图，制作密文图的鉴定码。解码器的功能与转码器的功能正相反，即要验证和鉴定密文图的真实性，解密和解压缩，准确地复原密文图里的原始数据文件。

如图 8 所示，多组转码器和解码器安全钥匙系统的结构。1. 一对多安全钥匙系统（本发明的基本设定的钥匙系统）；2. 一对一安全钥匙系统；3. 联合安全钥匙系统；每种安全钥匙系统都有自己的独特功能和作用。多组转

码器和解码器安全钥匙系统不但强大，而且灵活。用户可以其要求的加密强度，选择恰当的安全钥匙系统。

一对多安全钥匙系统（基本设定）是一对转码器和解码器。其转码器把任何格式的数据文件转换成密文图，其解码器可以发给所有被授权使用的人员去解开用其配对转码器制作的密文图，阅览数据文件。

基本钥匙系统的另一个强大的功能。为了保护用户的隐私和安全，每组安全钥匙系统都是不同的，即各组安全钥匙系统不能互相通用，即 A 组的解码器钥匙不能打开用 B 组的转码器钥匙制作的密文图。这个设计可以有效地保护用户的隐私和安全。

通过给不同组一对多安全钥匙系统的制作的密文图文件的以不同的延展名(3 个字符)，这个延展名只能被其制作的密文图那对安全钥匙认识，如 A 组密文图的延展名是“axd”，B 组密文图的延展名是另外的名字“xyz”。这样 A 组的解码器不能打开 B 组的密文图，反之，B 组的解码器也打不开 A 组的密文图。密文图的延展名是随机选定，没有任何规律可循。延展名可以由用户自己输入到电脑系统内，或由本发明的系统随机确定。

一对一安全钥匙系统是对每对转码器和解码器安全钥匙有严格的限制。每对钥匙只能对同一数据文件转码和解码，即一个数据文件只能有其唯一的转码器和解码器。制作一对一安全钥匙系统是通过给转码器和解码器钥匙输入一个特别密码。这个特别密码由安全钥匙系统自动输入密文图内。解码器除了要验证鉴定码外，还要鉴定密文图内的这个特别密码。如果解码器找不到对应的特别密码，解码系统会自动停止，并发出警告。这个特别密码内的信息包含需要保护文件的概括说明，它可以用任何方法产生。然而，本发明建议用被保护的文件自身生成一个加密基数，再用 SHA-1 制作出特别密码。

一对一的安全钥匙系统是保护高度机密文件和用户隐私的最佳工具。

第三种安全钥匙系统是联合安全钥匙系统。联合安全钥匙系统是转换器在把数据文件转换成密文图的同时生成一个伴随密文图的解码器，称之为联合解码器。只有这个解码器才能打开其伴随密文图。例如，用联合安全钥匙系统中的转码器把一个音乐文件 eleventree.mp3 转换成密文图，同时生成两个文件是一个音乐文件的密文图 eleventree.pav，另外一个文件是联合解码器 eleventree.exe。这个音乐文件密文图只能被其联合解码器打开和播放。这种联合安全钥匙系统可以有效地保护音乐、软件、视频产品的知识产权。它是对付盗版犯罪的利器。

第八部分：转码器钥匙和解码器钥匙的传送

如何安全传送密码制作钥匙和解码钥匙一直未能很好的解决。本发明设计了几种传输安全钥匙的方法。

图 9 介绍了送安全钥匙系统的几个步骤。首先把转码器钥匙和解码器钥匙用隐形加密技术把钥匙隐藏在隐形图片中，同时配有一套钥匙代码和密码。任何图片都可以作为隐形加密技术的隐藏转码器或解码器的媒介。其次，用隐形技术加密的转码器或解码器可以从发送者的服务器上下载，或通过电子邮件等其他方式发送。第三，接受者可以从隐形媒介取出转码器或解码器。然后，通过另外的方式取得钥匙代码和密码。这是非常安全的传送安全钥匙和其配套的钥匙代码和密码。

身份证码和密码必须通过语音等其他方法传送给收件人。这套传送系统非常安全，非授权的人是无法破解的。只有授权的人才能得到安全钥匙及配套身份证码和密码。

前面曾讨论过，隐形加密技术有隐藏信息容量的局限。然而，加密小容量的信息，隐形加密技术仍不失为一个好的技术。安全钥匙系统里的转码器和解码器、钥匙代码和码的容量非常小，隐形加密技术隐藏这些资料没有任何问题。本发明对使用什么样的隐形加密技术没有特殊要求。因此，只要能完成本发明的要求的任务，可以使用任何现成的或自行开发的隐形加密技术。

第九部分：转码器钥匙和解码器钥匙系统工作机制

如图 10 说明成对的转码器钥匙和解码器钥匙系统工作机制。首先，读取准备加密的数据文件。数据文件可以是任何格式、任何大小、任何类别的数据资料。转码器按照图二所示的步骤，信息矩阵转换成密文图。所有加密好的密文图都会被存储在预先设置的文件夹“encoderfile”内。在打开密文图之前，解码器会自动对密文图原始性和真实性进行鉴定。如果发现密文图不是原始数据文件或被改动了，系统会发出警告信息，如“此密文图不是原始文件或是已被改动，解码器将终止工作”等警告信息。如果密文图通过鉴定，在密文图里的数据文件将被复原，并存入预先设置的文件夹“decoderfile”内。预先设置的文件夹可以由用户自行设置，如用户没有设置，本发明系统会自动给预设两个文件夹，以便用户方便地找到密文图和被解码的密文图的在电脑内存放位置。

转码器和解码器安全钥匙系统还有另外两个特点：一是本发明的安全钥匙系统可以在用户阅读完后被打开的密文图里的数据文件会自动关闭，这样可以保护打开的数据文件，不会被窃取。此功能是选择性，用户可以根据需要启动或关闭此功能。二是对转码器钥匙和解码器钥匙的处理数据文件的容量控制，从而达到限制成对的转码器和解码器的处理数据文件的能力。本发

明可以给成对的转码器和解码器规定可以处理的数据文件的大小，如，本发明限定成对的转码器和解码器只能处理 100K 位元以内的数据文件。超过了 100K 的数据文件，这对被限定处理的容量转码器和解码器则不能工作。这个功能可以满足客户在对安全加密钥匙能力进行控制的需求。

传统的加密技术和方法基本多是在原始数据上加上保护罩或壳。这种加密的方式很脆弱，一旦部分加密的地方被破解，整个加密的文件就很容易被破解。然而，本发明是把原始的文件格式彻底改变，经过压缩和机密后，转换成有特殊的鉴定码的密文图。本发明的加密技术完全符合加密技术的四个基本条件，即辨识性、保密性、完整性和鉴定性。本发明最强的部分是其多组安全钥匙系统的设计。用户可以根据其需要选择加密模式。本发明可以根据现实世界的情况制作各种不同类别的转码器和解码器安全钥匙系统。

第十部分：本发明实际应用的领域

利用信息矩阵密文图技术强大的功能和特性可以制作许多产品，如防假冒、防伪造、防盗版及进行验证和鉴定的各种产品。信息矩阵密文图技术可以应用许多产业和领域，如银行、证券部门、金融机构、教育部门、医学部门、政府部门等等。正在研发的产品有：银行文件安全系统、证书验证系统、试卷安全系统、医学档案安全系统、企业文件安全系统、音乐版权保护系统、软件版权保护系统、电子邮件保护系统等等。

信息矩阵密文图技术可以和其他硬件设备如 RFID 和 PDA 等设备制作出更多的强大的产品，如防假冒上表/封条系统、资产追踪及管理系统等。

总之，本发明信息矩阵密文图技术的功能和特性的潜力可以开发出更多的、各种各样的关防假冒、防伪造、防盗版和鉴定方面的产品。

本申请对本发明的功能和特性作了详细的介绍，并说明这些功能和特性如能实现。任何在本发明领域和在本发明的精神原则内，对本发明的功能和特性所作的各种修改，补充及修正都是欢迎的。

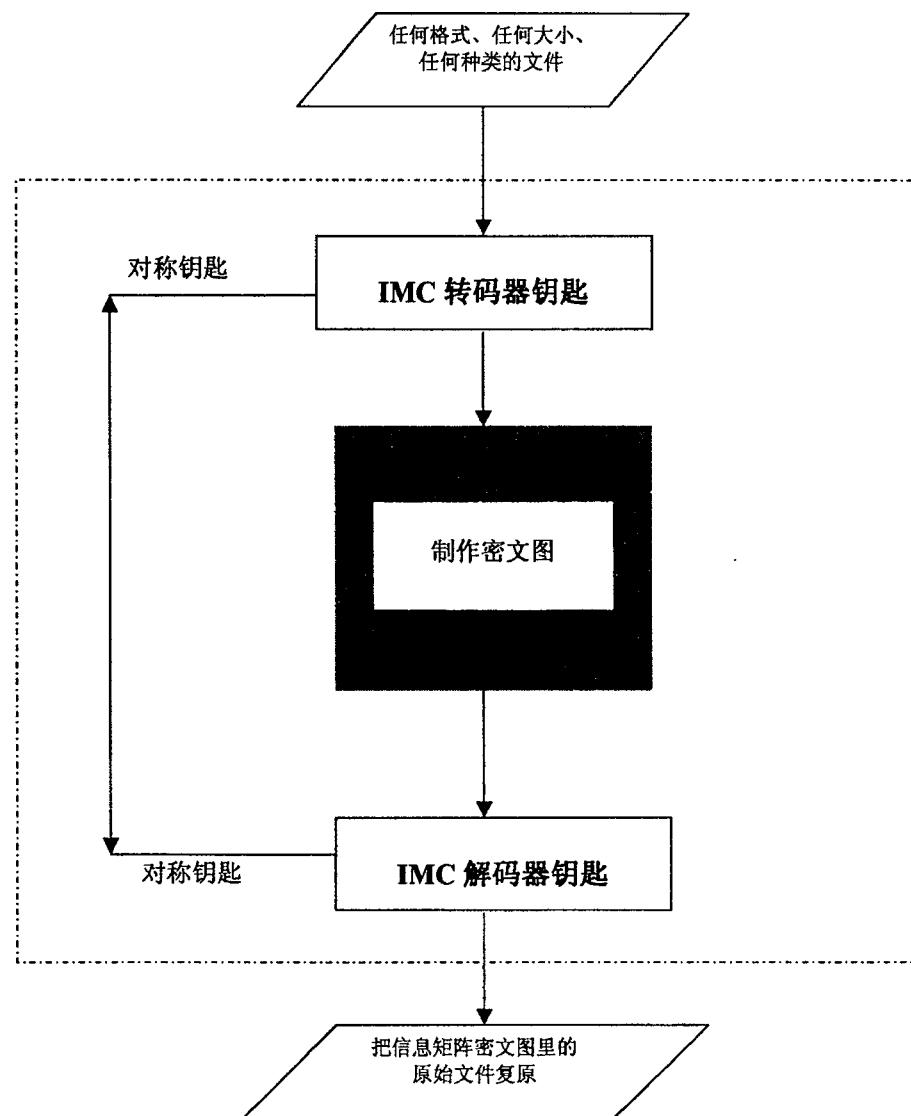


图 1

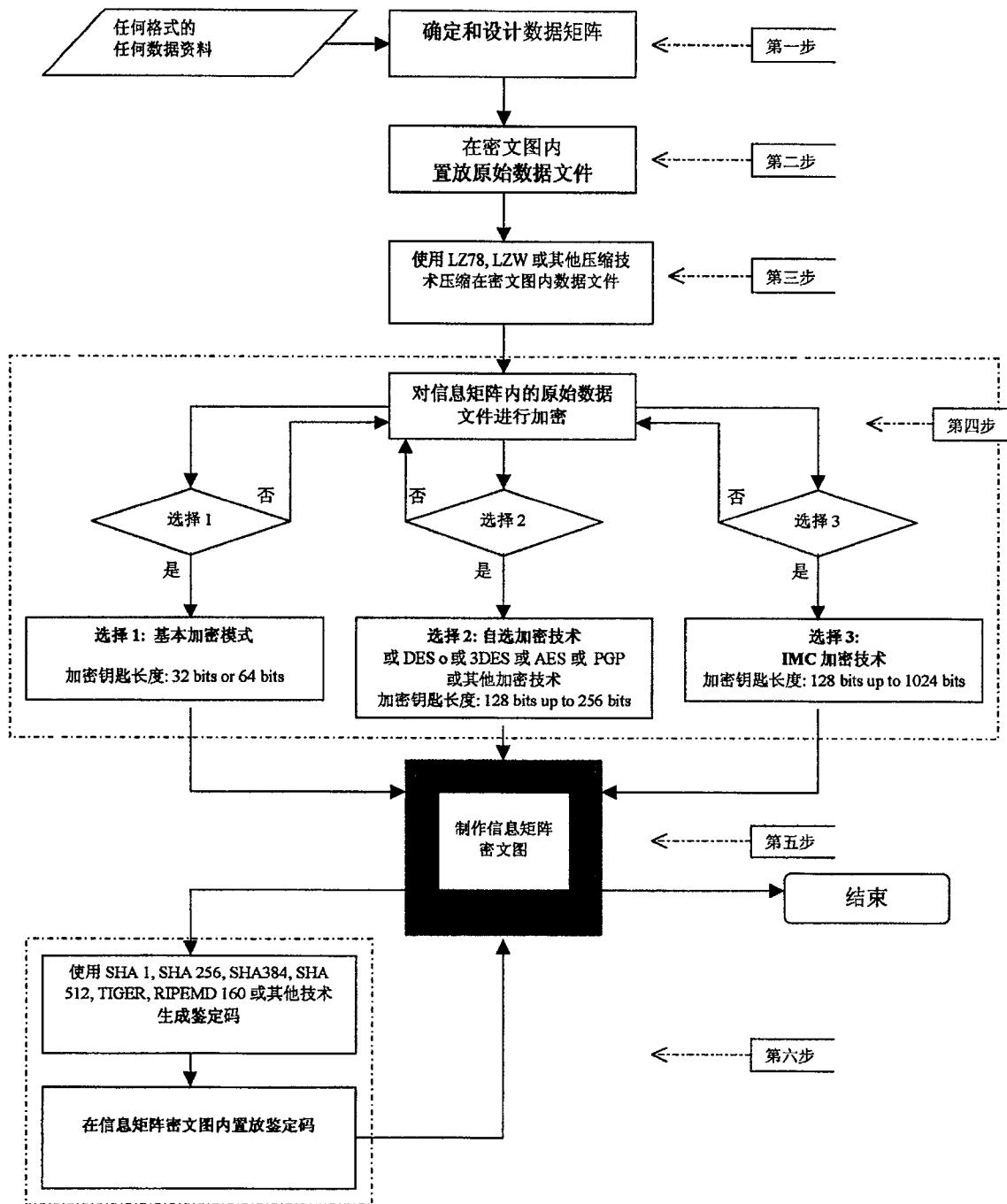
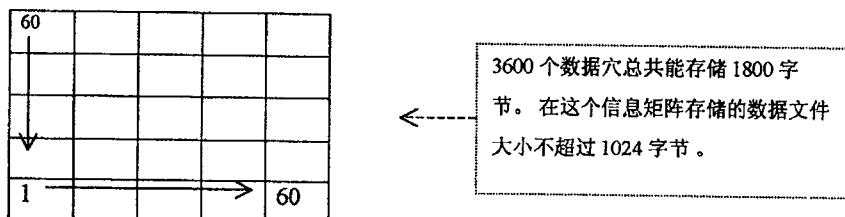
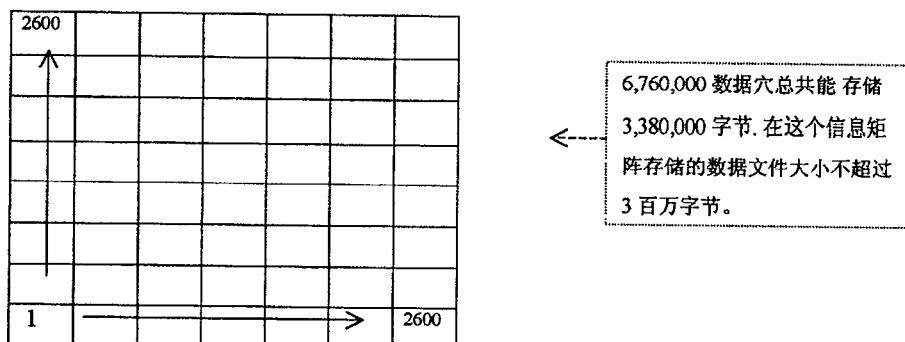


图 2

1. 存储 1 个字节 至 1 千个字节数据 的基本尺寸的信息矩阵



2. 存储 1 字节 至 3 百万个字节数据的中等尺寸的信息矩阵



3. 存储超过 3 百万个字节数据的大型尺寸的信息矩阵

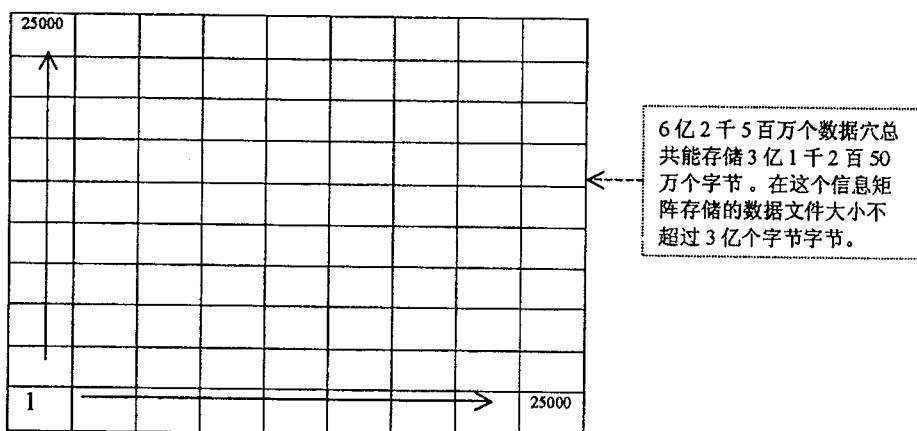


图 3

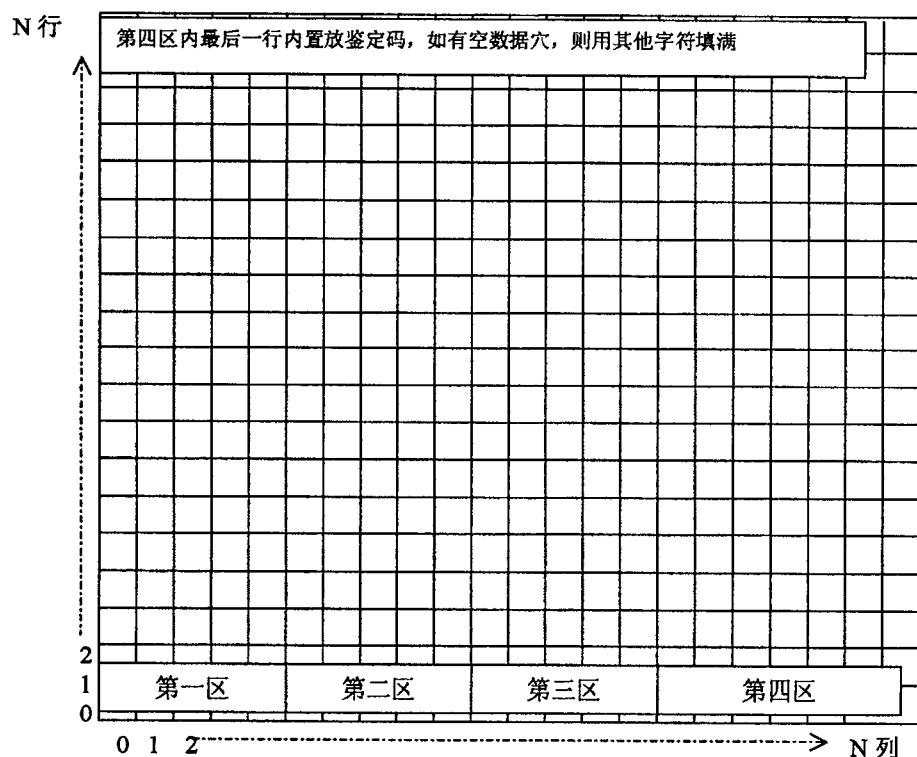


图 4-1

第一区: 14 字节

第一个字节	第2个字节	第3个字节	第4个字节	第14个字节
-------	-------	-------	-------	-------	--------

第一组 2 个字节 (**bfType**): 2 个字符 “BM” 如点阵图

信息矩阵的类别

第二组 4 个字节 (**bfSize**): 决定整个数据矩阵的大小

数据矩阵的尺寸

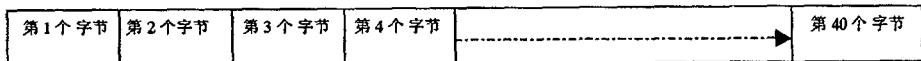
第三组 4 个字节 (**bfReserved1** and **bfReserved2**): 保留空间
(2 个字节 为保留空间 1 及 2 个字节为 保留空间 2)

数据矩阵的空间 (初始值为 0)

第四组 4 个字节 (**bfOffBits**): 描述位元的个数

从数据文件开始处的位元字节缓冲区

图 4-2

第二区: 40 字节**第一组 4 字节 (biSize):**

点阵信息首注点阵图结构的尺寸

第二组 4 字节 (biWidth):

数据矩阵影像点宽度

第三组 4 字节 (biHeight):

数据矩阵影像点高度

第四组 2 字节 (biPlanes):

数据矩阵平面的数目 (初始值为 1)

第五组 2 字节 (biBitCount):

数据矩阵的深度(4 个位元 表示 1 种颜色)

第六组 4 字节 (biCompression):

数据矩阵被压缩后的长度

第七组 4 字节 (biSizeImage):

数据矩阵内的影像数据的长度 (实际的影像点数)

第八组 4 字节 (biXPelsPerMeter) 和第九组 4 字节 (biYPelsPerMeter):

数据矩阵内每米影像点的解析度 (初始值为 0)

第十组 4 字节 (biClrUsed):

数据矩阵内所使用的彩色列阵的彩色数目 (初始值为 0)

第十一组 4 字节 (biClrImportant):

数据矩阵内实际上使用最多的色彩 (初始值为0), 增加显示速度

图 4-3

第三区: 256 个字节

这只是一个四彩色的结构图示

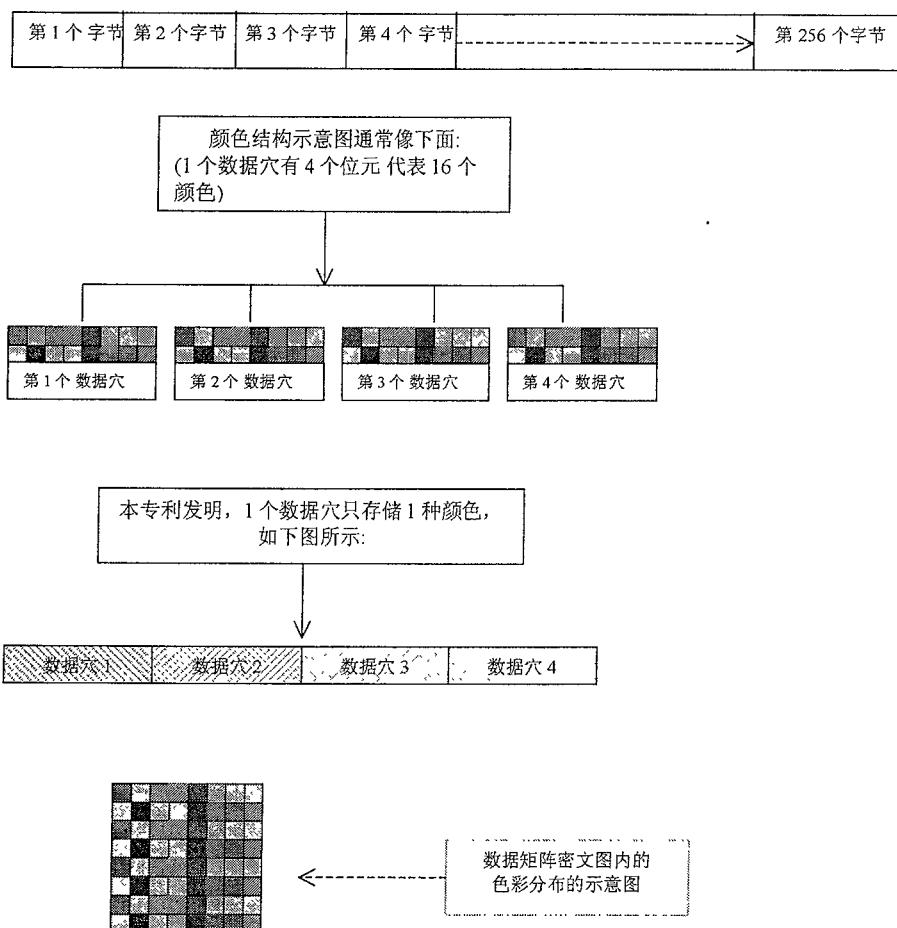


图 4-4

第四区：没有容量限制

第1个字节	第2个字节	第3个字节	第4个字节	----->	没有尺寸限制
-------	-------	-------	-------	--------	--------

数据置放的示意图

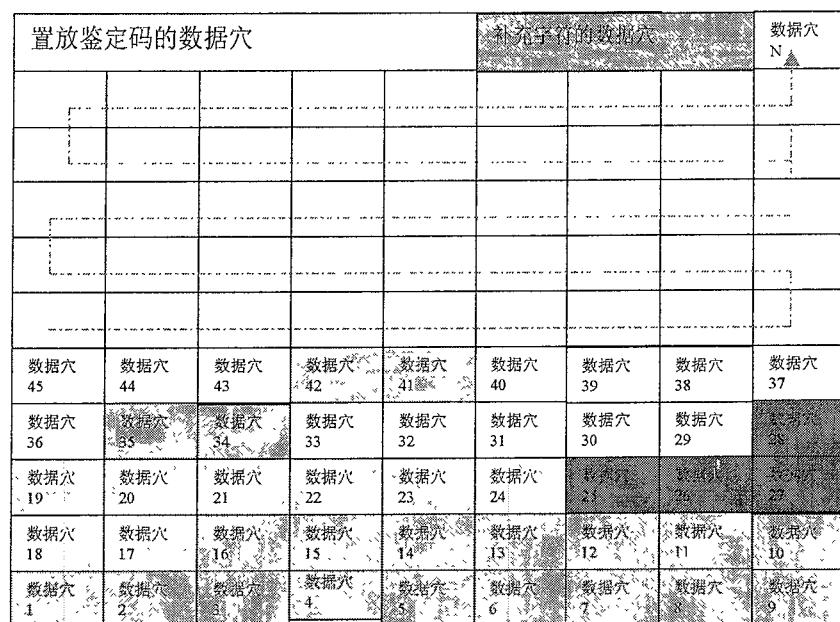


图 4-5

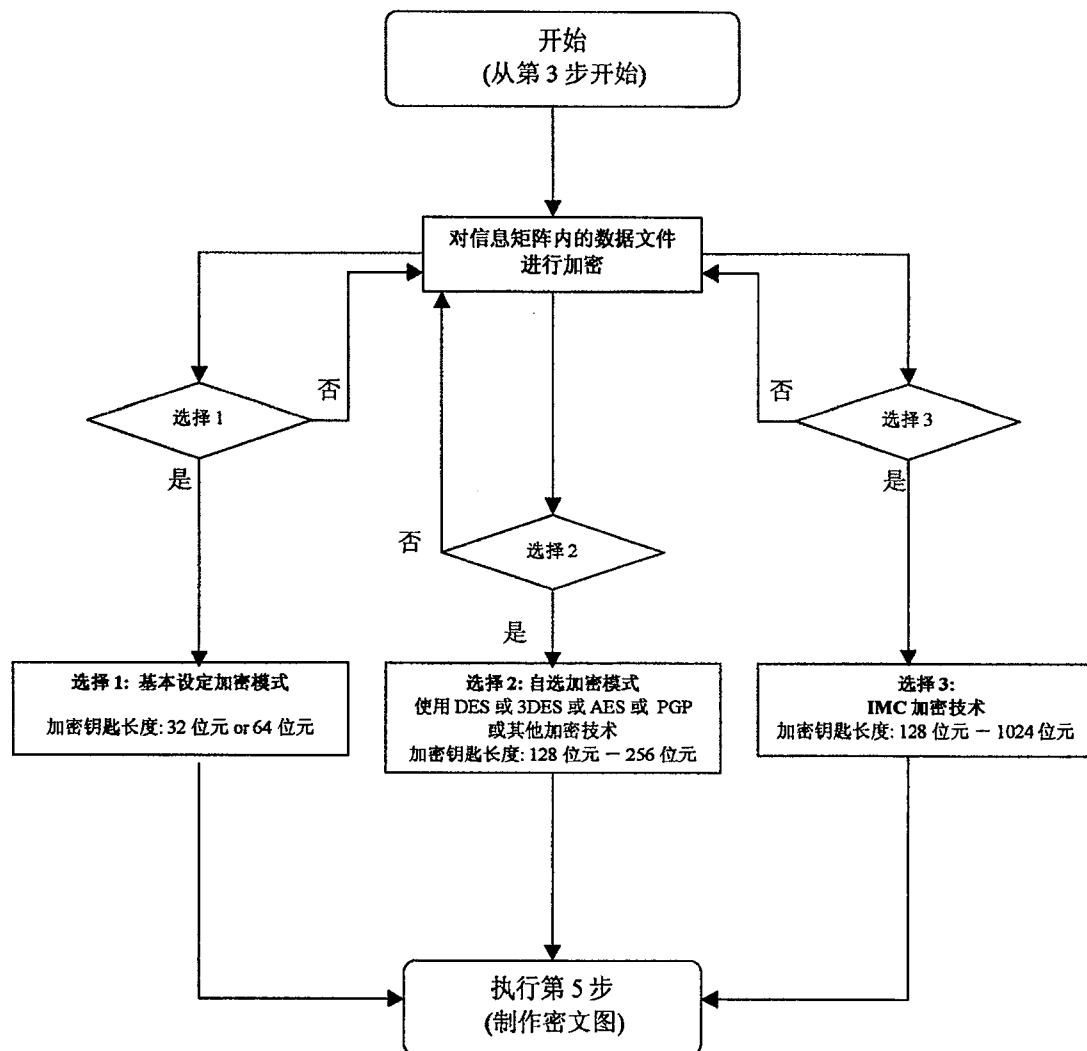


图 5-1

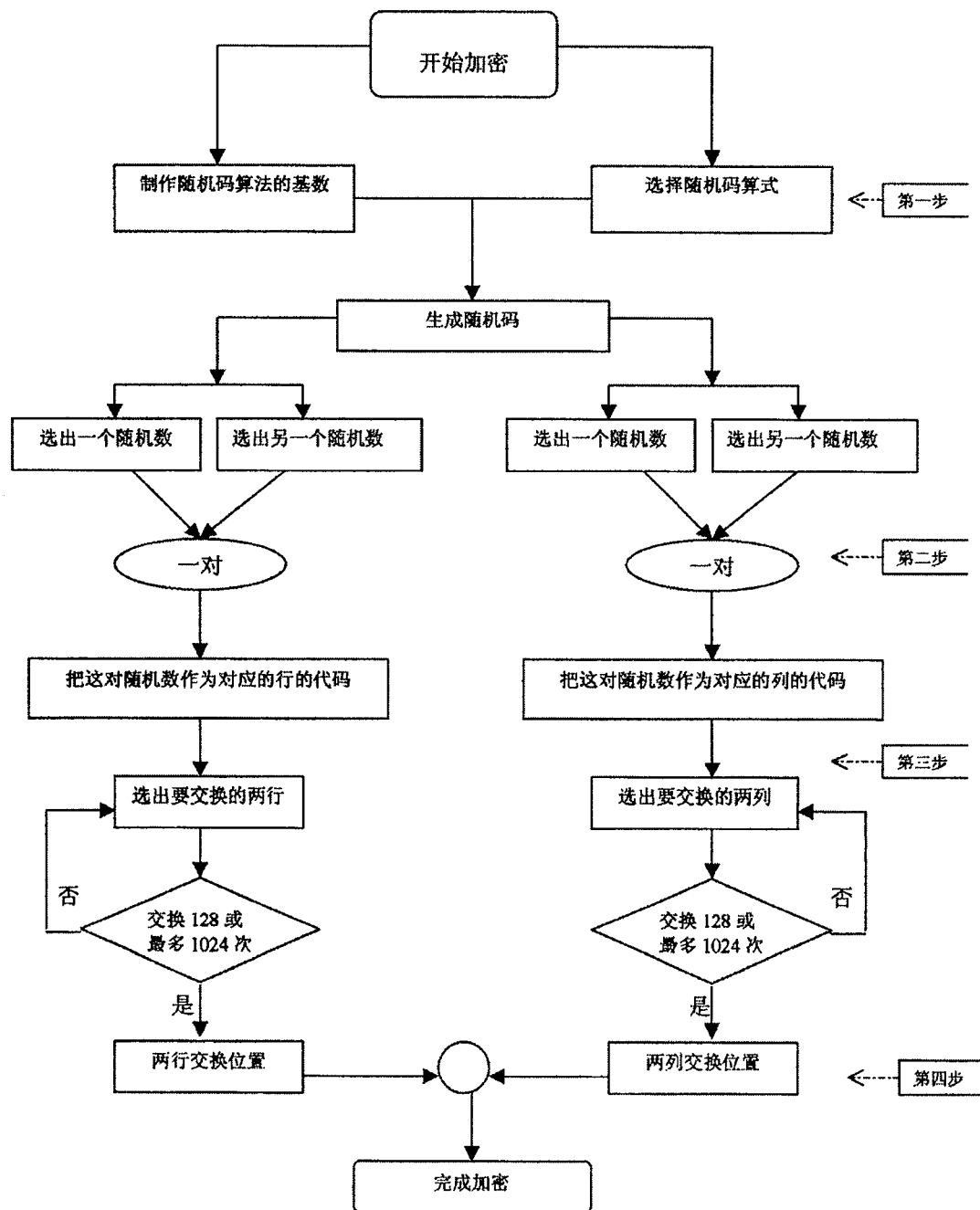


图 5-2

以 10×10 数据矩阵为例说明在数据矩阵的数据文件，在数据矩阵的行和列位置交换前和后的密文图的状态

交换前：

C10		3		5		7		9	
C9	9	9	9	9	9	9	9	9	9
C8		3		5		7		9	
C7	7	7	7	7	7	7	7	7	7
C6		3		5		7		9	
C5	5	5	5	5	5	5	5	5	5
C4		3		5		7		9	
C3	3	3	3	3	3	3	3	3	3
C2		3		5		7		9	
C1	R2	R3	R4	R5	R6	R7	R8	R9	R10

交换后：(这只是信息矩阵的行和列交换后的示意图。在信息矩阵内的行和列至少要分别交换 128 次，或多达 1024 次，或更多)

5	3	5	9	5	7	5	C10	5	5
4		9		3			C4		7
7	7	7	3	7	5	7	1	7	7
8		9		3			C7		9
R8	R9	R6	R2	R4	R5	R7	C6	R3	R4
6		9		3			C8		9
3	9	3	9	3	7	3	C9	3	7
10		7		3			C10		7
2		9		3			C2		7
9	7	9	3	9	3	9	C3	9	7

图 5-3

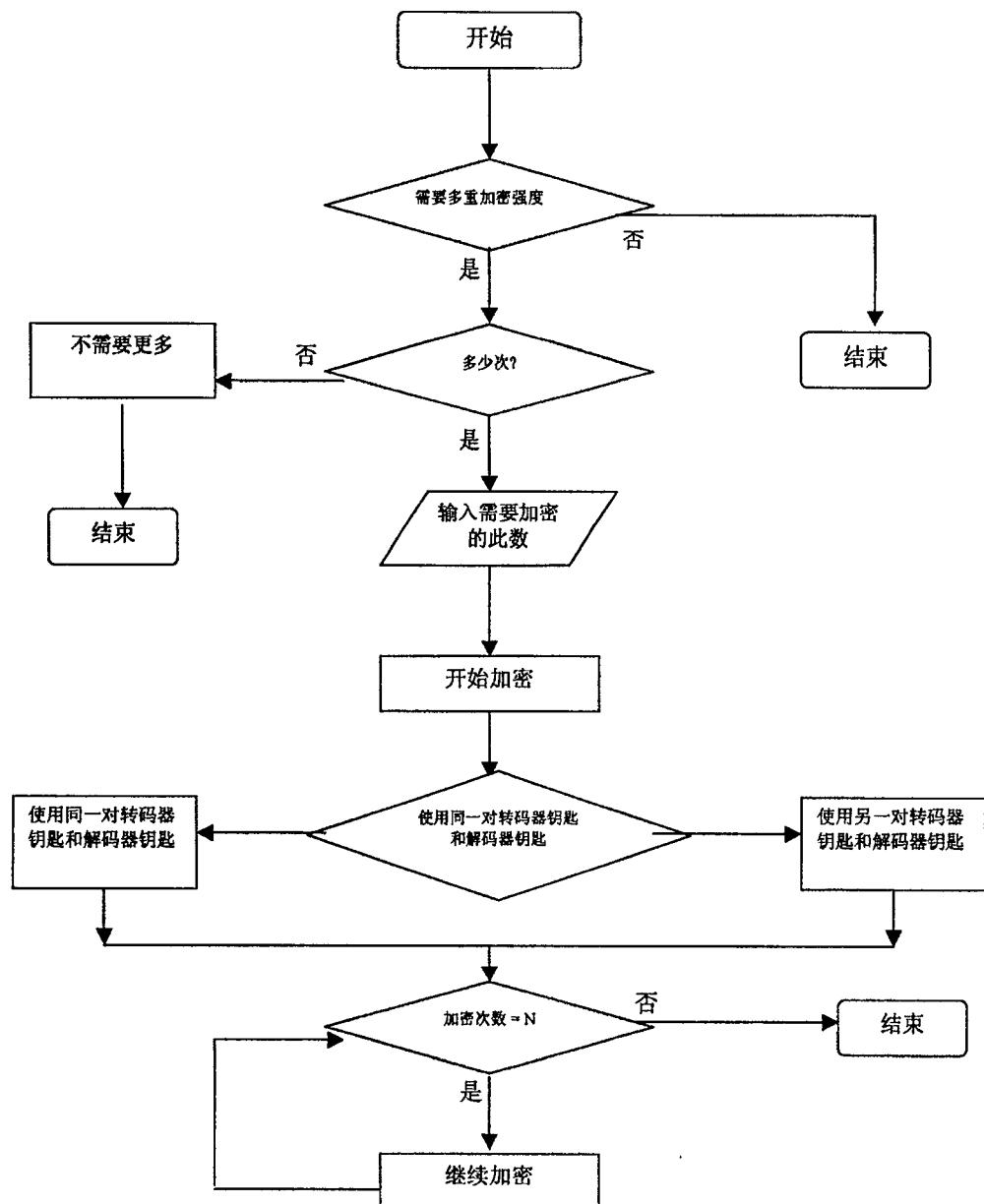


图 6

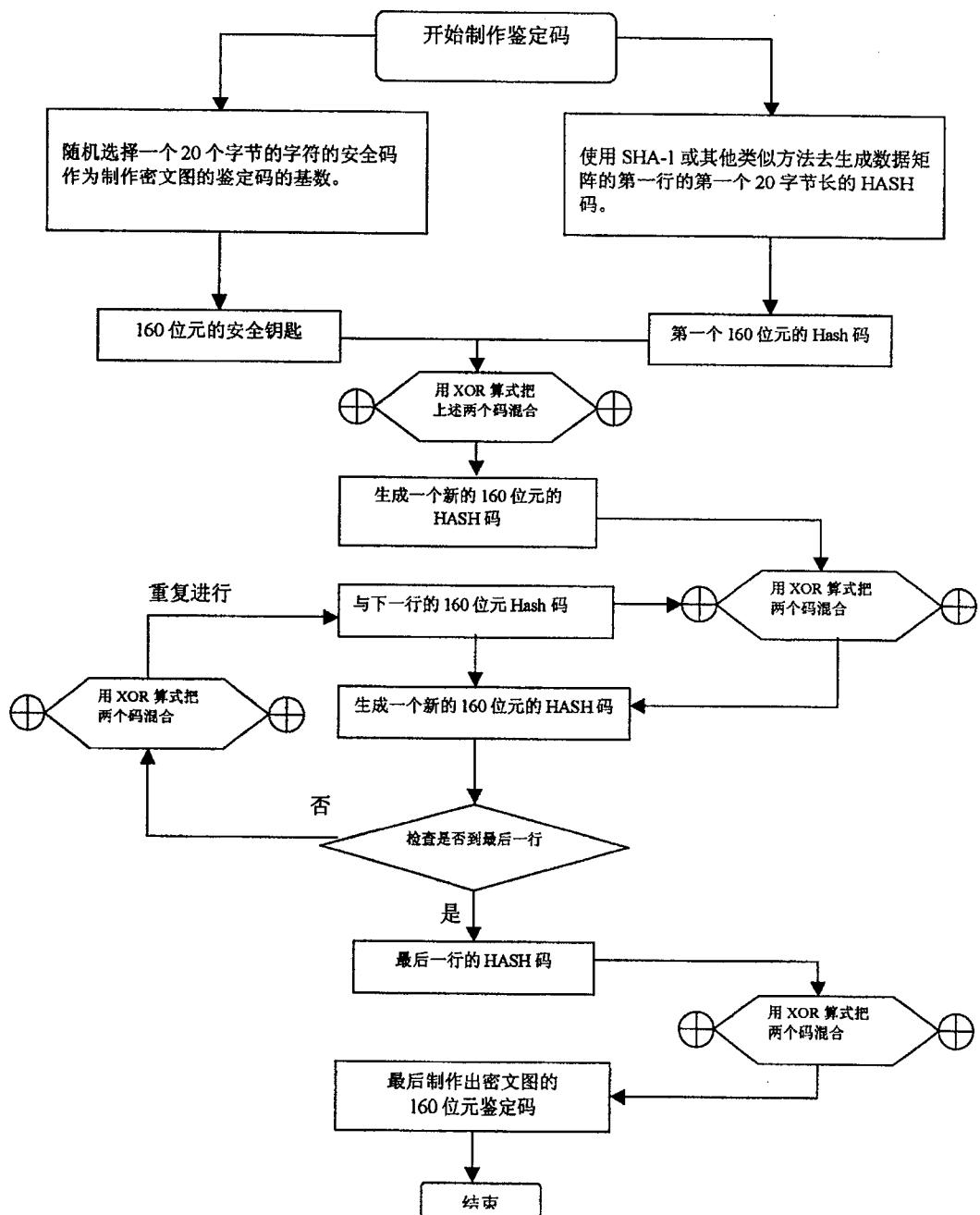
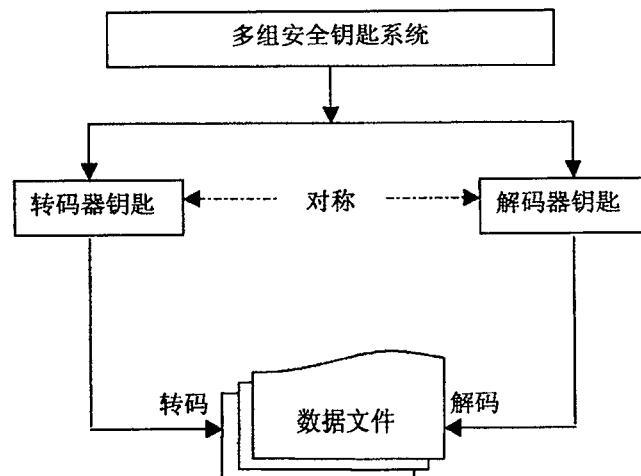
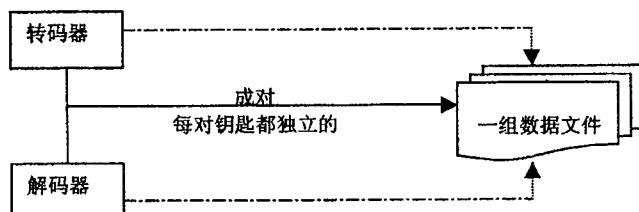


图 7

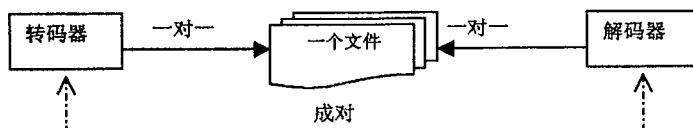
A. 多组转码器和解码器安全钥匙系统示意图



B. 一般使用的:一对多安全钥匙系统(基本设定)



C. 为高度机密的文件使用的:一对一的安全钥匙系统



D. 为防盗版等其他目的使用的: 联合安全钥匙系统

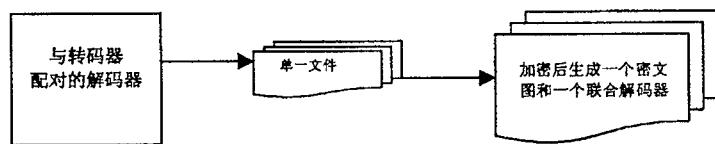


图 8

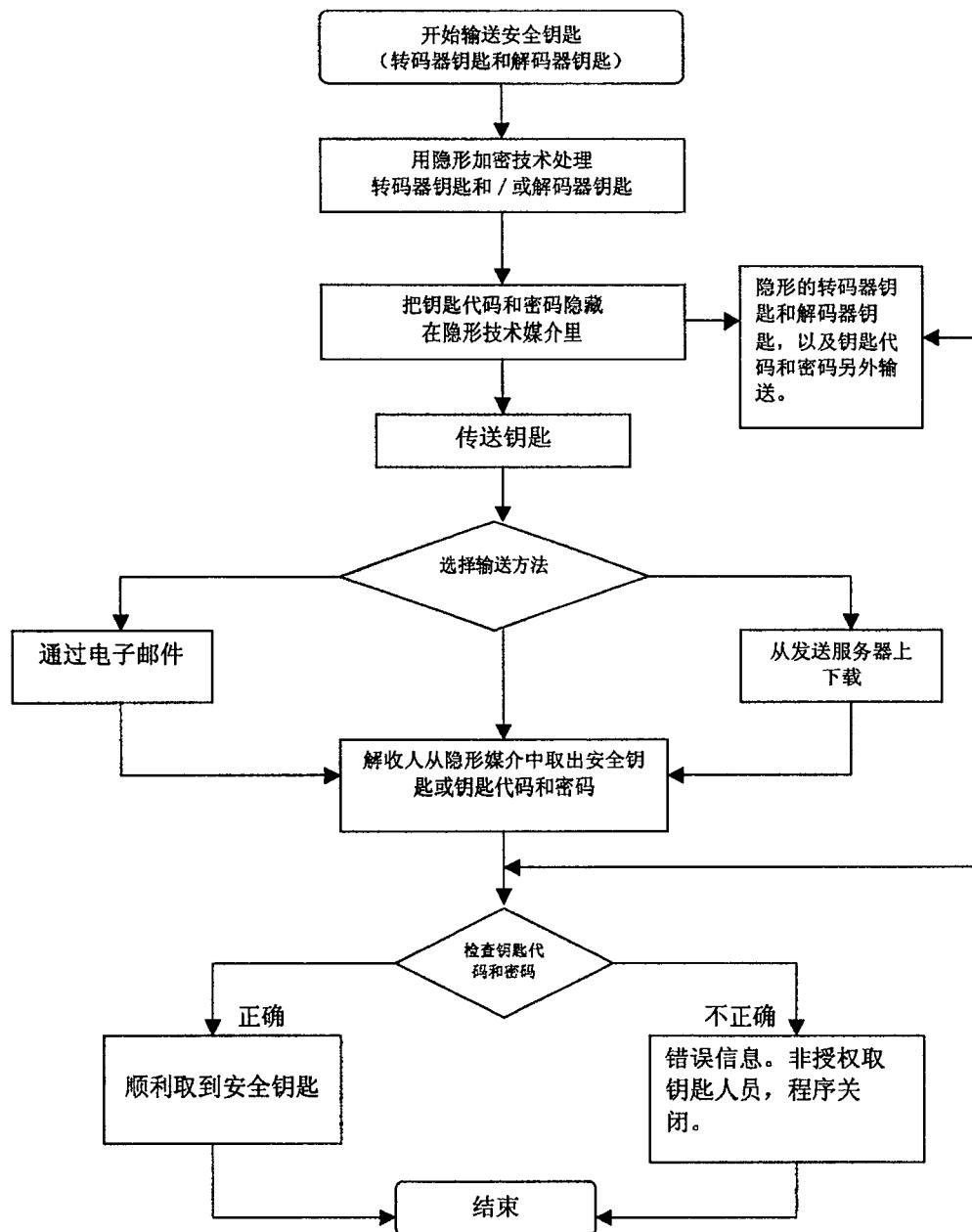


图 9

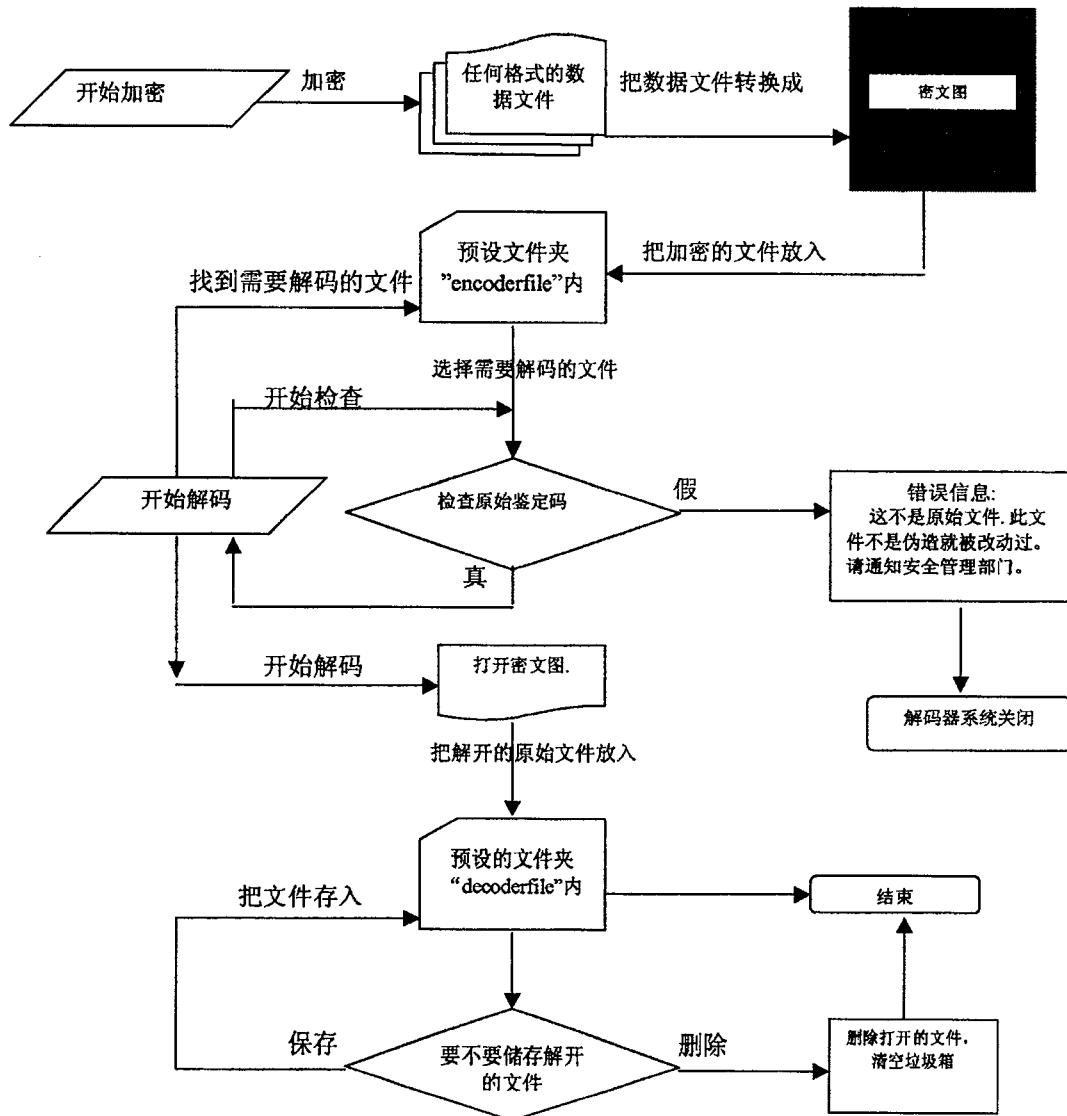


图 10