第 3 章　通信保密技术

保密通信已经有了几千年的历史，它最先用于政治和军事，进入信息时代后，通信保密不仅仅限于军事和政治，商业和个人隐私的保护使得保密通信成为越来越多人的基本需要。信息时代的军事、政治更依赖于保密通信，因为信息传送已成为现代信息战的重要一环。

通信保密技术包括数据保密通信、话音保密通信和图像保密通信。

3.1　保密通信的基本要求

保密通信的基本要求是：保密性、实时性、可用性和可控性。

1. 保密通信的保密性要求

通信的保密性指防止信息被非授权地泄露，包括通信的隐蔽性、通信对象的不确定性和抗破译能力。

1）通信的隐蔽性

要从通信中获得信息首先必须明确是否正在进行通信，如果不知是否正在通信，当然无法窃取通信中的信息。

2）通信对象的不确定性

窃密者虽然知道正在进行通信，但根本无法知道通信的双方是谁，这在技术上称为对抗业务流分析。

3）抗破译能力

虽然窃密者获得了通信信息，但是由于信息已被加密，窃密者不能破译信息的内容。

上述三种要求中，最基本的是抗破译性，其次是通信对象的不确定性，最后才是通信的隐蔽性。

2. 保密通信的实时性要求

保密通信可能会影响到通信的实时性，保密通信的实时性要求就是要把这个影响减少到最低程度，使传送的延迟时间越短越好。

例如对于实时性要求很强的电话业务，如果保密电话时延较大，一方的讲话过很久才传到对方，就违反了正常电话通信的方式，没有人会愿意使用。

又如活动图像通信，如果本来连续的画面，由于时延大，成了木头人一样不连贯的动作，即使保密性很好，也不能满足活动图像通信的要求。

3. 保密通信的可用性要求

可用性指合法使用者能方便迅速地使用保密通信系统，满足使用者要求的各种服务。

例如保密电话，合法使用者随时拿起话筒即可通话，不能使接通率下降，不能让使用者

过多地等待或进行过多的操作。

4. 保密通信的可控性要求

可控性要求指某些保密通信经过一定的法律法规批准后,可以由法律规定部门监听通信内容,避免犯罪分子利用保密通信进行犯罪活动,保护国家利益和人民利益,保证社会的安定。

3.2 数据保密通信

数据通信是把数据的处理和传输合为一体,以实现数字形式信息的接收、存储、处理和传输,并对信息流加以控制、校验和管理的一种通信形式。

数据通信与电话、电报通信方式的区别是:电话传送的是话音,电报传送的是文字或传真图像,而数据通信传送的是数据,即由一系列字母、数字和符号所表示的概念、命令等。在电话和电报通信中,通信双方都是人,而数据通信则是操作员使用终端设备,通过线路与远端的计算机,或计算机之间交换信息,其本质是机器之间的通信。

数据通信的加密可以通过下列方式实现:在数据传送前,对欲传送的信息进行加密或隐藏处理;在数据传送过程中,对传输信道和传输设备中传送的信息采用逐链加密、端端加密或混合方式加密。

3.2.1 网络通信保密技术

现代通信中数据通信大多呈现网络通信,网络通信保密技术是指根据网络的构成和通信的特点,根据应用环境的不同要求,将密码术加到计算机网络上的技术。其基本的保密技术就是加密,加密的方法包括:逐链加密、端端加密和混合方式加密。

1. 逐链加密

逐链加密在OSI的数据链路层实现。在数据传输的每一个节点上,对数据报文正文、路由信息、校验和等控制信息全部加密,每一个节点都必须有密码装置,以便解密、加密报文。

当数据报文传输到某个中间节点时,必须被解密以获得路由信息和校验和,进行路由选择和差错检测,然后再被加密,发送到下一个节点,直到数据报文到达目的节点为止。

在中间节点上的数据报文是以明文出现的,所以要求网络中的每一个中间节点都要配置安全单元(即信道加密机)。

由于报文和报头同时进行加密,有利于对抗业务流量分析。

2. 端端加密

数据在发送端被加密,在最终目的地(接收端)解密,中间节点不以明文的形式出现。

端端加密是在应用层完成的。除报头外的报文,均以密文形式贯穿于全部传输过程中。只是在发送端和接收端才有加解密设备,在任何中间节点报文均不解密,因此,不需要有密码设备。同逐链加密相比,可减少密码设备的数量。

另一方面,信息是由报头和报文组成的,报文是要传送的信息,报头是路由选择信息。

由于网络传输中涉及路由选择，在逐链加密时，报文和报头两者均须加密。而在端端加密时，由于通道上的每一个中间节点虽不对报文解密，但为将报文传送到目的地，必须检查路由选择信息，因此，只能加密报文，而不能对报头加密。

端端方式对整个网络系统采取保护措施，解决了在节点中数据是明文的缺点，但报头必定以明文形式出现，容易遭受业务流量分析。

3. 混合方式加密

采用逐链加密方式，从起点到终点，要经过许多中间节点，在每个节点均要转换为明文，如果链路上的某个节点安全防护比较薄弱，那么按照木桶原理(木桶水量由最低一块木板决定)，虽然采取了加密措施，但整个链路的安全只相当于最薄弱节点处的安全状况。

采用端端加密方式，由发送方加密报文，接收方解密报文，中间节点不必加解密，也就不需要密码装置。此外，加密可采用软件实现，使用起来很方便。在端端加密方式下，每对用户之间都存在一条虚拟的保密信道，每对用户共享密钥，所需的密钥总数等于用户对的数目。对于几个用户，若两两通信，共需密钥 $n(n-1)/2$ 个，每个用户需 $n-1$ 个密钥。这个数目将随网上通信用户的增加而增加。为安全起见，每隔一段时间还要更换密钥，有时甚至只能使用一次性密钥，密钥的用量很大。

逐链加密，每条物理链路上，不管用户多少，可使用一种密钥。在极端情况下，每个节点都与另外一个单独的节点相连，密钥的数目也只是 $n(n-1)/2$ 个。这里 n 是节点数而非用户数，一个节点一般有多个用户。

从身份认证角度看，逐链加密只能认证节点，而不是用户。使用节点 A 密钥的报文，仅仅保证它来自节点 A。报文可能来自 A 的任何用户，也可能来自另一个路过节点 A 的用户。因此逐链加密不能提供用户鉴别。端端加密对用户是可见的，可以看到加密后的结果，起点、终点很明确，可以进行用户认证。

总之，逐链加密对用户来说比较容易，使用的密钥较少，而端端加密比较灵活，用户可见。将两种加密方式结合起来，对于报头采用逐链方式进行加密，对于报文采用端端方式加密，称为混合方式加密。

3.2.2　信息隐藏技术

信息隐藏起源于古老的隐写术。在古希腊战争中，为了安全传送军事情报，奴隶主剃光奴隶的头发，将情报纹在奴隶的头皮上，待头发长长后再派出去传送消息。我国古代也早有以藏头诗、藏尾诗、漏格诗以及绘画等形式，将要表达的意思和“密语”隐藏在诗文或画卷中的特定位置，一般人只注意诗或画的表面意境，而不会去注意或破解隐藏其中的密语。

使用加密技术对信息进行加密，使得在信息传递过程中的非法拦截者无法从中获取机密信息，从而达到保密的目的。但这种方法有一个明显的不足：加密技术把一段有意义的明文信息转换成看起来没有意义的密文信息，它明确提示攻击者哪些是重要的信息，容易引起攻击者的注意，从根本上造成了一种不安全。即使攻击者破译失败，也可将信息破坏，使合法接收者无法阅读信息内容。

信息隐藏技术正是在上述背景下发展起来的，它将机密信息秘密隐藏于普通文件中，然后通过网络发送出去。非法拦截者从网络上拦截下的经伪装后的机密资料，并不像传统加

密过的文件那样是一堆乱码,而是看起来和其他非机密性的一般资料无异,因而容易欺骗非法拦截者。

信息隐藏技术作为一种新兴的信息安全技术已经在许多应用领域被使用,它主要的两个分支为隐秘术和数字水印,应用于 Internet 传输秘密信息时,被称为隐秘术;应用于版权保护时,被称为数字水印技术。

信息隐藏的目的不是限制正常的信息存取,而是保证隐藏的信息不引起攻击者的注意和重视,从而减少被侵犯的可能性,在此基础上再使用密码学中的经典方法来加强隐藏信息的安全性。

信息隐藏的方法是利用人类感觉器官的不敏感(感觉冗余)和多媒体数据中存在的冗余(数据特性冗余),将受保护信息隐藏在载体信息中,对外只表现载体信息的外部特征,而不改变载体信息的基本特征和使用价值。

替换系统是最常用的隐藏系统。基本的替换系统试图用秘密信息比特替换伪装载体中不重要的部分,以达到对秘密信息进行编码的目的。如果接收者知道秘密信息嵌入的位置,他就能提取出秘密信息。由于在嵌入过程中仅对不重要的部分进行修改,发送者可以假定这种修改不会引起攻击者的注意。

1. 基于文本的信息隐藏

在文本数据中隐藏秘密信息的方法可以将信息直接编码到文本内容中(利用语言的自然冗余性),或者将信息直接编码到文本格式中(如调整字间距或行间距等)。

【例 3-1】 使用 ByteShelter Ⅰ实现将秘密信息隐藏在 rich text 文本中。

(1) 运行 ByteShelter Ⅰ软件,界面如图 3-1 所示。

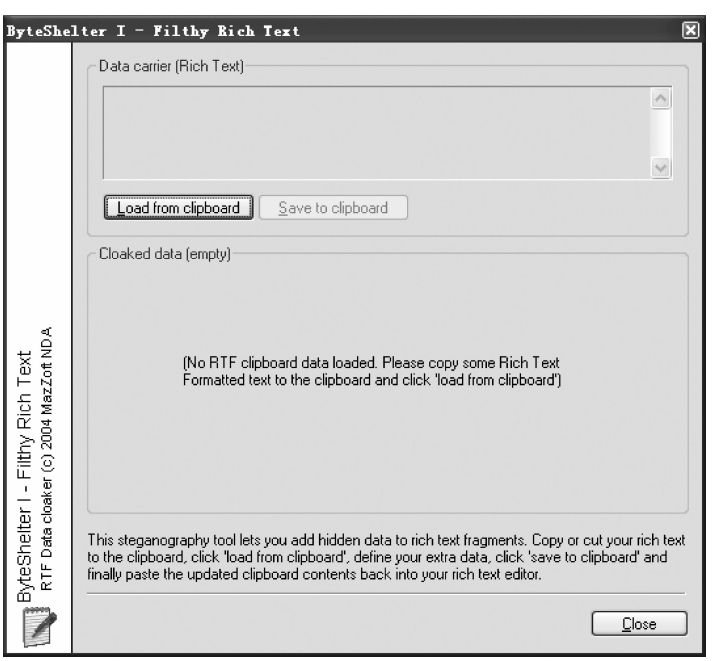


图 3-1 ByteShelter Ⅰ软件运行界面

（2）运行包含 rich text 的软件，如 Word，在其中输入任何文字，选中它们后复制到剪贴板。

（3）单击 Load from clipboard 按钮，出现如图 3-2 所示的 Password 对话框。

（4）输入密码，单击 OK 按钮，显示从剪贴板中粘贴的文字的字符数，如图 3-3 所示。

（5）在 Message 文本框中输入要隐藏的文本，注意输入的文本不能超出 Total cloaking space 中显示的长度。完成后单击 Save to clipboard 按钮，软件将要输入的信息隐藏在前面 Word 中输入的文字中，并复制到剪贴板中。

图 3-2　Password 对话框

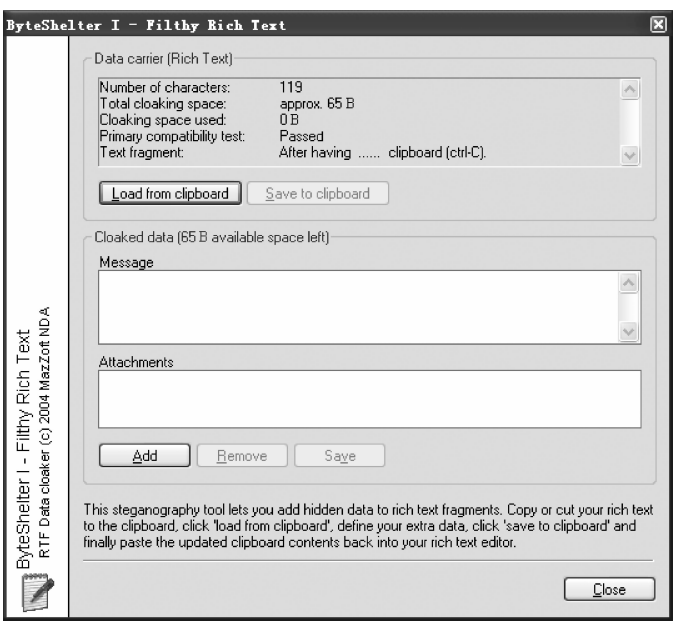


图 3-3　显示粘贴的字符数

（6）退出 ByteShelter Ⅰ软件。新建 Word 文件，粘贴剪贴板中的内容，保存该 Word 文件。

（7）要显示隐藏信息，则打开该 Word 文件，复制文本内容到剪贴板。运行 ByteShelter Ⅰ软件，单击 Load from clipboard 按钮，出现 Password 对话框，输入正确的密码，在 Message 文本框中自动显示隐藏的信息，如图 3-4 所示。

2. 基于图像的信息隐藏

图像和数字声音天然地包含各种噪声形式的冗余，可以将秘密信息放置在信号的噪声成分中，通过对秘密信息进行某种方式的编码，使它与真正的随机噪声不可区分，以实现信息隐藏。

【例 3-2】 使用 Easycode 将文本文件 test.txt 嵌入 test.jpg 文件中。

（1）运行 Easycode，单击“文件嵌入”选项。

（2）查看并记下 test.jpg 和 test.txt 文件的内容。

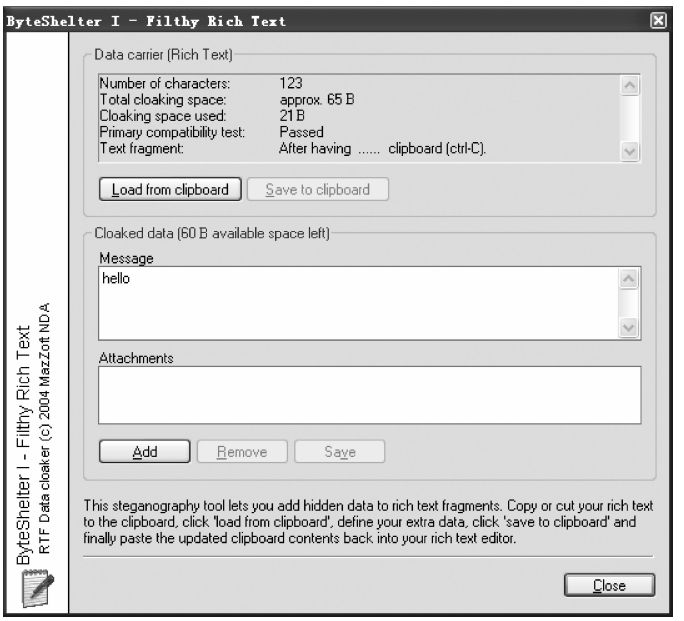


图 3-4　显示隐藏的文本内容

(3) 分别单击右上角的“浏览”按钮,选择寄主文件 test.jpg 和寄生文件 test.txt,在下方的“密码”文本框和“确认”文本框中输入密码,选中“嵌入后删除寄生文件”复选框,如图 3-5 所示。

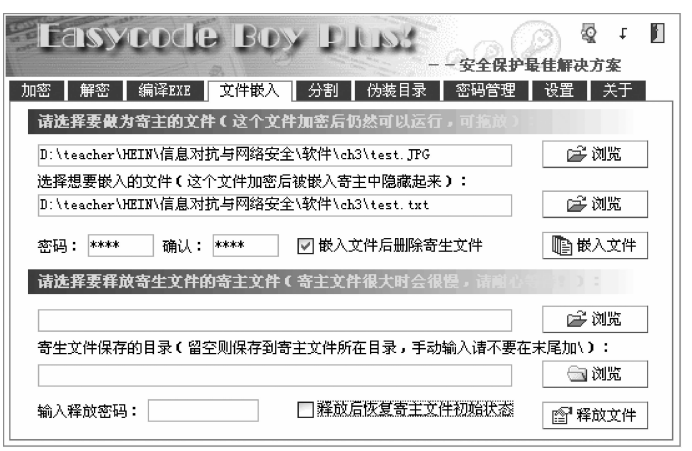


图 3-5　将文本文件嵌入到 jpg 文件中

(4) 单击“嵌入文件”按钮,出现如图 3-6 所示的对话框,表示 test.txt 文件已被嵌入 test.jpg 中。查看 test.txt 文件,发现已被删除。

(5) 分别查看嵌入文本文件前后的 jpg 文件,如图 3-7 所示,可以发现文件内容没有发生变化。

【例 3-3】 使用 Easycode 释放 test.jpg 文件中的寄生文件 test.txt。

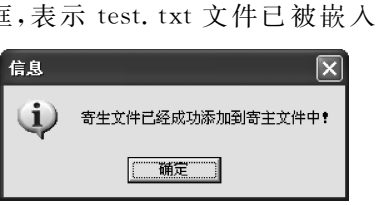


图 3-6　嵌入成功

(a) 嵌入前　　(b) 嵌入后

图 3-7　嵌入前后 jpg 文件的比较

(1) 运行 Easycode,单击“文件嵌入”选项。

(2) 单击右下角的“浏览”按钮,选择寄主文件 test.jpg,在下方的“输入释放密码”文本框中输入密码,选中“释放后恢复寄主文件初始状态”复选框,如图 3-8 所示。

图 3-8　释放文件

(3) 单击“释放文件”按钮,释放成功后,显示如图 3-9 所示的对话框。

(4) 打开 test.txt 文件,其内容与原来一致。

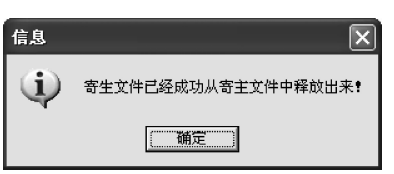


图 3-9　释放成功

3. 基于声音的信息隐藏

由于人类的听觉系统对声音的相位不敏感,因此可以根据这个事实将秘密数据隐藏在数字声音中。通常的做法是对音频信号进行快速傅里叶变换,通过修改相位值以插入秘密信息,将结果反变换到时域上即可得到伪装结果。

【例 3-4】 使用 MP3 Stego 将 WAV 文件压缩成 MP3 的过程中隐藏文本文件。

(1) 在命令行方式下执行以下命令:

```
encode -E hidden_text.txt -P pass svega.wav svega_stego.mp3
```

(2) 压缩 svega.wav 的过程如图 3-10 所示,压缩成功后将 hidden_text.txt 文件隐藏在 svega_stego.mp3 文件中。

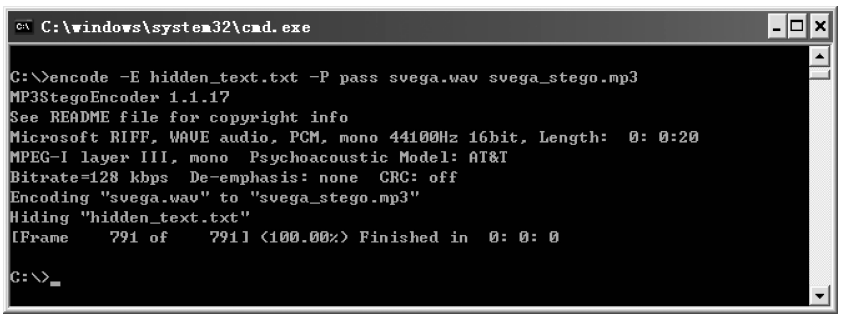


图 3-10 压缩声音文件时隐藏文本文件

(3) 要从 svega_stego.mp3 文件中释放隐藏的文本文件,执行命令:

```
decode -X -P pass svega_stego.mp3
```

(4) 释放过程如图 3-11 所示,释放出的文本文件名为 svega_stego.mp3.txt,内容与 hidden_text.txt 完全相同。

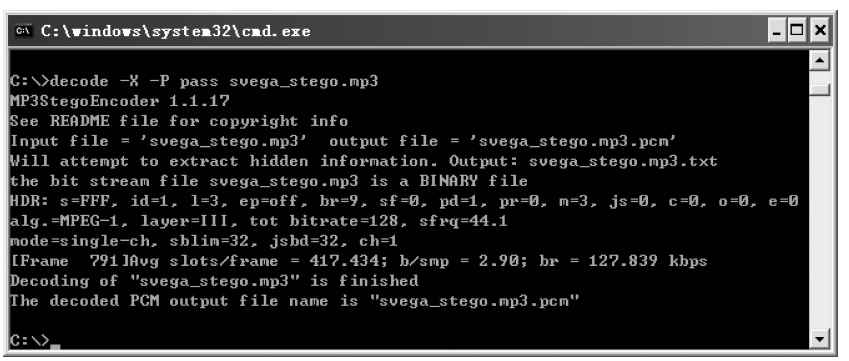


图 3-11 将隐藏的文本文件从 MP3 释放

4. 基于可执行文件的信息隐藏

可执行文件中也包含大量的冗余信息,可以通过安排独立的一串指令或者选择一个指令子集来隐藏数据。代码迷乱技术正是一种用于在可执行文件中隐藏信息的技术,该技术通过把一个程序 P 变换成一个功能等价的程序 P,实现将秘密信息隐藏在所用的变换序列中。

5. 隐藏信息的检测

信息隐藏技术的发展也带来了一定的负面效果,据美国媒体透露,已经发现恐怖组织利用隐藏在图像中的信息传递联络情报,甚至将计算机病毒隐藏在载体图像中进行传输,这些都对国家安全和社会稳定产生了很大的威胁。因此,研究对图像中可能存在的各种隐藏信息进行有效检测的方法已经迫在眉睫,基于图像的信息隐藏检测技术也就成为目前信息安全领域的重要研究课题。

近几年来,世界各国的信息安全专家在这一方面进行了深入的研究,并提出了一定的隐藏信息检测模型,开发了相关的信息隐藏检测软件,如美国著名的信息安全产品开发公司 Wetstone 开发的信息隐藏检测软件 Stego 套件。其中,Stego Watch 是一套隐藏信息自动

扫描软件，基本包括了所有常见图像格式和 WAV 声音格式文件的检测能力；Stego Analyst 是一款图像分析处理工具，针对 Stego Watch 发现的可疑图像，从视觉上进行细微的分析；Stego Break 是一套隐藏信息破解软件，以字典攻击的方式破解出一些最常用的隐藏信息工具埋藏于图片中的信息，支持对 JP Hide & Seek、F5、JSteg、Camouflage 等信息隐藏软件的破解。

StegDetect 是一款免费的隐藏检测软件，通过统计测试方法检测 JPEG 图像中是否被隐写，以及可能使用了何种隐写软件，如 JSteg、JPHide、OutGuess、Invisible Secrets、F5、appendX 和 Camouflage 等。

Stegdetect 的主要选项 t 用来设置要检测哪些隐写工具，可设置的选项如下：

j——检测图像中的信息是否是用 jsteg 嵌入的。

o——检测图像中的信息是否是用 outguess 嵌入的。

p——检测图像中的信息是否是用 jphide 嵌入的。

i——检测图像中的信息是否是用 invisible secrets 嵌入的。

如果检测结果显示该文件可能包含隐藏信息，那么 Stegdetect 会在检测结果后面使用 1～3 颗星来标识隐藏信息存在的可能性大小，3 颗星表示隐藏信息存在的可能性最大。

图 3-12 对于指定目录下的所有 JPG 文件进行检测，其中一幅图像没有隐藏信息，其余四幅图像通过 jphide 隐藏了信息。

图 3-12　免费的检测软件 Stegdetect

3.3　语音保密通信

语言交流是最基本、最方便的通信方式。早期无线电语音通信使用的防泄密手段主要是密语。为了实现密语通话，需要事先把可能用到的词汇编写成密语本，由话务员熟练记忆，正式通信时现场翻译。密语通信使用方便，实时性强，但密语中多少总要保留一些自然语言的结构，仔细分析便能猜出其中的意思，所以只能用在保密时效短、保密等级低的场合。

人的原始语音信号是一种模拟信号。受技术条件的限制，早期的保密电话和电台语音加密都直接针对模拟信号，通过改变语音信号的时间、频率、幅度特征使原来的话听不懂。例如把语音的频谱划分成若干个子带，重新排列它们的次序以达到置乱的效果。这种模拟加密体制的音质差、保密强度低，用专门的分析仪器可以破译，甚至经过特殊训练的话务员还能直接听懂部分模拟加密后的语音。

随着将模拟信号转换成数字信号再加密的新技术的出现，语音加密的音质、强度、实用性都大为改观。20 世纪 50 年代苏联研制的声码器保密电话，是一台用了大量电子管、代价昂贵的庞然大物，如今装在移动电话里的同样的保密机只用了一个小芯片。

随着通信手段的丰富与发展，特别是无线信道的大量使用，在通信过程中，收发双方交换的敏感信息被第三者感知的可能性大大增加。针对敌方可能采用的截收、窃听、破译、假

冒、侦听、测向手段,跳频技术、扩频技术的应用成为无线电通信防泄密的重要方向。当频带宽度扩展了数倍至数千倍后,信息将淹没在一片噪声中,从而实现以隐蔽方式对抗无线电侦听和干扰。

与过去相比,现在通信保密的技术、手段、措施、应用环境和使用要求都发生了很大的变化:从过去单一的电报加密发展到电话、传真、图像、电视会议等多种媒体加密;从单一的无线电加密发展到有线、无线、卫星、微波、散射等多种信道加密;从原始的手工密码发展到采用机械设备、电子设备、计算机进行加密作业;从点对点保密通信发展到网络化保密通信,并出现了通信保密技术与信息安全技术相融合的一体化趋势。

3.3.1 窃听与反窃听

窃听是指使用专用设备直接窃取目标的话音、图像等信息,从中获得情报的一种手段。随着科学技术的不断发展,窃听的含义早已超出隔墙偷听、截听电话等,它借助于技术设备和手段,不仅窃取语音信息,还窃取数据、文字、图像等信息。

窃听技术是窃听行动所使用的窃听设备和窃听方法的总称,它包括窃听器材,窃听信号的传输、保密、处理,窃听器的安装、使用以及与窃听相配合的信号截收等。

反窃听技术是指发现、查出窃听器并消除窃听行动的技术。

防窃听则是对抗敌方窃听活动,保护己方秘密的行为和技术手段。在可能被窃听的情况下,使窃听者得不到秘密信息的防范措施。

窃听技术的内涵非常广泛,特别是高档次的窃听设备或较大的窃听系统,包括了诸如信号的隐蔽和加密技术、信号调制与解调技术、网络技术、信号处理、语言识别、微电子、光电子技术等现代科学技术的很多领域。

窃听手段包括声音窃听、电话窃听和无线电波窃听。针对不同的窃听手段,也有针锋相对的反窃听技术。

1. 声音窃听——直接窃听法

声音窃听是一种古老的方法,它直接拾取从空气中传来的声波从而获得谈话内容。直接窃听法包括专线话筒窃听和无线窃听,间接窃听法包括口型分析法、激光窃听法和微波窃听法。

1) 专线话筒窃听

随着现代声音窃听技术的发展,出现了许多类似人耳功能的"电耳朵"。它们有的像黄豆粒或针尖那么小,有的做成和电源插座一样,拾音范围都在10m以上,连写字的声音都能听得一清二楚。把它们埋设在墙壁里或房间内,然后用一对导线将信号引出,窃听者就能听到室内的谈话,也可以用录音机记录。这种窃听方式叫作专线话筒窃听。

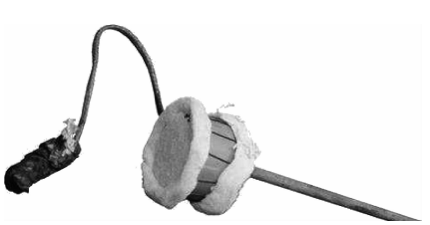


图3-13 窃听装置:电磁传声器

"电耳朵"的埋设方式要巧妙隐蔽:有的窃听话筒被安装在墙面的自然裂缝里;有的把连接话筒与放大器或录音机的金属导线沿着建筑物的钢骨架或其他金属管道敷设,在容易被肉眼察觉的地方则使用导电油漆代替导线。

图3-13是在冷战时期,美国驻东欧大使馆发现的电磁传声器,与扩音器相连的长木管能让它隐藏

在墙壁内，通过木管尾部的小针孔偷听房间里的谈话。

由于专线话筒窃听系统隐蔽、耐用、效果好，间谍把它作为窃听的主要工具。据美国反间谍机关的档案记载，1960 年以前，在美国驻苏联的大使馆内查获了 130 多个窃听器。1964 年春，美国的反窃听专家又在大使馆大楼的内墙里挖出了 40 个专线话筒。原来，1953 年苏联政府在帮助美国大使馆进行大楼改建时，就把这个专线话筒窃听网安装了进去。就这样，美国驻苏联大使馆在毫无察觉的情况下，向苏联克格勃“义务”提供了 10 年的情报。

如图 3-14 所示的是在美国华盛顿“国际间谍博物馆”中展出的从第二次世界大战末期到现在的窃听装置。从中可以看出，间谍使用的窃听装置的体积越来越小。

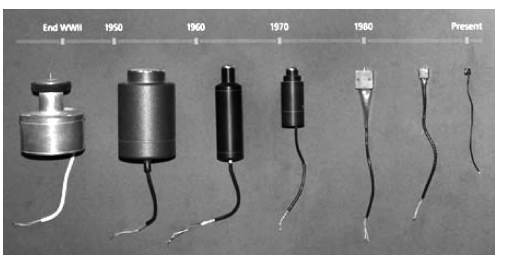


图 3-14　国际间谍博物馆中展示的窃听装置

对付专线话筒窃听，最简单的办法就是用肉眼看。细心检查墙上是否有裂缝和小孔，因为窃听话筒都要靠通向室内的洞眼拾取声音。而对于那些隐藏在墙壁深处的金属话筒或电源线，可以用金属探测器进行搜索。1964 年，联邦德国反窃听电子专家赫斯特·舒维尔克曼以外交官的身份到达联邦德国驻莫斯科大使馆。他很快就用金属探测器查出了克格勃所埋设的专线话筒窃听网。舒维尔克曼每查到一个窃听器，就用自己发明的仪器向话筒窃听线路里送进高压电脉冲，把正戴着耳机窃听的克格勃人员电得像被开水烫到的活虾一样乱跳。

2）无线窃听

无线窃听器体积小、重量轻，不需要敷设传输导线，可以在一个地区布设若干个，用一个接收机进行接收。它还可以做成子弹、炮弹，发射到敌人阵地里侦察动向。正因为如此，无线窃听器已经成为窃听最主要的工具。

随着微电子技术的发展，无线窃听技术水平得到了空前提高。

首先，无线窃听器体积的微型化程度越来越高。有的无线窃听器仅一粒米大小，伪装起来也更加巧妙，窃听器可以隐藏在钢笔、手表、打火机、鞋跟中，甚至人的器官也成了无线窃听器材的安装场所。日本就发生过这样一件事：一家银行为窃取某公司的财务情报，指使一名牙科医生利用该公司会计师镶牙的机会，把一个微型窃听器镶在他的假牙中，结果没几天功夫，这家银行就把会计室里谈论的秘密事项全部截获了。

图 3-15　树桩窃听器

如图 3-15 所示的树桩窃听器依靠太阳能，于 20 世纪 70 年代初期在莫斯科附近的森林地带不间断从事窃听。它截获了往来于苏联在该地区的空军基地的通信信号，将信号发送给一颗卫星，再由卫星将情报转发给美国境内的情报分析中心。由于依靠太阳能驱动，树桩窃听器就不存在更换电池的必要性。

其次，窃听器的自我保护功能大大加强。档次高的无线窃听器大多有遥控功能，当发现有人检查窃听器时，可以让窃听器停止工作。有的窃听器还采取了加密措施，加密

后的无线电信号,一旦被搜索到也只是一片噪声或交流声,难以判断是否是无线窃听器发出的信号。有的还把无线窃听器做成“枪弹”,用特制的枪械射到目标住所的窗框上或墙壁上,窃听器有吸附装置,可以牢固地吸附在物体上,安装方便也很隐蔽,不易被人察觉。

图 3-16 便携式窃听手枪

德国 PK 电子器材公司公开出售的一种微型无线窃听器只有 6g,用一节 1.5V 的纽扣电池可连续工作 12 小时。它的体积很小,通过如图 3-16 所示的便携式窃听手枪将其射到房间的窗户旁,使其牢固贴附在墙上,可以把窃听到的谈话声用无线电波发送到一二百米外。

下面是两个无线窃听的例子——会偷听的“鸟枪”和鞋跟里的“间谍”。

(1) 会偷听的“鸟枪”。

在某国的一个公园内,游客们散步、骑马、划船,尽情享受大自然的恩赐。在湖边的灌木丛中,一枝乌黑的“鸟枪”架在三脚架上,枪口始终瞄着湖心的一条划艇,那上面有对似乎在热恋中的男女正在交谈。守在“鸟枪”旁的两个男子则聚精会神地戴着耳机。直到划艇上的男女上了岸,两个男子才收起“鸟枪”悄悄离去。原来,他们是该国反间谍机关的侦探。利用“鸟枪”,他们偷听了男女间谍在划艇上的全部对话。

这里的“鸟枪”是一种“追捕”声音的设备——远距离定向话筒窃听器。借助这种窃听器,可以听到几百米甚至更远的声音。它的工作原理和扩音机的原理差不多,只是其话筒体积要小得多、灵敏度要高得多。“鸟枪”枪管上有规律地开有许多小孔,当声波从正前方传来时,经过小孔进入枪管就会增强,而当其他声波从枪管两侧传来时,穿过小孔就会互相抵消。远距离定向话筒窃听器还有做成抛物面形或喇叭形的,主要设立在两国对峙的边界线或军事分界线上。

(2) 鞋跟里的“间谍”。

一天早晨,某国大使馆的保安人员用无线电搜索机做例行检查时,突然收到了大使同别人的谈话声。根据电波的方向,保安人员来到大使的办公室,递上一张纸条:“请您走出办公室并继续谈话,但是要小心讲话的内容,因为您正在被窃听。”大使走出办公室,但搜索机里仍然响着他的声音。这说明窃听器就在大使身上。保安人员围着大使检查了好久,直到最后脱下了他的皮鞋才发现,原来窃听器就藏在大使的皮鞋后跟里。

大使皮鞋里的窃听器是一种无线窃听器,如图 3-17 所示。它所窃取的声音是通过无线电波传送到窃听接收机的。在无线窃听器里,除了有话筒,还有把微弱信号功率放大的电子线路以及发射天线和电池。

图 3-17 鞋跟窃听器

2. 声音窃听——间接窃听法

以上的方法都是直接窃听,还有一些间接窃听的方法,如口型分析法、激光窃听法和微波窃听法。

1) 口型分析法

在有些场合下能够看到讲话者却听不见他的声音,这时就可以用带有长焦距的摄像机拍下讲话者的

口型和手势，然后用口型分析法“看出”他的声音。事实上，许多聋哑人就是用这种方法来理解别人的语言内容的。对于一个长期接受这方面训练的特工来说，同样可以做到。有时几个特工合作，甚至能把讲话内容一字不差地还原出来，他们被称为“唇读间谍”。

2）激光窃听法

激光窃听法则是利用激光发生器产生一束极细的激光，射到被窃听房间的玻璃上。当房内有人谈话时，窗玻璃会随声波发生轻微震动，而玻璃同时又能对激光有一定的反射效应。如果用一束激光发射到玻璃窗上，室内的谈话声就会在反射回来的激光中反映出来，经过激光接收器的接收，再经过解调放大，就能将室内的谈话声音录制下来。这种窃听器最大的优点是不需要在目标房内安装任何东西，作用距离可达 300～500m。图 3-18 是激光窃听系统示意图，图 3-19 是激光窃听装置。

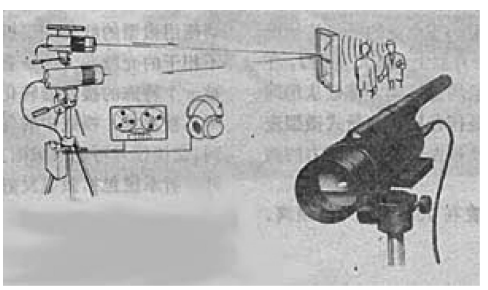


图 3-18　激光窃听系统

图 3-19　激光窃听装置

在海湾战争中，美国人就曾使用了激光窃听技术，从伊拉克高级将领座车的反光镜上，窃听到了车内的谈话内容。

3）微波窃听法

有些物体如玻璃、空心钢管等被制成一定形状后，既能对说话的声波有良好的振动效果，又能对微波有良好的反射效应。一些情报机构利用物体的这种特性，进行微波窃听。如果把这种物体巧妙地放在目标房内，在一定距离外向它们发射微波，这些物体反射回来的微波中就会包含房内话音的成分，用微波接收机接收并解调后，就能获得目标在房内讲话的内容。

微波窃听法的原理同激光窃听法比较相似，但微波的方向性不如激光那样强，它的反射波在一定区域内都可以收到，所以窃听者可以躲藏在被窃听房间周围的许多地方。1945 年，莫斯科向美国大使哈里曼赠送了一件珍贵的礼物——一个雕刻非常精致的美国国徽，如图 3-20 所示。哈里曼把国徽悬挂在书房里，他总是习惯在这里和人密谈。哈里曼并不知道国徽里藏了一个微波反射器，声波会激起它的振动。苏联特工就在与美国使馆一街之隔的房子里向国徽发射比较强的微波，同时用一个灵敏度很高的微波接收机接收反射回来的微波，从而窃听美国大使在书房里的谈话。这个秘密活动一直到 1952 年才被发现。

3. 无线窃听的预防

为了预防无线窃听，一些国家的重要机构专门采用一种“笼子”办公室来谈论机密。所谓“笼子”，就是安装在房间中央的一个特制的小房间，它的四周用金属网屏蔽，地板用绝缘体隔绝，照明电也经过滤波，以防止电波进入或泄出。“笼子”内部没有任何装饰，家具都是透明的，一放窃听器就露馅。

图 3-20 国徽中的微波窃听器

使用灵敏度较高的无线电全波侦测接收机能检查无线窃听,包括无线窃听报警器、无线窃听器探测仪、PN结探测器。

1) 无线窃听报警器

超小型无线窃听报警器,实质是一种袖珍式场强计,如图3-21所示。当最近的无线发射机在任何频率上工作时,报警器发出闪光信号或产生轻微的震动。这种报警器体积很小,携带方便,可以伪装在各种日常用品中,如香烟、笔记本、手表、笔架等。缺点是任何当地无线电台的电磁场都可能引起它的报警,容易产生虚报。

2) 无线窃听器探测仪

这种接收机能在20kHz～1000MHz或30～1500MHz的范围内进行全频段的慢速扫描或快速扫描,有的接收机分好几挡速度供挑选。设定速度后接收机自动扫描搜索,当房内有工作着的无线窃听器时,接收机扫到与窃听器工作频率相同的频率,报警信号灯亮并发出报警声。然后用手持探测器进行寻找,当探测器接近窃听器所在位置时,声调发生变化,表示此处隐藏有窃听器。这种探测器通常装在一个标准的手提箱内,手提或肩背都很方便,如图3-22所示。

图 3-21 无线窃听报警器

图 3-22 无线窃听器探测仪

3）PN 结探测器

如图 3-23 所示的是非线性结探测器，这种探测器可探测不工作的无线窃听器，也可探测包含晶体管或集成电路块，即含有 PN 结元器件的各种窃听器。

它工作时，发送一个低电平微波束，当遇到任何二极管、三极管或集成电路等 PN 结元器件时，产生反射波，并在反射波中出现谐波分量，可探测到隐藏到墙壁、家具、天花板内几十厘米处的窃听器。它的缺点是如果窃听器隐藏在电器中，则探测器区别不出是窃听器中的 PN 结器件，还是电器中的 PN 结器件。

图 3-23　非线性结探测器

4. 激光窃听的预防

预防激光窃听的方法有很多，从原理上讲主要掌握以下两个要素：防止激光射入目标房间的窗玻璃上、破坏反射体随声音的正常振动。

具体方法有：

（1）在玻璃窗外加一层百叶窗或其他能阻挡激光的物体。

（2）窗玻璃改用异形玻璃，异形玻璃表面不平滑，不影响透光，但使散射回去的激光无法接收。

（3）将窗玻璃装成一定角度，使入射的激光束反射到附近的地面。

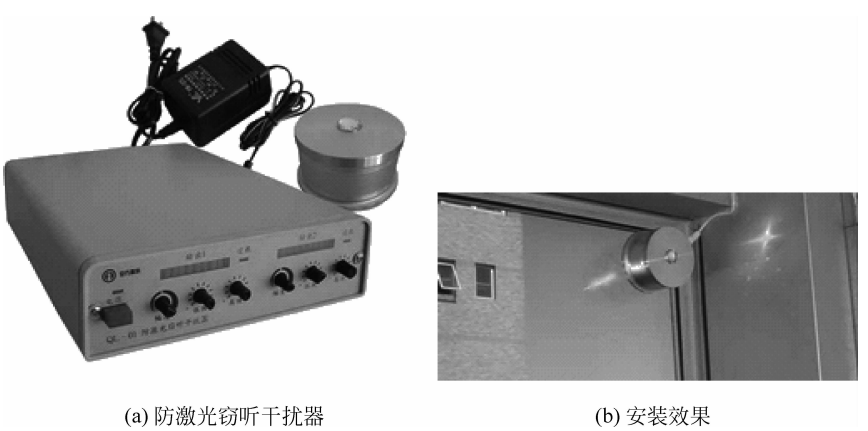
（4）窗户配上足够厚的玻璃，使之难以与声音共振。

（5）将压电体或电机的音频噪声源贴在窗玻璃上或置于窗户的附近，使噪声附加在反射光束上。

（6）谈话时室内放录音（最好是在公共场所录的嘈杂音），将谈话声淹没在杂声中。这一措施对防止其他手段的窃听也是有用的。

（7）用激光探测器探测室内是否存在激光，如果室内有超量的激光强度时就发出警报信号。

如图 3-24 所示的防激光窃听干扰器可产生频带、强度可调的随机混合声波，对谈话现场声波引起的玻璃振动进行掩蔽干扰，阻断窃听源，确保重要房间内话音内容不会遭受激光窃听干扰器的窃收。



(a) 防激光窃听干扰器　　(b) 安装效果

图 3-24　防激光窃听干扰器（玻璃振动干扰）

5. 电话窃听

电话窃听的手段很多,常用的有:

(1) 通过电话交换机控制用户电话。

这种电话窃听系统很大,自动化程度很高,只要目标电话一使用,监听设备立即起动实施窃听,始叫话机的号码、通信的日期和时间也同时被自动记录下来。

(2) 利用电话线路的串音窃听。

由于电话线、变压器或其他线路元件并置后,电磁感应造成一路电话线上可能感应另一路电话线上的电话信号。对于技术质量比较差的通信线路,如采用架空明线或质量差的通信电缆,有时两条线路只要有几十厘米长的间隔相互平行,就能产生足够强的串音。这种串音有时直接听不出来,但用放大器放大便可听清楚。早期有些国家的情报机关利用这种特性设计制造串音窃听器,提供给他们秘密派往国外的间谍使用。这些间谍在居住地把电话串音窃听器跨接在电话线上,窃听与此线平行的其他线路里的通话声。

随着通信线路及通信设备质量的不断提高,特别是优质通信电缆及光纤电缆替代了架空明线,给串音窃听增加了困难。

(3) 在电话系统里安装窃听器件。

用得比较多的是落入式电话窃听器。这种窃听器可以当作标准送话器使用,用户不易察觉。它的电源取自电话线,并以电话线作天线,当用户拿起话机通话时,它就将通话内容用无线电波方式传输给几百米外的接收机。这种窃听器安装非常方便,从取下正常的送话器到换上窃听器,只要几十秒钟时间。可以以检修电话为由,潜入用户室内安装或卸下这种窃听器。

还有一种米粒大小的窃听电话发射机。将它装在电话机内或者电话线上,肉眼观察很难发现。这种窃听器平时不工作,只有打电话时才工作。20世纪70年代轰动世界的美国“水门事件”就是使用这类电话窃听器,如图3-25所示。

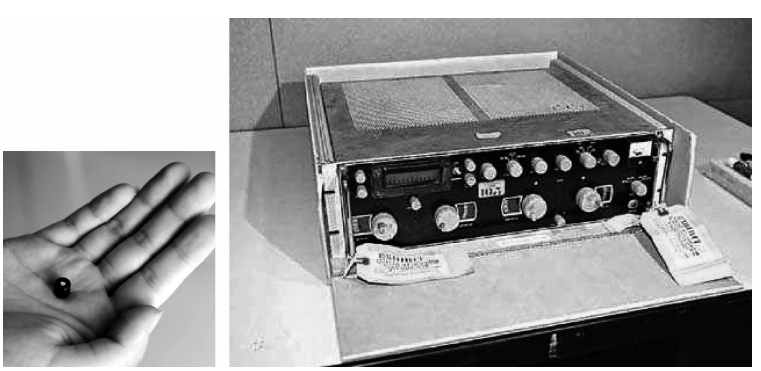


图3-25 水门事件中的窃听器和接收器

在架空明线上安装两只伪装成绝缘瓷瓶的窃听器,跨接在电话线路上,其中一只装有窃听感应器、发射机和蓄电池,另一只装有窃听感应器和蓄电池。当线路上电话、电报、传真信号经过两个窃听感应器时,将感应的信号送到发射机,通过固定在架线杆顶部的天线将信号发射出去,被约一千米外的接收机所接收。由于蓄电池是太阳能电源,所以能长期使用。

(4) 利用电话系统的某一部分窃听房内谈话。

利用电话系统的某一部分窃听房内谈话，也是国外广泛使用的一种窃听技术。用得比较多的是谐波窃听器，它是一个由音调控制的话筒形状装置。窃听者可以利用另一部电话，对目标房间的电话进行遥控。当目标电话中的谐波窃听器收到遥控信号后，便自动启动窃听器，窃听者就可以在远离目标房间的另一部电话中，窃听目标房间的谈话内容。

6. 电话反窃听

防电话窃听的方法有：电话窃听报警器、电话分析仪、采取语音保密技术等。

1) 电话窃听报警器

电话窃听报警器可以对装在电话系统中的窃听器发出报警信号。其基本原理是测试电话线的线电压，与正常的参数相比较，如原线电压为 13V，分线盒前或分线盒后串接窃听器后，线电压就降至 6V，报警器产生报警信号。这种报警器除有报警指示灯外，还有数字读出的电压表。可以 24 小时监视电话系统，也可连接录音机将被窃听的话音记录下来，如图 3-26 所示。

还有一种防窃听电话，本身带有窃听报警装置。此装置利用电话机中的电源，对电话机周围进行无线电波监测，一旦有无线窃听器工作，它就发出报警信号。这种电话机外表与普通电话机一样，不影响正常通话，使用方便。

2) 电话分析仪

如图 3-27 所示的电话分析仪能够测试电话系统中挂钩或脱钩时的阻抗、电压、电流，检测有无射频辐射、有无谐波窃听器。例如在电话系统中任何地方插入窃听器件时要切断电话线，这时它就会发出报警信号。

图 3-26　固定电话窃听报警器

图 3-27　电话分析仪

3) 采取语音保密技术

以上方式都是被动反窃听，在现实生活中人们还可以主动反窃听，即使用话音保密器。

话音保密器是加装在电话机上的附属设备，当人们拿起电话通话时，它会首先对话音信号进行加密，再传输给对方。在对方的话机上，最先收到信号的也是保密器。它把信号解密后再送入听筒里。也就是说，用户虽然讲的是明话，但在线路上传递的却是没人能听懂的密语，因而能有效防止窃听。如图 3-28 所示的是布什总统使用的带有话音保密器的防窃听电话机。

目前还出现了一种“数字化话音保密通信”，由话音保密器把语音信号数字化，然后将它们与近似随机的一串信号结合在一起，变成一种似乎没有规律的加密电码，这种方法非常适合现代战争的通信保密。

图 3-28 防窃听电话机

7. 无线电波窃听

由于无线通信是以电磁波在空间传播的，窃听无线通信比窃听有线通信更容易、更安全。因此，一些国家把窃取目标国的无线通信秘密，作为获取政治、军事、经济、科技情报的重要手段，不惜投入大量的人力、物力和财力，在全球范围内，建立起现代化的立体侦听系统。

无线电波窃听的方法主要有：

1) 地面侦听站

在本国或外国使领馆、派出机构建立大型侦听基地和侦听站，在陆地截收无线电信号，并进行分析处理，获取情报。

2) 空间侦察卫星

如图 3-29 所示的空间侦查卫星，利用卫星上的电子侦听设备对空中电磁波信号进行截收。由于卫星具有位置高、无线增益高、侦察面积大、飞行速度快和侦察合法化等特点，能成功侦听地面所有强弱无线电通信信号。

图 3-29 空间侦察卫星

1996 年 4 月 21 日，车臣总统杜达耶夫的卫星电话频率被俄情报机构的无线电测向定位监听到，并连续三次确定杜达耶夫的通话位置后，俄罗斯立即发射了空对地导弹，准确击中了杜的密巢，误差仅几米，杜当即丧命。

2001 年 11 月中旬，由于反塔联盟攻占马扎里沙夫，塔利班撤出喀布尔。这时，美国的间谍卫星和侦察机几乎同时发现，在溃败的人群中有一支特别的部队。当这支特别的部队停驻在一个小镇的旅店时，美军司令部下达了消灭目标的命令。伴随着巨大的爆炸声，旅店

燃起了熊熊大火。数小时后，美国中情局从监视的目标通信中截听并破译了一个从阿富汗发出的卫星电话信号，得知拉登基地组织的多名高层领导在这次攻击中丧生，其中包括拉登的副手阿提夫。

3）间谍船

通过在船上安装电子侦听设备，在近海或目标附近侦听截收各种无线电通信信号，此外还可以窃取海底通信电缆的信号。图 3-30 为美国“普韦布洛号”武装间谍船中的侦听设备。

图 3-30　间谍船中的侦听设备

4）间谍飞机

在军用、民用或无人驾驶飞机上安装先进的电子和通信侦听设备，截收空中电磁信号。图 3-31 是著名的间谍飞机 U-2 驾驶舱。

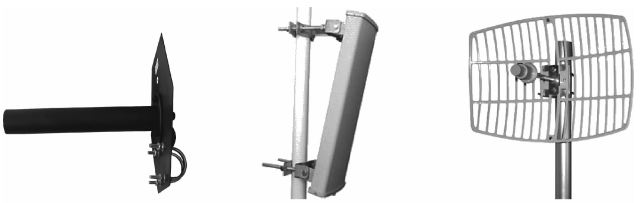
图 3-31　间谍飞机

8. 无线电波反窃听

防止窃听者截收无线电波是反窃听的一项重要手段，它的目的是让窃听者的“耳朵”听不到、听不全或听走耳，包括：

1) 定向通信

无线电波在空中传播时就好像水面激起波纹,四面扩散。但有些特殊形状的天线和特殊形式的电波却只能向一个方向扩散,如定向性很好的激光。这样,人们就可以限制无线电波的传输方向,只对着己方接收机发射,让窃听的接收机截收不到。即使窃听者掌握了目标的通信方向,其截收天线势必阻挡电波,导致通信中断而无法窃听。如图3-32所示的是各类定向天线。



(a) 螺旋定向天线 (b) 双极化定向天线 (c) 栅格定向天线

图3-32 定向天线

2) 快速通信

快速通信是指在通信前,发方和收方同时做好准备,突然将简要的情报发出去,窃听者因毫无准备来不及截收。1978年,伊朗就发生了一起通信间谍案。伊朗陆军少将阿赫默德·莫格勒比是克格勃发展的特务。苏联大使馆领事鲍里斯·卡巴诺夫经常开着小汽车经过他住宅前的马路。每次进入马路路口时,卡巴诺夫就按动座位下的开关,发出一个无线电遥控信号。信号打开莫格勒比家中的快速收发报机,使其预先记录在磁带上的情报快速发出,由汽车上的接收机记录下来。整个过程在卡巴诺夫离开这条马路时完成。伊朗反间谍机关一直暗中跟踪卡巴诺夫,但每次都觉得他没有"作案时间",竟让其在眼皮底下窃取了4年的情报。

3) 跳频通信

一般电台的工作频率是固定的,窃听者找到这个频率就可以截收通信信号。针对这一点,目前一些国家采用频率捷变的方法,通信时发收双方的频率都按照约定的规律同步快速跳变,使窃听者无法捕捉,即使偶然碰上一个频率,它又很快跳到别的频率上了。

4) 伪装通信

对于窃听者来说,如果截收到的无线电波虚实难分,就必须花费相当的精力和时间去辨别。因此,通过设置假电台、使用假信号、传送假报文等伪装通信手段,可以迷惑窃听者,使真情报因时间延误而失去价值,而假情报又因时间紧迫而识别有误。

5) 无线电静默

还有一种在军事上经常采用的反电波窃听方式,就是在重大军事行动开始前或开始阶段,突然停止一切无线电通信联络,使敌方侦察不到己方情况。这在战术手段上称为无线电静默。1941年,日本偷袭珍珠港时,就停止了突击舰队和大本营的无线电通信,使庞大的舰队在大海中人不知鬼不觉地航行了12天。当大批日本舰载飞机飞临珍珠港上空时,美军才如梦初醒,躲闪不及。

9. 小结

现代声音窃听技术还在不断发展,纳米技术、微电子技术、遥感技术、空间技术等高新技

术正促使它变得更加隐蔽、方便、高效，成为无孔不入的“顺风耳”。

反窃听技术概括起来有“四大法宝”：隐蔽，不该说的机密绝对不说；加密，使用口令、代号、隐语、密码、语音保密器等进行保密；欺骗，用带有假情报的对话、声音、电文、信号来掩盖通信的真实意图；破获，如找出窃听器，识破窃听的技术手段，捉住暗藏的窃听者等。可以说，当今世界上窃听和反窃听的斗争也是一场比科学、比技术、比智慧的较量。

3.3.2　模拟话音保密技术与数字话音保密技术

话音保密技术包括模拟置乱和数字加密两大类。模拟置乱指对模拟话音所含频率、时间、振幅进行处理和变换，破坏话音的原有特征，尽可能使之不留下任何可以辨认的痕迹，达到保密传输话音信号的目的；数字加密是把话音模拟信号变换成数字信号，然后用数字方法加密，保密性比模拟加密好。

1. 模拟置乱技术

模拟话音信息包含频率、时间和振幅三大基本特征，模拟置乱对这三大特征进行某些人为的处理和变动，使原来的话音信号面目全非，达到保密的目的。单独的置乱分别称为频率置乱、时间置乱和幅度置乱，如果同时对两个或两个以上的参数进行置乱，则称为二维置乱或多维置乱。

1）频率置乱

频率置乱包括频率倒置、频带移位、频带分割置乱等，其作用是通过置乱改变话音信号的瞬时功率谱密度的分布，使得各个话音的频谱特征与原始的大相径庭。

倒频器是最早的话音加密器，它的原理是把话音信号 300～3400Hz 的频谱反转过来，即把 300Hz 一端的频谱移到 3400Hz 一端，而把 3400Hz 一端的频谱移到 300Hz 一端。由于频谱两端成分的偏移很大，从而形成不可理解的话音信号；但是中间的频谱成分偏移却很小，所以仍然有相当一部分话音信号是可以理解的。当窃听者制造出相同的倒频器时，这种体制很快就被破译了。

现在一般采用多重倒频加密的滚码方法，如把话音频带一分为二，各部分以不同频率倒置，再把这两部分相加产生出带宽与原始信号一样的组合信号。

2）时间置乱

时间域置乱指改变时间单元的先后关系，包括颠倒时段、时间单元跳动窗置乱、时间单元滑动窗置乱、时间样点置乱等，造成奇异的话音组合，使话音的节奏、能量、韵律等发生变化。

3）幅度置乱

幅度域置乱又称为噪声掩蔽，将噪声信号或伪随机信号叠加到话音信号上，将其可理解的话音信号掩蔽起来。

4）变换域置乱

变换域置乱是获得高保密度的有效置乱技术，其原理是将模拟信号变换成数字信号，做数字加密，然后再还原成模拟信号进行传输。变换域置乱包括扁球体置乱、傅氏变换置乱、离散傅氏变换置乱、数论变换置乱等。

5）模拟置乱的缺点

模拟置乱不能全部去掉原始模拟信号的基本属性，保密性较差，将逐渐被数字话音加密

技术所取代。

2. 数字话音加密技术

数字话音加密技术是通常采用的保密通信技术,具有较高的保密性,其特点是先把原始信号转换为数字信号,然后采用适当的数字加密方法实现保密通信。

话音数码化的方式可分为直接数码化方式和话音频谱压缩编码方式两大类。

1) 直接数码化方式

直接进行编码,编/解码器采用增量调制方式实现。随着大规模集成电路技术的发展及对增量调制技术的深入研究,推出了许多改进形式,如连续可变斜率增量调制(CVSD)已成为军事话音保密机的主要数码化技术。

2) 话音频谱压缩编码方式

对话音频谱进行压缩后再编码,如用于短波波段的保密通信声码器,它是按预定间隔提取并只传输话音的主要特征,然后在接收端利用这些特征恢复出话音。

3.3.3 扩展频谱与无线通信保密技术

扩频技术的历史可以追溯到20世纪50年代中期,其最初的应用包括军事抗干扰通信、导航系统等。直到20世纪80年代初,扩频技术仍然主要应用在军事通信和保密通信中,这种状况到了20世纪80年代中期才得到改变。美国联邦通信委员会(FCC)于1985年5月发布了一份关于将扩频技术应用到民用通信的报告,从此,扩频通信技术获得了更加广阔的应用空间。

扩频技术最初在无绳电话中获得成功应用,因为当时已经没有可用的频段供无绳电话使用了,而扩频通信技术允许与其他通信系统共用频段,所以扩频技术在无绳电话的通信系统中获得了其在民用通信系统中应用的第一次成功经历。而真正使扩频通信技术成为当今通信领域研究热点的是码分多址(CDMA)的应用。

扩频技术为共享频谱提供了可能,使用扩频技术能够实现码分多址,即在多用户通信系统中所有用户共享同一频段,但是通过给每个用户分配不同的扩频码实现多址通信。利用扩频码的自相关特性能够实现对给定用户信号的正确接收;将其他用户的信号看作干扰,利用扩频码的互相关特性,能够有效抑制用户之间的干扰。此外由于扩频用户具有类似白噪声的宽带特性,它对其他共享频段的传统用户的干扰也达到最小。由于采用CDMA技术能够实现与传统用户共享频谱,因此它也就成为个人通信业务(PCS)首选的多址方案。

1. 扩展频谱技术

扩频通信的理论基础是香农定理:$C=W\mathrm{Log}_2(1+S/N)$。

式中,C为信道容量,W是传输带宽,S/N是信号功率/噪声功率。

在信息速率一定时,可以用不同的信号带宽和相应的信噪比来实现传输,即信号带宽越宽,信噪比可以越低,甚至在信号被噪声淹没的情况下也可以实现可靠通信。因此,将信号的频谱扩展,可以实现低信噪比传输,并且可以保证信号传输有较好的抗干扰性和较高的保密性。

2. 频谱扩展的主要方式

频谱扩展的方式主要有以下几种：

(1) 直接序列扩频(Direct Sequence Spread Spectrum，DSSS)，使用高速伪随机码对要传输的低速数据进行扩频调制；

(2) 跳频(Frequency Hopping)，利用伪随机码控制载波频率在一个更宽的频带内变化；

(3) 跳时(Time Hopping)，数据的传输时隙是伪随机的；

(4) 宽带线性调频(Chip Modulation)，频率扩展是一个线性变化的过程。

以上方法中最常用的是直接序列扩频和跳频。一般而言，跳频系统主要在军事通信中对抗故意干扰，在卫星通信中用于保密通信；而直接序列扩频则主要是一种民用技术，CDMA 系统在移动通信中的应用已成为扩频技术的主流，已经在第二代移动通信系统(2G)的应用中取得了巨大的成功，在目前所有建议的第三代移动通信系统(3G)标准中(除了 EDGE)，都采用了某种形式的 CDMA。

3. 直接序列扩频技术

直接序列扩频使用伪随机码(PN Code)对信息比特进行模 2 加操作，得到扩频序列，然后使用扩频序列去调制载波发射，由于 PN 码通常比较长，因此发射信号在比较低的功率下可以占用很宽的功率谱，即实现宽带低信噪比传输。PN 码的长度决定了扩频系统的扩频增益，而扩频增益又反映了一个扩频系统的性能。

直接序列扩频系统的解扩与常规无线通信解调方式完全不同。在接收端，接收信号经过放大混频后，经过与发射端相同且同步的 PN 码进行相关解扩，从扩频信号中恢复出窄带信号，再对窄带信号进行解调，解出原始信息序列。

就无线传输方式来说，传统的窄带微波传输由于抗干扰性、保密性、可靠性、频率占用、传输带宽等多方面的问题，已经很难适应现代信息技术的要求，而扩频通信技术的发展和应用及时有效地为这个问题提供了解决手段。

现代通信的新领域，包括数字蜂窝移动通信、专用网络通信、室内无线通信、CDMA 移动通信、无线局域网、无线广域网、“蓝牙”传输技术等都是基于扩频通信体制的通信方式。

目前，应用了扩频通信技术的通用产品主要有两类，一是扩频无线调制解调器，二是专门提供无线网络连接的无线网桥、无线网卡、无线路由器。

无线调制解调器能够提供透明的数据通道，根据需要配置终端设备，可以支持多种数据业务，如话音、数据、网络、图像等。由于技术原因限制，还不能实现真正的话音点对多点业务，基本上都是依赖系统的叠加来实现的。对于单独的数据业务或网络连接，如果数据延时没有特别严格的要求，可以采用轮询方式传输。

无线网络类产品基本可以分为两类，一类是基于 802.11 无线网络协议标准的无线网络产品，另一类是基于各个厂商传输标准的无线网桥或无线路由器。它们都提供了高速的无线网络连接，可以广泛应用于点对点或点对多点无线局域网、无线广域网连接或宽带无线接入。

无线网络产品是扩频通信技术在数据通信领域的一个典型应用，充分发挥了扩频通信技术的各种优越性，为现代网络技术的广泛应用提供了更灵活、多样的解决手段。随着网

络技术的发展和进一步应用,移动无线网络,漫游无线接入必将成为现实,话音、数据、图像的多业务移动应用也将得到巨大的发展和应用,这又将极大地促进扩频通信技术的快速发展。

4. 跳频扩频通信技术

跳频扩频的实现方法是载频信号以一定的速度和顺序,在多个频率点上跳变传递,接收端以相应的速度和顺序接收并解调。这个预先设定的频率跳变的序列就是PN码。在PN码的控制下,收发双方按照设定的序列在不同的频率点上进行通信。由于系统的工作频率在不停地跳变,在每个频率点上停留的时间仅为毫秒级或微秒级,因此在一个相对的时间段内,就可以看作在一个宽的频段内分布了传输信号,也就是宽带传输。当然,跳频通信系统在每个跳频点上的瞬时通信实际上还是窄带通信。

跳频通信系统的频率跳变速度反映了系统的性能,目前,跳频系统的基本水平是:短波电台100跳/秒,超短波电台500跳/秒。每秒数千跳的扩频电台也已经问世,预计未来十年,跳频电台的发展可以达到每秒几万甚至几十万,上百万跳。目前,跳频系统的同步时间基本在几百毫秒的水平,今后也必将越来越短。同步时间越短,信息被发现、截获和测向的概率越低,通信的保密性、隐蔽性越好。

无线电通信由于它的灵活性,常常被用于作战通信。但是,传统的无线电通信都是在某一固定频率下工作的,很容易被敌方截获或施加电子干扰。跳频通信就是针对上述传统无线电通信的弊端,使原先固定不变的无线电频率按一定的规律和速度来回跳变,而让约定通信方也按此规律同步跟踪接收。由于敌方不了解我方无线电信号的跳变规律,很难将信息截获。

跳频通信可以有效地避开单频干扰和多频干扰,但是电子对抗中的跟踪干扰是它的"天敌",跟踪干扰的步骤是:侦听、处理、施放干扰。当我方截获到敌方的跳频序列后,迅速以同样的跳频序列施放干扰,由于跳频序列相同,预先设定的跳频序列就无法实现正常通信,这时只有通过转换跳频序列才能恢复通信,但是又会被重新跟踪并干扰。

因此只有提高系统性能,提高跳频速度,才能达到反侦听目的。由于受到技术条件、元器件的限制,不可能无限制提高跳频速度。今后的跳频通信应该是跳频与直接序列扩频技术的综合,或者是跳频、直接序列扩频、跳时技术的综合。

3.4 图像保密通信

在人们的工作、学习和生活中,有大量的数字图像和数字视频(动态图像)需要进行传输、存储等处理。这些数字图像和视频所包含的信息,有的涉及个人隐私和生命安全、有的涉及公司的巨大商业利益、有的甚至涉及国计民生和国家安全,其价值无法衡量,因此不同程度地需要保密。随着多媒体技术、特别是网络通信技术的飞速发展和普及,以及无线通信技术的广泛使用,越来越多的人更容易接触和获取传输或存储中的数字图像和视频,威胁到其中所包含信息的安全。因而数字图像和视频信号的保密工作及其加密技术的研究就显得十分紧迫和重要。

以前由于数字图像和视频的应用还不广泛,直接使用密码技术,将图像和视频数据与文

本等其他数据等同对待，对全部数据不加区别地按通用方法加密。这种方法安全性高，也易于实现，但实用中存在难以克服的缺点。主要是因为视频数据的海量性，密码学方法需要很大的加解密计算量，难以同时满足实时和安全的需要；并且由于视频编码信号的标志信息因加密无法识别，导致不能在线检索。这些问题严重阻碍了图像视频加密的应用。

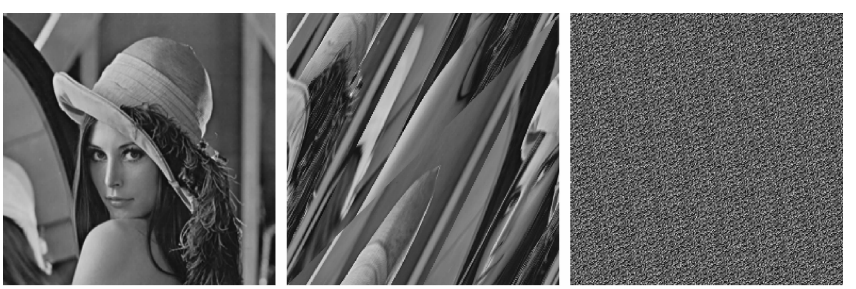
适用于数字图像加密的技术和方法，主要包括数字图像置乱、分存、隐藏、水印等，它们是针对数字图像特征的一些特殊加密方法。

数字视频在许多方面与静止图像有相同的特性，例如数据量大、结构性强、各部分数据的重要性不相同，视频的帧内编码与静止图像编码类似，上述方法和思路值得视频加密借鉴。但为了保证流畅的视觉效果，视频加密必须在较短时限内实时处理大量数据，要求有很高的实时处理速度，因此需要采用针对视频编码信号信源特征的各类视频加密技术。

3.4.1　数字图像置乱、分存、隐藏技术

1. 数字图像置乱技术

数字图像置乱是指将图像中像素的位置或者像素的颜色“打乱”，将原始图像变换成一个杂乱无章的新图像。其本质是使用某种算法（如 Arnold 变换、幻方排列、Hilbert 曲线、FASS 曲线、Gray 代码等），将原来(x,y)处的像素值变换到(x',y')处，使原图像无法辨认，解密时再恢复原(x,y)值。如果不知道所使用的置乱变换，很难恢复出原始图像。图 3-33 是经 Arnold 变换的效果图。



(a) 原图　(b) 单步Arnold变换结果　(c) 185步Arnold变换结果

图 3-33　Arnold 变换

置乱过程不仅可以在图像的空间域（色彩空间、位置空间）上进行，还可以在频域上进行。如果先将图像经 DCT 或小波变换，再对变换域系数按同样的算法置乱，效果更好，而且可以只对少量的重要系数置乱，减少了计算量。

2. 数字图像分存技术

将图像信息分为具有一定可视效果、没有互相包含关系的 n 幅子图像。只有拥有图像信息中的 $m(m\leqslant n)$幅子图像后，才可以恢复原始图像的信息；而任意少于 m 幅的子图像信息，都无法恢复原来的图像。如果丢失了子图像中的若干幅，只要剩余的子图像不少于 m 幅，并不影响图像的恢复。

图像分存可以避免由于少数几份图像信息的缺失（失密或丢失）而造成严重的事故，而个别图像信息的泄露或丢失也不会引起整个图像信息的失密或损失，从而降低了窃取或毁坏原始图像信息的可能性。

3. 数字图像隐藏技术

将信息隐藏于数字化媒体之中,实现隐蔽传输、存储、身份识别等功能。把指定的信息(可以是图像,也可以是声音或者文字、数值等信息)隐藏于数字化的图像、声音、甚至文本当中,来迷惑恶意攻击者。

3.4.2 数字水印技术

数字水印技术是指用信号处理的方法在数字化的多媒体数据中嵌入隐蔽的标记,这种标记通常是不可见的,只有通过专用的检测器或阅读器才能提取。

日程生活中为了鉴别纸币的真伪,人们通常将纸币对着光源,会发现真的纸币中有清晰的图像信息显示出来,这就是人们熟悉的"水印"。之所以采用水印技术是因为水印有其独特的性质:水印是一种几乎不可见的印记,必须放置于特定环境下才能被看到,不影响物品的使用;水印的制作和复制比较复杂,需要特殊的工艺和材料,而且印刷品上的水印很难被去掉。因此水印常被应用于诸如支票、证书、护照、发票等重要印刷品中,长期以来判定印刷品真伪的一个重要手段就是检验它是否包含水印。

随着数字技术和 Internet 的快速发展,多媒体作品(图像、视频、声频)的传播范围和速度突飞猛进,但同时盗版现象也愈演愈烈。于是保护数字音像产品的版权,维护创作者的合法利益,成为关系文化市场繁荣的重大课题。数字水印技术正是在这个背景下诞生的,它通过在原始数据中嵌入秘密信息——水印,来证明多媒体作品的所有权。它在数字作品的知识产权保护、商品交易中的票据防伪、声像数据的隐藏标识和篡改提示、隐蔽通信及其对抗等领域具有广泛的应用价值。

图 3-34 数字水印相机

如图 3-34 所示的数字水印相机将数字水印技术与数码相机技术结合起来,在拍摄数码照片时添加隐藏水印,第一时间内对图像的原始版权和图像内容进行保护,图像添加水印后,对其做任何更改(即使一个像素)均可以被有效识别,而图像的质量及大小则不会有任何变化,保证了数码影像的数据安全性。

1. 数字水印的基本特征

数字水印中包含音像作品的版本、创作者、拥有者、发行人等信息,数据量并不大,一般控制在 100 位以内,与动辄上兆字节的音乐、影视文件相比犹如藏在草堆中的一根针。

数字水印必须具备以下基本特征:

1) 隐蔽性

在数字作品中嵌入数字水印不会引起明显的质量下降。利用人类视觉或听觉特性,使带水印的作品欣赏起来无异于原先的作品。

2) 隐藏位置的安全性

水印信息隐藏于数据而非文件头中,文件格式的变换不会导致水印数据的丢失。

3）安全性

具有较强的抗攻击能力，能够承受一定程度的人为攻击，而暗藏的水印不被破坏。水印作品和普通作品在统计噪音分布上不存在区别，攻击者无法用统计学方法确定水印的位置。

4）鲁棒性

指在经历多种无意或有意的信号处理过程后，数字水印仍能保持完整性或仍能被准确鉴别。可能的处理包括：对图像进行尺寸缩放、剪裁、扭转等；对图像进行有损压缩；调整图像和视频的对比度、亮度、色度；进行模/数、数/模转换等。

在数字水印技术中，水印的数据量和鲁棒性构成了一对基本矛盾。从主观上讲，理想的水印算法应该既能隐藏大量数据，又可以抵抗各种信道噪声和信号变形。然而在实际中，这两个指标往往不能同时实现，不过这并不会影响数字水印技术的应用，因为实际应用一般只偏重其中的一个方面。如果是为了隐蔽通信，数据量显然是最重要的，由于通信方式极为隐蔽，遭遇敌方篡改攻击的可能性很小，因而对鲁棒性要求不高。但对保证数据安全来说，情况恰恰相反，各种保密的数据随时面临着被盗取和篡改的危险，所以鲁棒性是十分重要的，此时，隐藏数据量的要求居于次要地位。

2. 水印嵌入算法

水印嵌入算法可以分成两大类：空间域算法（水印被直接嵌入图像的亮度值上）和变换域算法（将图像做某种数学变换，然后水印被嵌入变换系数中）。

目前国内外的典型算法有以下几种：

1）最低有效位算法

它是国际上最早提出的数字水印算法，是一种典型的空间域信息隐藏算法。它可以隐藏较多的信息，但当受到各种攻击后水印很容易被移去。

2）Patchwork 算法

麻省理工大学多媒体实验室提出的一种数字水印算法，主要用于打印票据的防伪。其缺点是所隐藏的数据量较少，对仿射变换敏感。

3）基于 DCT 的频域水印算法

这是目前研究最多的算法，具有鲁棒性强、隐蔽性好等特点，可以与 JPEG、MPEG 等压缩标准的核心算法相结合，能较好地抵抗有损压缩。

4）扩展频谱方法

是扩频通信技术在数字水印中的应用，其特点是应用一般的滤波手段无法消除水印。

5）小波变换算法

具有空间域方法和 DCT 变换域方法的优点，是一种既有自适应功能，又有鲁棒性的技术，缺点是计算量大。

3. 嵌入水印的基本原理

所有嵌入水印的方法都包含两个基本的构造模块：水印嵌入系统和水印恢复系统（水印提取系统、水印解码系统）。

如图 3-35 所示的水印嵌入系统，其输入是水印、载体数据和一个可选的公钥或私钥。水印可以是任何形式的数据，如数值、文本、图像等。密钥可用来加强安全性，以避免未授权方恢复和修改水印。

如图3-36所示的水印恢复系统,其输入是已嵌入水印的数据、公钥或私钥,输出的是水印,它表明了所考察数据中存在给定水印。

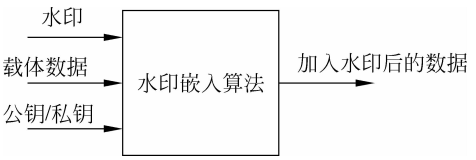


图3-35 水印嵌入系统

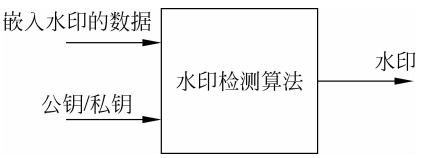


图3-36 水印恢复系统

【例3-5】 使用AssureMark嵌入数字水印。

(1) 运行AssureMark软件,在上方的"模式选择"中选择"嵌入水印"模式,如图3-37所示。

图3-37 AssureMark程序运行界面

(2) 单击"输入原始图像"文本框右侧的按钮,选择原始图像文件。若此时"水印容量(字节)"文本框中显示为0,表示图像文件过小,可以使用ACDSee的Resize功能扩大图像文件以增大水印信息容量。

(3) 单击"输出水印图像"文本框右侧的按钮,填入输出水印图像名。

(4) 在"输入水印信息"编辑框中输入水印信息内容。

(5) 在"密码"文本框中输入密码。

(6) 单击"嵌入水印"按钮开始嵌入水印,水印嵌入完毕后,程序显示原始图像和水印图像,如图3-38所示。可以看出嵌入水印图像后画质没有明显受损。

【例3-6】 使用AssureMark检测文件中的水印信息。

(1) 运行AssureMark软件,在上方的"模式选择"中选择"检测水印"模式。

(2) 单击"输入原始图像"文本框右侧的按钮,选择被检测的图像文件。

(3) 在"密码"文本框中输入水印的密码,如图3-39所示。

(4) 单击"检测水印"按钮,水印检测完毕后,程序显示检测结果,如图3-40所示。

(a) 原始图像　　(b) 水印图像

图 3-38　原始图像和水印图像

图 3-39　检测水印

图 3-40　检测结果

3.4.3　视频加密技术

视频信号具有数据量大的特点，在实际应用中需要压缩编码，当前应用广泛的标准有：MPEG1、MPEG 2、MPEG 4、H.261、H.263、H.264 等。

MPEG、H.26x 都按层次结构组织图像数据，各层的头标志是规定的易于从数据流中分辨出来的特殊码字组合，起同步、描述数据特征等作用，如果受到破坏(加密)，则会妨碍收方正确恢复原视频图像。

MPEG、H.26x 都采用 I(帧内)、P(预测)、B(双向预测)三种帧格式组成编码帧序列(MPEG4 采用类似的 I、P、B 三种 VOP 格式)，如图 3-41 所示。

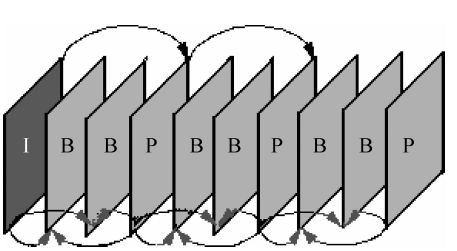


图 3-41　I、P、B 帧格式

I 帧独立编码，P 帧以其前帧为参考，使用运动估计和补偿技术编码本帧与其前帧相应块间的残差，B 帧也是差值编码，与 P 帧编码不同的是要

同时以前后帧为参考。P、B帧都不是独立编码,其编解码要依赖相应的I帧。因此I帧比较重要,对I帧加密不仅影响本帧解码和图像恢复,也影响到其后的P、B帧解码和图像恢复。与编码块相对应的前后帧的参考块由运动矢量指示,改变运动矢量即改变参考块,也影响了P、B帧正确解码。

当前视频压缩编码算法主要基于DCT变换和熵编码(主要是Huffman和算术编码)等基本算法,如图3-42所示。

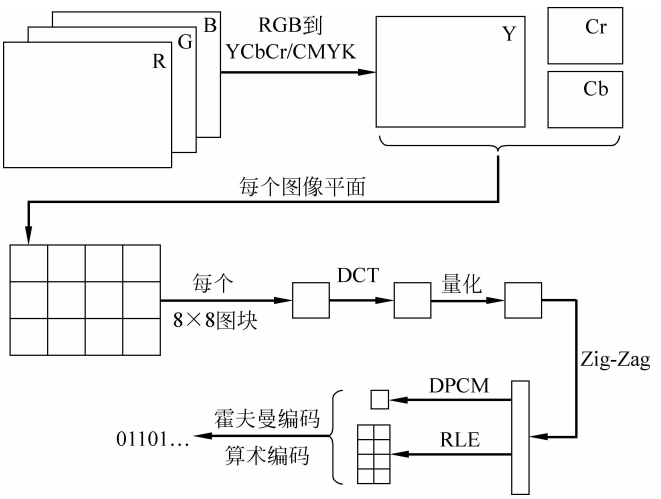


图3-42 视频压缩编码算法框图

视频数据一般分成8×8像素块,经DCT变换成频域系数,直流和低频系数集中了大部分能量,比较重要。8×8视频系数通常按Zig-Zag顺序映射成1×64的序列,低频系数在前,集中了主要能量,高频系数在后,大部分接近为零,通过量化和游程编码达到压缩的目的。

改变DCT系数的顺序,能改变解码图像,但会降低压缩率。Huffman码表通过统计码流中各种位组合模式出现的概率制作,编解码要使用统一的Huffman码表,否则不能正确解码。

下面是一些常见的视频加密方法:

1. 传统加密方法

最早的视频加密方法,对全部视频数据流直接用密码技术加密和解密,易于实现,在目前视频加密方法中,安全性最高。但是由于视频信号数据量很大,所以这种加密方法计算量非常大,不仅浪费资源,而且难以保证实时性。另外标志信息经加密后无法识别,不能实现在线检索等功能。

2. 选择性加密方法

选择性加密是基于信源特征的视频加密方法的主要方向,只对选择的重要数据加密,可分为以下几类:

1) 仅对I帧加密

仅对I帧DCT系数块加密,具有扩散作用,使P、B帧利用运动补偿进行差值编码的相

应块不加密也难以正确解码，达到了选择部分数据加密减少计算量的目的。该算法节约加解密时间 30%～50%，提高了加解密速度。且不改变原视频编码数据码流量大小，不影响压缩率。但这种算法不安全，在保密要求高的场合中不能单独使用。

2）加密运动矢量

随机改变运动矢量的符号位或同时改变符号位和数值来影响 P、B 帧的正确解码，对 I 帧编解码完全没有影响，故不能单独使用。加密数据量小，计算量小，因而速度快，不降低编码压缩率。

3）DCT 块内系数分层加密

把 DCT 系数从低频到高频分为基本层、中间层和增强层三部分。只加密基本层和中间层，可以减少计算量，保证基本层传送，即使中间层和增强层丢失，接收方也能显示出主要信息。该算法只对部分 DCT 系数加密，减少了计算量。

4）仅加密头信息

将头信息加密，再与其他数据随机混合，使接收方难以按原数据结构区分结构信息和视频信息并解码。该算法不降低压缩率，计算量小。但是安全性较低，因为头信息所含信息量小，加密效率低，这种加密方式比较容易破解。为便于合法接收方解码，需加入同步信息，或保留原来部分同步信息。

3. Zig-Zag 置乱算法

Zig-Zag 置乱算法的基本思想是：使用一个随机的置乱序列来代替 Zig-Zag 扫描顺序，将各个 8×8 块的 DCT 系数映射成一个 1×64 矢量。

Zig-Zag 置乱算法速度很快，不影响视频的实时传输。但是经过加密的 MPEG 流将显著增大，最大可增加 46%，且有严重的安全性问题。

4. 改变 Huffman 码表算法

将通用 Huffman 码表修改（加密）后使用，并将其作为密钥。非法接收方无此特殊码表，不能正确解码。该算法完全不增加计算量，适用于使用 Huffman 编码的各种视频和图像压缩编码标准和算法，其缺点是安全性较差。

5. 基于统计规律的视频加密算法

该方法不加密头信息结构格式等数据，只加密图像数据本身。将待加密数据分为两半，一半用密码方法加密，另一半用简单异或，因此总体减少了计算量，提高了计算速度。

该方法不影响压缩率，适用于压缩的视频编码数据，而且压缩效果越好，加密效果也越好。

【例 3-7】 使用“多媒体文件加密器”加密视频文件。

（1）运行程序，界面如图 3-43 所示。

（2）单击“选择&添加文件”按钮，选择要加密的文件。在“请指定加密密钥”文本框中输入密码，如 test1234，单击“执行加密”按钮，系统进行加密，如图 3-44 所示。

（3）单击“加密完成”按钮，完成加密。用户得到加密文件后，双击该文件，出现如图 3-45 所示的“播放授权信息”界面。

（4）用户复制“您的电脑标识”文本框中的内容，发送给加密者。

（5）加密者单击“多媒体文件加密器”的“创建播放密码”选项，输入加密时的密码和用

户标识,如图 3-46 所示。

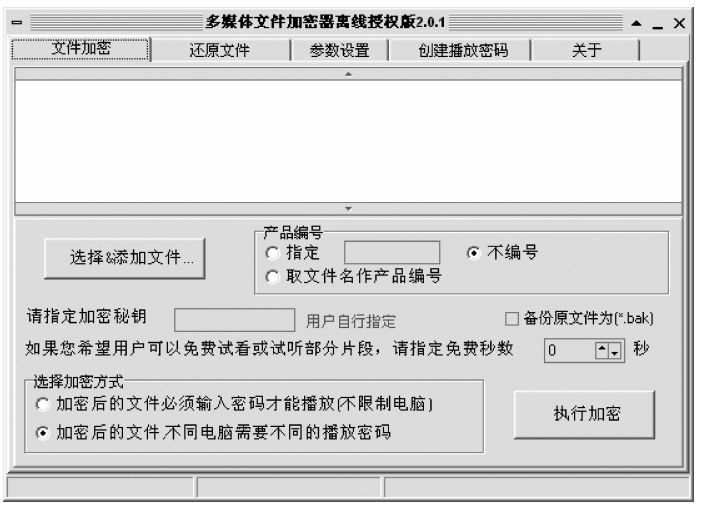


图 3-43 多媒体文件加密器界面

图 3-44 多媒体文件加密器界面

图 3-45 “播放授权信息”界面

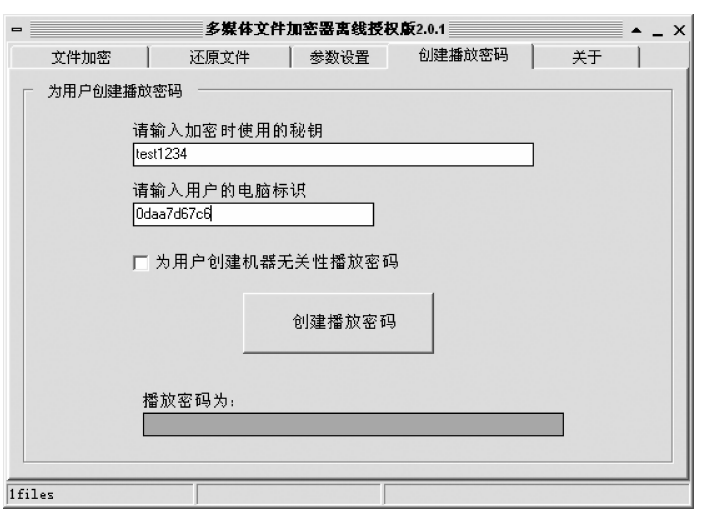


图 3-46 “创建播放密码”界面

(6) 单击“创建播放密码”按钮,产生针对该用户电脑的播放密码,如图 3-47 所示。

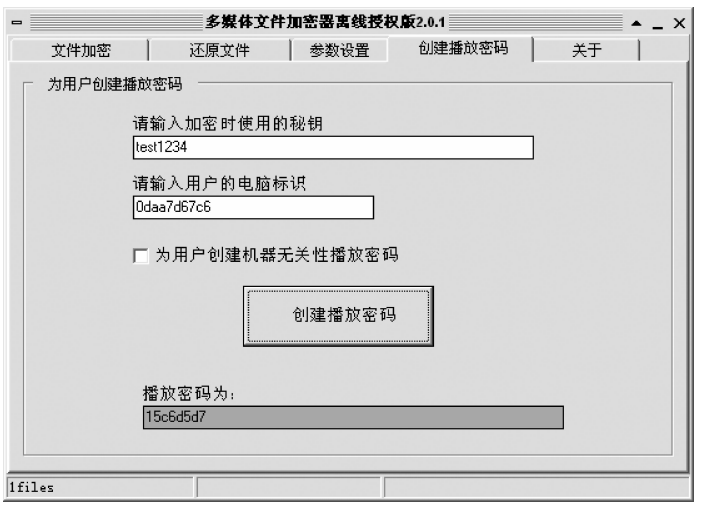


图 3-47　创建播放密码

(7) 将该密码发送给用户,用户在“请输入播放密码”文本框中输入上述“播放密码”,单击“确定”按钮,实现视频播放。

习　　题

1. 简述通信保密的基本要求。
2. 简述网络通信保密的基本方法。
3. 信息隐藏技术与加密技术的区别是什么?
4. 上机实现基于文本的信息隐藏。
5. 使用 Easycode 将一幅 GIF 图片隐藏在另一幅 JPG 图片中。
6. 上机实现基于声音的信息隐藏。
7. 什么是窃听、反窃听、防窃听?
8. 简述话音保密技术。
9. 简述无线通信保密技术。
10. 什么是图像置乱、分存、隐藏技术?
11. 数字水印技术的基本特征有哪些?
12. 上机实现数字水印的嵌入与检测。
13. 常见的视频加密方法有哪些?
14. 上机实现对视频的加密。