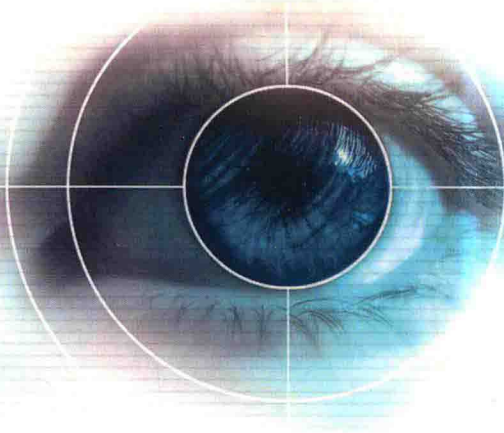
从眼透漏出的大脑秘密

基于视觉的身份识别技术



穆振东　金　玲　胡剑锋◎著

红旗出版社

从眼透漏出的大脑秘密——

基于视觉的身份识别技术

CONG YAN TOULOUCHU DE DANAO MIMI——

JI YU SHIJUE DE SHENFEN SHIBIE JISHU

穆振东　金　玲　胡剑锋　著

红旗出版社

红旗出版社
RED FLAG PRESS
推动进步的力量

图书在版编目（CIP）数据

从眼透漏出的大脑秘密：基于视觉的身份识别技术 /穆振东, 金玲, 胡剑锋著. —— 北京：红旗出版社，2016.3
ISBN 978-7-5051-3731-8
Ⅰ. ①从… Ⅱ. ①穆… ②金… ③胡… Ⅲ. ①身份认证—机器识别—安全技术 Ⅳ. ①TP391.4
中国版本图书馆CIP数据核字(2016)第045823号

书　　名　从眼透漏出的大脑秘密——基于视觉的身份识别技术
著　　者　穆振东　金　玲　胡剑锋
责任编辑　赵春霞　　装帧设计　宣是设计
出版发行　红旗出版社　　地　　址　北京市沙滩北街2号
邮政编码　100727　　编 辑 部　010-84017280
E - mail　hongqi1608@126.com
发 行 部　010-64024637
经　　销　全国新华书店
印　　刷　北京文良精锐印刷有限公司
开　　本　787毫米×1092毫米　1/16
字　　数　282千字　　印　　张　11
版　　次　2016年3月北京第1版　2016年3月北京第1次印刷
ISBN 978-7-5051-3731-8　定　　价　38.00元

欢迎品牌畅销图书项目合作　联系电话：010-84026619
凡购本书，如有缺页、倒页、脱页，本社发行部负责调换。

前　言

随着科学技术的发展，各种身份识别技术被伪造的成本越来越低，为保护自身财产和信息所设定的各种保密手段被攻破的可能性也大大提高。为了更好地保护自身财产和信息的安全，发展新的识别技术和手段也显得越来越重要。从最初的各种加密技术到后期利用各种生物的识别技术，都曾经被作为保护的最后屏障，但是现在，这些技术越来越不能满足人们对它们的期望。越来越多的伪造手段使得人们对这些现有的识别技术变得越来越失望。

从2006年至今，作者团队利用脑电信号做了很多研究，在对运动想象脑电信号进行研究的过程中，有人提出，不同的人对相同的想象模式会不会带有个体差异性，如果有差异性，那么这种差异性会不会影响识别率？带着这种想法，课题组开始了一系列的研究，研究结果表明，不同的人对相同的想象带有显著的个体差异性，我们定义这种差异性为“脑纹”。那么脑纹是否能作为身份识别的工具呢？脑电是一个弱点信号，这个“天赋”决定了脑电信号特征的不稳定性和不确定性，因此利用脑电信号作为身份识别工具具有很强的挑战性。

不同的人对自己的照片和对别人的照片，反应是不同的，这种不同会反射到脑电信号上，但是这种信号会不会随着人的不同而不同呢？本书以解决这个问题为目的，分别从不同的角度进行了阐述。

本书共分七章，第一章概述了身份识别的一些概念和评价体系；第二章和第三章分别介绍了密码和身份识别中常用的生物信号，并分析了它们的优、缺点；第四章介绍了脑电信号生物基础和分析方法，第五章介绍了基于运动想象的身份识别成果；第六章介绍了基于视觉的身份识别成果；第七章介绍了一个利用脑电信号的小型身份识别应用系统。

本书由穆振东、胡剑锋、尹晶海和金玲共同完成。其中第一章由胡剑锋同志编写，第二、三、四章和参考文献由金玲同志编写和整理，第五第六章由穆振东同志编写，第七章由尹晶海同志编写。本书由江西省科技厅发明专利产业化技术示范课题“No：20143BBM26048”和江西省科技厅科技支撑项目“基于移动平台的脑电信号方法库建设(No. 20151BBE50079)”资助。为了完成本书的编写，王平同志和闵建亮同志也都提供了不少的帮助，在此表示感谢。

编　者

目 录

第一章 绪 论

1.1 身份识别技术简述

身份识别技术是人们为了保护自身的财产和信息不被他人侵入而采取的自我保护的一种技术。从总体上来说，身份识别技术分为三大类——认证、识别和监控(图 1—1)。

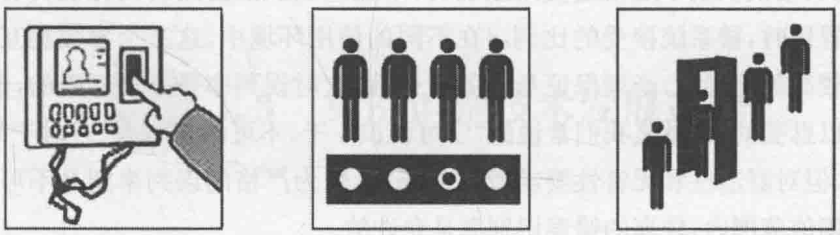


图 1—1 认证、识别和监控

认证是一对一的匹配过程，回答“这是否为某人?”的问题(判断题)。系统按照某一决策或匹配方式，判定待识别者身份的真实性，接受或拒绝待识别者声明的身份。

识别是一对多的匹配过程，回答“这是谁?”的问题(选择题)。系统将待识别信号参数与特征库中存储的所有已知身份的模板进行一一比较来决定待识别者的身份，通过在数据库中寻找与测试信号相似度最高的模板来完成对待识别者的识别。

监控同时具有识别和验证的功能，回答“这是否为要找的人?”的问题(问答题)。被测试对象可能在也可能不在特征库中。

身份识别技术是一个综合性技术，涉及信息技术、机械技术、数学、生物等，几乎涉及所有现行的学科。随着量子密码技术的提出，身份识别技术更是引申入分子层面。

身份识别研究过程中，最为重要的两个方面是身份识别所用工具和身份识别技术(算法)，其中身份识别工具是指在身份识别过程中，利用什么作为身份识别，如今的身份识别工具包括机械工具、电子工具、软件工具、密码工具、生物特征等多种，身份识别算法包括各种信号分析算法、数学算法、统计算法等。

1.2 身份识别技术特点

目前的身份识别技术有很多种，其中有利用硬件和软件实现身份识别的，有利用加密解密的密码技术的，也有通过指纹面孔等生物特征进行的。这些技术虽然各有千秋，但是可以被用来作为身份识别的技术都有相同的特点，主要可总结为几个方面：可用性、可靠性、稳定性、无害性和舒适性。

可用性：是指身份识别技术在被使用的环境下，必须满足使用的要求。在可用性上可以用三个参数来描述：正确识别率和错误识别率和误判率。正确识别率是指能够正确识别出使用者的比例；错误识别率是指当使用正确时，不能正确识别使用者的比例；误判率是指当别的使用者冒用时，被系统接受的比例。在不同的使用环境中，这三个参数相互制约，比如在安全性能较高的情况下，必须保证身份的安全性，这时误判率是不可忍受的，但是错误识别率却是可以忍受的，这就是我们常说的“宁可误识一千，不可漏识一人”。对于某些安全性能要求不高，但对舒适性和无害性要求较高的场所，较为严格的误判率则是不可接受的，只要在稳定的阈值范围内，较高的错误识别率是允许的。

可靠性：是指身份识别技术最终被用来进行身份识别的参数必须是能够真实地反映使用者身份的特征。可靠性是身份识别技术应用的基础，与识别技术采用的工具密不可分。身份识别技术最核心的技术是特征提取和分类识别。被提取的特征有些是非常容易提取的，而有些则是不容易提取的，但是并非容易提取的特征就是好的特征。一个身份识别技术是否可靠，可以用两个参数进行描述：特征数的数量和提取出特征所需样本数的多少。其中特征数是指为了进行身份识别，必须需要多少特征才能描述使用者；特征样本总数，是指为了能提取出特征，必须从多少个样本中进行提取，特征数量过多会影响身份识别的速度，同样样本总数过多，则说明特征提取过于困难。

稳定性：是指被用作身份识别的特征不能随着使用的环境、时间和状态的变化而变化。在身份识别技术发展之初，稳定性就是一个重要指标，就是基于这种指标之下，最初的钥匙就是以较难磨损的金属制成，例如铁、黄铜、合金等。如今的身份识别技术发展到了生物信息技术应用，例如指纹、面孔等，虽然相对而言特征较为稳定，但是随着年龄、状态、伤害等的发生，都会影响到身份识别的稳定性。

无害性：身份识别技术所采用的客体都是人，人身安全是目前国内外都非常重视的一个问题。因此身份识别所采用的技术必须是对人体无害的。例如在钥匙的选择上，就必须考虑到是否出现重金属污染，是否有放射性。当生物信息用于身份识别时，安全性更是被提升

到一个新的高度，因为各种基于生物信息的身份识别技术，所采用的特征都是从人体上采集，采集过程中是否会对人体造成伤害？如果造成了伤害，即使其他参数都非常好，也会被摒弃。例如曾经盛极一时的视网膜识别技术，因为视网膜在人体结构上位于眼球底部，因此必须用强度较高的红外光照亮人的眼底，但是这种照射是会伤害人的眼睛，因此，虽然这项技术被证明是非常好的身份识别技术，但是还是被摒弃了。

舒适性：当一个身份识别技术被证实，可靠性、稳定性、可用性和无害性都满足了相关技术的要求，但是如果每次使用时使用者都需要有极大的耐心和容忍度，强迫自己使用，那么这项技术肯定生命周期不长。随着经济的发展，人们使用各项技术的时候，对它的舒适性要求越来越高。身份识别技术的舒适性主要体现在两个方面：一方面是使用的便利性，主要体现在便于携带、不容易丢失和被盗等，这也是为什么要提出生物识别技术、为什么要把脑电信号引入身份识别技术中的原因；另一个方面是相应速度，当一个身份识别过程需要客户等很长时间时，客户会失去耐心而去使用其他技术。

1.3 身份识别技术发展过程

自从人类进入了奴隶社会，社会生产力的发展使得人们有了富裕的资产，在脱离了饥饿的威胁之后也带来了新的烦恼，那就是如何保护自己的财产不被别人盗取，这就开启了最初的身份识别技术。身份识别技术是跟随所需要保护对象的发展而发展的，最初所需要保护的对象仅仅是自己日常生活剩余的生活资料，例如工具、小饰品、食物等。这时候的技术仅仅是一扇门关住，一个绳子绑住避免别人看到，或者是一堵墙挡住等。随着剩余生活资料的增多，财产价值的增加，人们发明了很多新的身份识别技术来保护这些财产，锁和钥匙的出现就是身份识别技术发展的一个突破，后续很长时间内的身份识别技术都是基于这个技术之上发展起来的。

当财富的争抢演变为族群生存空间的争夺的时候，身份识别技术发展出了一个分支：密码技术，通过密码技术进行各种信息传递而不被敌人发现。在公元前 440 年的古希腊战争中，就出现了原始的密码技术——隐写术。当时为了安全传送军事情报，奴隶主剃光奴隶的头发，将情报写在奴隶的光头上，待头发长长后将奴隶送到另一个部落，再次剃光头发，原有的信息复现出来，从而实现这两个部落之间的秘密通信。公元前 400 年，斯巴达人发明了“塞塔式密码”，即把长条纸螺旋形地斜绕在一个多棱棒上，将文字沿棒的水平方向从左到右书写，写一个字旋转一下，写完一行再另起一行从左到右书写，直到写完。解下来后，纸条上的文字消息杂乱无章、无法理解，但将它绕在另一个同等尺寸的棒子上后，就能看到原始的

消息，这是最早的密码技术。同样，我国的密码技术发展也较早，例如，我国古代也早有以藏头诗、藏尾诗、漏格诗及绘画等形式，将要表达的真正意思或“密语”隐藏在诗文或画卷中，在特定位置记载，一般人只注意诗或画的表面意境，而不会去注意或很难发现隐藏其中的“话外之音”。例如，浪漫的秋香传说的藏头诗：

我画蓝江水悠悠，
爱晚亭上枫叶愁。
秋月溶溶照佛寺，
香烟袅袅绕经楼。

受到计算机和数学的发展和推动，一方面为加密技术提供了新的概念和工具，另一方面也给破译者提供了有力武器。计算机和电子学时代的到来给密码设计者带来了前所未有的自由，他们可以轻易地摆脱原先用铅笔和纸进行手工设计时易犯的错误，也不用再面对用电子机械方式实现的密码机的高额费用。总之，利用电子计算机可以设计出更为复杂的密码系统。

科技的发展不仅带动了身份识别技术的发展，也带动了破解身份识别技术的发展。再难的密码也存在被破解的可能性，因此人们开始寻求新的身份识别技术，这就促使了身份识别技术的第三次发展和突破，那就是选择人体的生物特征，例如指纹、虹膜等技术。

身份识别技术发展过程如图 1—2 所示。

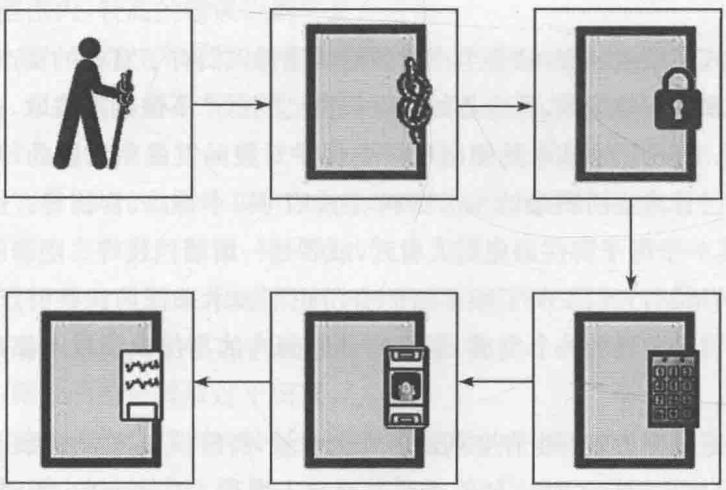


图 1—2　身份识别技术发展过程

同样基于伪造技术的发展和威胁，身份识别技术在越来越高的信息化浪潮中越来越难以胜任，如今的身份识别技术到了第四次发展和突破的阶段，需要寻求更加新颖的身份识别手段和工具。

第二章　传统的密码技术

2.1　密码技术简介

密码技术经历了从古典密码到现代密码的演变。许多古典密码虽然已经经受不住现代手段的攻击，但是它们对现代密码技术的研究是功不可没的，其思想至今仍然被广泛使用。随着计算机的出现，不论是在军事、外交、情报、商业，还是个人通信方面，运用计算机加密和解密技术都已经得到广泛的发展和应用。

密码技术是身份识别技术发展的一个里程碑。密码学是以保护通信的内容不被第三方窃取为目的的一门学科，通过利用一种用来混淆的技术，把原来的正常的信号变成一种无法识别的信息。

“自从有了文字，人们为了某种需要总是想方设法隐藏某些信息，以起到保证信息安全的目的。在这些神秘莫测的字符背后，或是隐含着政客那冷酷阴毒的计谋、武士那阴森滴血的剑影，或是携带着智者狡黠的微笑、情人绵绵不绝的秋波……可以说，密码是当一种文化在文学、科学和语言发达到一定的复杂程度，当秘密的、符号性的信息交流达到不可或缺的阶段时应运而生的一种信息交流的特殊工具。”①

密码通信的历史极为久远，其起源可以追溯到几千年前的埃及、巴比伦、古罗马和古希腊。古典密码术虽然不是起源于战争，但其发展成果却首先被用于战争。交战双方都为了保护自己的通信安全，窃取对方情报而研究出各种方法，这正是密码学主要包含的两部分内容：一是为保护自己的通信安全进行加密算法的设计和研究；二是为窃取对方情报而进行的密码分析，即密码破译技术。因而，密码学是这二矛盾的统一体。任何一种密码体制都包括5个要素：明文、密文、密钥、加密运算、解密运算及用户与对手。需要加密的消息称为明文；将明文变换成的不可懂的文本称为密文；密钥是一种参数，它是在明文转换为密文或将密文转换为明文的算法中输入的参数，密钥分为对称密钥与非对称密钥；采用某种方法将明文变为另一种不能被非授权者所理解的信息或字符串的过程称为加密变换；明文经加密过程变

① 杨旭刚，杨子涵。密码中的秘密[M]. 黑龙江科学技术出版社，2007。

成的信息或字符串称为密文；用于具体加密编码的参数称为密钥，将密文还原为明文的过程称为解密变换。

密码通信的过程可以用图 2—1 表示。

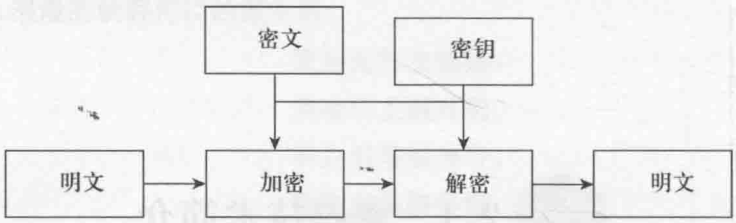


图 2—1　密码通信过程

用文字可以表述为：若 m 是要传送的明文，在传送前，利用密钥 k 将 m 经加密变换为密文 c，由通信通道发给接收者，接收者根据密钥 k' 利用解密变换将密文 c 变为明文 m。从以上过程可以看出，一个密码体制的安全性依赖于密钥 k 的个数和加密变换的复杂程度。密钥太少，敌方可以根据其截获的密文用不同的 k 逐个试译即可得到明文；密钥也不能太多，太多则不利于管理。加密变换太简单则容易找出解密变换，太复杂则导致解密过程耗费时间太多，不利于通信。

密码学的发展历程大致经历了三个阶段：古典密码、近代密码和现代密码(表 2—1)。

表 2—1　密码学发展的三个阶段

	起始时间	密码体制	通信手段
古典密码	从古代到 19 世纪末，长达几千年	纸、笔或者简单器械实现的替代及换位	信使
近代密码	从 20 世纪初到 20 世纪 50 年代，即第一次世界大战至第二次世界大战时期	手工或电动机械实现的复杂的替代及换位	电报通信
现代密码	从 20 世纪 50 年代至今	分组密码、序列密码以及公开密钥密码，有坚实的数学理论基础	无线通信、有线通信、计算机网络等

2.2　古典密码技术

在欧洲，公元前 405 年，斯巴达的将领莱杉德使用了原始的错乱密码；公元前 1 世纪，古

罗马皇帝恺撒曾使用有序的单表代替密码；之后逐步发展为密本、多表代替、加乱、离合诗技术、倒读隐语、语言隐写技术，还有漏格方法和俚语黑话等。这些方法已经体现了密码编码学中代替和换位的基本思想。

2.2.1　CASAR 体制

一种典型的加法密码。

密钥 $k=3$

明文字母和密文字母的对应关系见表 2—2。

表 2—2　明文字母和密文字母的对应关系

明文字母	a b c d e f g h i... w x y z
密文字母	w x y z c a i b d... r s u v

2.2.2　隐写术

隐写术是将秘密消息隐藏在其他消息中，这样，真正存在的秘密就被隐藏了。通常发送者写一篇无伤大雅的消息，然后在同一张纸中隐藏秘密消息。历史上的隐写方式有隐形墨水，用小针在选择的字符上刺小的针眼，在手写的字符之间留下细微差别，在打印字符上用铅笔做记号，除了几个字符外，大部分字符用格子盖起来，等等。

最近，人们在图像中隐藏秘密消息，用图像的每个字节的最不重要的比特代替消息比特。图像并没有怎么改变——大多数图像标准规定的颜色等级比人类眼睛能够觉察得到的要多得多——秘密消息却能够在接收端被剥离出来。用这种方法可在 1024×1024 bit 灰色刻度图片中存储 64 kb 的消息。能做此类加密的公开程序已有好几种。

Peter Wayner 的模拟函数也能使消息隐匿，这类函数能修改消息，使它的统计外形与一些其他东西相似，如《纽约时报》的题录部分、莎士比亚的戏剧、Internet 上的新闻组。这类隐写术愚弄不了普通人，但却可以愚弄那些为特定的消息而有目的地扫描 Internet 的大型计算机。

2.2.3　代替密码和换位密码

在计算机出现前，密码学是由基于字符的密码算法构成。不同的密码算法是字符之间互相代换或者是互相之间换位，好的密码算法是结合这两种方法，每次进行多次运算。现在事情变得复杂多了，但原理还是没变。重要的变化是算法对比特而不是对字母进行变换，实际上这只是字母表长度上的改变，从 26 个元素变为 2 个元素。大多数好的密码算法仍然是代替和换位的元素组合。

(1)代替密码

代替密码就是明文中每一个字符被替换成密文中的另一个字符。接收者对密文进行逆

替换即可恢复出明文。

在经典密码学中，有4种类型的代替密码。

①简单代替密码或单字母密码：就是明文的一个字符用相应的一个密文字符代替。报纸中的密报就是简单的代替密码。

②多名码代替密码：它与简单代替密码系统相似，唯一的不同是单个字符明文可以映射成密文的几个字符之一。例如A可能对应于5、13、25或56，B可能对应于7、19、31或42，等等。

③字母代替密码：字符块被成组加密，例如ABA可能对应于RTQ，ABB可能对应于SLL等。

④多表代替密码：由多个简单的代替密码构成，例如，可能有5个被使用的不同的简单代替密码，单独的一个字符用来改变明文的每个字符的位置。

著名的恺撒密码就是一种简单的代替密码，它的每一个明文字符都由其右边第3个(模26)字符代替(A由D代替，B由E代替……W由Z代替，X由A代替，Y由B代替，Z由C代替)。它实际上更简单，因为密文字符是明文字符的环移，并且不是任意置换。

ROT13是建在UNIX系统上的简单的加密程序，它也是简单的代替密码。在这种密码中，A被N代替，B被O代替等，每一个字母是环移13所对应的字母。用ROT13加密文件两遍便恢复出原始的文件：P=ROT13[ROT13(P)]。ROT13并非为保密而设计，它经常用在互联网Vsenet电子邮件中隐藏特定的内容，以避免泄露一个难题的解答等。

简单代替密码是很容易被破译的，因为它没有把明文的不同字母的出现频率掩盖起来。

多名码代替密码早在1401年由Duchy Mantua公司最先使用，这些密码比简单代替密码更难破译，但仍不能掩盖明文语言的所有统计特性，用已知明文攻击、破译这种密码非常容易，唯密文攻击要难一些，但在计算机上只需几秒钟。

字母代替密码是字母成组加密，普莱费尔在1854年发明了这种密码。在第一次世界大战中英国人就采用这种密码。字母成对加密，把Huffman编码用作密码，这是一种不安全的多字母代替密码。

多表代替密码由Leon Battista在1568年发明，在美国南北战争期间由联军使用。尽管容易被破译(特别是在计算机的帮助下)，但许多商用计算机保密产品都使用这种密码形式。维吉尼亚密码(第一次在1586年发表)和博福特密码均是多表代替密码的例子。

多表代替密码有多个单字母密钥，每一个密钥被用来加密一个明文字母。第一个密钥加密明文的第一个字母，第二个密钥加密明文的第二个字母，等等。在所有的密钥用完后，密钥再循环使用，若有20个单个字母密钥，那么每隔20个字母的明文都被同一密钥加密，这叫作密码的周期。在古典密码学中，密码周期越长越难破译，使用计算机就能够轻易破译具有很长周期的代替密码。

滚动密钥密码(有时叫书本密码)是多表代替密码的另一个例子，就是用一个文本去加

密另一个文本，即使这种密码的周期与文本一样长，它也是很容易被破译的。

(2)换位密码

在换位密码中，明文的字母保持相同，但顺序被打乱了。在简单的纵行换位密码中，明文以固定的宽度水平地写在一张图表纸上，密文按垂直方向读出，解密就是将密文按相同的宽度垂直地写在图表纸上，然后水平地读出明文。

2.3　近代密码技术

古典密码体制是在有线与无线通信技术产生后逐步兴起的，特别在军事斗争中，秘密的无线通信就显得格外重要。古典密码体制的典型例子有 CASER 加密体制和 PLAYFAIR 加密体制，其主要方法就是利用文字的代替和换位，有时还运用某些简单的数学运算。随着高速、大容量和自动化保密通信的要求，出现了机械与电路相结合的转轮加密设备，古典密码体制也就退出了历史舞台。

2.3.1　轮转机恩尼格马(Enigma)——密码学界划时代的丰碑

在 20 世纪 20 年代，人们发明了各种机械加密设备用来自动处理加密。大多数是基于转轮的概念，机械转轮用线连起来完成通常的密码代替。

转轮机有一个键盘和一系列转轮(图 2—2)，它是 Vigenere 密码的一种实现。每个转轮是字母的任意组合，有 26 个位置，能够完成一种简单代替。例如，一个转轮可能被用线连起来以完成用“F”代替“A”，用“U”代替“B”，用“L”代替“C”，等等，而且转轮的输出栓连接到相邻的输入栓。

图 2—2　转轮机