编码技术　图像加密　信息隐藏　安全认证　光学成像

OPTICAL RANDOM PHASE CODING
TECHNOLOGY AND ITS APPLICATION

光学随机相位编码技术及应用

袁胜 \ 著

非外借

中国水利水电出版社
www.waterpub.com.cn

光学随机相位编码技术及应用

袁胜　著

中国水利水电出版社
www.waterpub.com.cn
·北京·

内 容 提 要

本书主要介绍了光学随机相位编码技术及其在图像加密、信息隐藏、安全认证、光学成像等方面的应用。全书主要概括为五个部分，第一部分主要介绍光学随机相位编码技术的理论基础；第二部分介绍基于随机相位编码的图像加密及攻击技术；第三部分介绍基于随机相位编码的信息隐藏及隐藏信息的检测技术；第四部分介绍基于光学干涉加密系统的安全认证技术；第五部分介绍基于随机相位调制的强度关联成像技术及其在图像加密中的应用。本书结合作者的研究成果，详细论述了相关理论和方法，并展望了光学随机相位编码技术的研究前沿和应用前景。

本书内容详实，并提供了当前国内外相关研究领域的最新进展和成果，可以供光信息技术研究人员阅读，也可以作为光信息科学与技术及相关专业本科生和研究生的教材及教学参考书。

图书在版编目（CIP）数据

光学随机相位编码技术及应用 / 袁胜著. -- 北京 : 中国水利水电出版社, 2018.4
ISBN 978-7-5170-6361-2

Ⅰ. ①光… Ⅱ. ①袁… Ⅲ. ①信息光学－安全技术 Ⅳ. ①O438

中国版本图书馆CIP数据核字(2018)第053636号

策划编辑：石永峰　责任编辑：陈　洁　加工编辑：张天娇　封面设计：李　佳

书　名	光学随机相位编码技术及应用 GUANGXUE SUIJI XIANGWEI BIANMA JISHU JI YINGYONG
作　者	袁胜　著
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路1号D座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（营销中心）、82562819（万水）
经　售	全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	三河市鑫金马印装有限公司
规　格	170mm×240mm　16开本　13.5印张　256千字
版　次	2018年4月第1版　2018年4月第1次印刷
印　数	0001—2000册
定　价	54.00元

前　言

在光学发展史中，20 世纪 60 年代诞生的激光是一项重大成就。激光的出现和发展，使光学的研究进入一个崭新的阶段，成为现代科学技术的前沿阵地之一。随着现代科学技术和工业技术以及信息处理技术的发展，光学与其他科学技术广泛结合并相互渗透，产生了许多新理论、新技术，形成了许多新的分支学科和交叉学科。随机相位编码是光学成像和信息编码的一项重要手段。它以光波为载体，以信息光学和光的传输理论为基础，能够实现对待测物体的成像、识别、加密、隐藏和认证，已被广泛应用于光学成像和信息安全领域。本书是在近年来从事光学信息处理技术研究的基础上，吸收了国内外同仁相关的研究成果，从光学成像和信息编码的角度编写而成的。

本书首先介绍了光学随机相位编码技术的研究背景和意义，随后以信息光学原理为基础，系统介绍了随机相位编码技术的基本原理以及在信息安全和光学成像方面的典型应用。第 1 章针对国内外基于随机相位编码的信息安全和光学成像典型方案进行了综述；第 2 章以基尔霍夫衍射公式为基础，介绍了光学标量衍射的基本原理，主要包括两种典型的衍射：菲涅耳衍射和夫琅禾费衍射，随后系统阐述了透镜的傅里叶变换性质、光学相干理论，以及热光和散斑场的相关概念；第 3 章介绍了以透镜实现傅里叶变换的理论为基础的双随机相位编码技术；第 4 章在 Kerckhoff 假设的前提下，系统介绍了四种典型的针对双随机相位编码系统的攻击方法；第 5 章针对双随机相位编码的攻击技术，介绍了增强其安全性的改进方案；第 6 章针对双随机相位编码技术属对称密码体制、其密钥需要单独传输的缺点，介绍了利用 RSA 公钥密码体制管理和传输双随机相位编码技术中的相位板密钥的方法；第 7 章首先介绍了基于双随机相位编码技术的信息隐藏技术，分析了借助图像复原技术提取秘密信息的方法，然后回顾了实虚部空域叠加的双随机相位编码信息隐藏方法，并针对其缺点，探讨了一种基于双随机相位编码技术和 RSA 公钥密码体制的信息隐藏技术；第 8 章介绍了一种基于统计假设检验的信息隐藏检测方法；第 9 章介绍了一种基于光学干涉原理和改进型纯相位相关器的光学认证系统；第 10 章介绍了基于随机相位调制的关联成像的相关知识和关联成像中用到的压缩感知算法；第 11 章分析了基于计算关联成像加密技术的基本原理，分析了三种基于计算关联成像的加密技术的选择明文攻击技术，给出了增强

其安全性的有效方法，最后介绍了基于计算关联成像的多图像加密方案。

全书从内容上主要概括为五个部分：第一部分（第 1、2 章）主要介绍光学随机相位编码技术的理论基础；第二部分（第 3～6 章）介绍基于随机相位编码的图像加密及攻击技术；第三部分（第 7、8 章）介绍基于随机相位编码的信息隐藏及隐藏信息的检测技术；第四部分（第 9 章）介绍基于光学干涉加密系统的安全认证技术；第五部分（第 10、11 章）介绍基于随机相位调制的强度关联成像技术及其在图像加密中的应用。

在编写中，我们努力使本书涉及的内容都是最新的研究进展，在理论上力求简明易懂，便于学生自学，激发读者的研究兴趣。本书在编写过程中，得到了中国水利水电出版社的大力帮助，在此表示衷心的感谢。

由于作者水平有限以及光电信息技术的不断发展，书中难免有不足和错误之处，敬请读者批评指正。

编 者

2017 年 11 月

目　　录

第 1 章　绪论

1.1　信息安全

随着因特网和多媒体技术的快速发展，数字化信息以不同的形式在网络上方便、快捷地传输，多媒体通信逐渐成为人们之间交流信息的重要手段。数字信息系统与网络在人们的工作、生活和学习中发挥的作用越来越明显，人们可以通过网络交流各种信息、进行网上贸易等。然而，因特网的平民化和便捷性给人们带来了信息传递快捷通道的同时，也带来了隐患。因为敏感信息容易被窃取、篡改、非法复制和传播等，所以确保信息的安全已成为人们极为关心的问题，也是当今各国科研人员研究的热点和难点之一。

信息加密、信息隐藏和安全认证是信息安全领域主要的研究方向[1,2]。信息加密主要是通过密码学的方法，将秘密信息变换为看上去毫无意义的乱码，使得在信息传输过程中，非法攻击者无法从乱码中获得秘密信息，从而保证信息的安全；而信息隐藏主要是将有意义的信息（或经密码学方法加密后的信息）隐藏在另一称之为载体的信息中，得到隐秘载体，借助载体实现秘密信息的传输。由于攻击者不知道这个普通载体中是否隐藏了秘密信息，从而隐藏了通信的存在，保证了信息的安全。信息加密技术隐藏了信息的“内容”，信息隐藏技术隐蔽了信息的“存在”；身份认证也称为“身份验证”或“身份鉴别”，是指在计算机及计算机网络系统中确认操作者身份的过程，从而确定该用户是否具有对某种资源的访问和使用权限，进而使计算机和网络系统的访问策略能够可靠、有效地执行，防止攻击者假冒合法用户获得资源的访问权限，保证系统和数据的安全，以及授权访问者的合法利益。

1.1.1　密码学简介

1. 密码体制

密码编码学是研究如何对信息进行变换，以隐蔽其真实含义的学科[3-6]。具有这种功能的系统称为密码系统（Cryptographic System）。被编码的信息称为明文（Plaintext），经过密码编码方法将明文变换成的另一种隐蔽形式称为密文（Ciphertext）。保密通信的过程如图 1.1 所示，发送方在加密密钥 k_e 的控制下经

过加密算法把信源的待加密信息 m（明文）变换成密文 c。密文 c 经信道发送给接收方。接收方收到密文 c 后，在解密密钥 k_d 的控制下将密文 c 还原成明文 m。另外，在保密通信的过程中还存在着两种攻击，即非法接入者的主动攻击和窃听者的被动攻击[5]，主动攻击者将经过篡改的密文信息 c' 插入信道，而被动攻击者只是将窃听到的密文 c 进行分析，试图获得明文 m。

设明文空间为 M，密文空间为 C，密钥空间分别为 K_e 和 K_d，其中 K_e 是加密密钥空间，K_d 是解密密钥空间，K 为密钥，C'为非法接入者攻击后的密文，M'为窃听者破译获取的明文。对给定的明文 $m \in M$，密钥 $k_e \in K_e$，加密变换将明文 m 变换成密文 c 的过程表示为：

$$c = E_{k_e}(m) \tag{1.1}$$

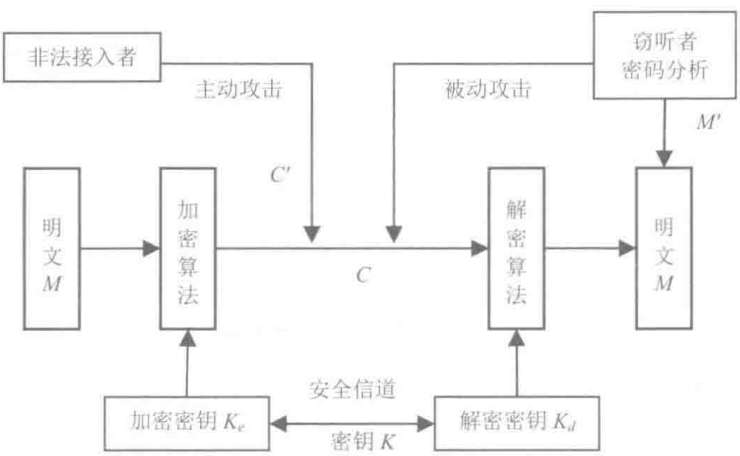


图 1.1 保密通信示意图

接收方利用解密密钥 $k_d \in K_d$，对收到的密文 c 实施解密运算，得到明文 m，该过程可以表示为：

$$m = D_{k_d}(c) \tag{1.2}$$

我们称总体 $(M, C, K_e, K_d, E_{k_e}, D_{k_d})$ 为一个密码系统或密码体制。其中，E_{k_e} 和 D_{k_d} 分别表示加密变换和解密变换。

2. 单钥密码体制

如果一个密码体制的加密密钥和解密密钥相同，或者两者之间存在简单的变换关系，则称此密码体制为单钥密码体制或对称密码体制[4,5]。单钥密码体制的保密性能主要取决于密钥的安全性。将密钥安全地分配给通信双方，需要处理包括密钥的产生、分配、存储、销毁等多方面的问题，统称为密钥管理[4,5]。这是影响单钥密码体制安全性的关键因素。因为倘若密钥管理不当，即使密码算法再好，

也不能实现系统的安全保密。

虽然对称密码体制提供了很多加密技术中所需要的服务，它能够安全地保护秘密信息，但是使用对称密码进行保密通信，仍然存在两个难题：

（1）通信双方必须事先就密钥达成共识。因为通信双方若不能通过非保密方式达成密钥共识，则密钥就容易被其他人窃取，所以通信双方需要进行私人会面以交换密钥。如果需要发送消息给许多用户，就需要建立许多新的密钥，那么，仅通过私人会面以达成密钥共识是不够的。因此，在利用对称密码体制进行保密通信的过程中，必须解决其密钥管理问题。

（2）在 A 向 B 进行了利用对称密码体制的保密通信后，A 可能会否认向 B 发送过加密消息。他可以说是 B 自己创建了这则消息，然后使用他们共享的密钥加密。由于用此密钥加密和解密的过程相同，并且他们都可以访问它，所以他们中的任何一个人都可以加密这则消息。因此，B 希望 A 的消息带有数字签名，这样 A 就无法否认了。然而，仅仅依靠对称密码体制却很难实现数字签名，目前只能依靠公钥密码来解决这个问题。

因此，密钥管理困难是对称密码应用的主要障碍；另外，不易实现数字签名，也限制了对称密码体制的应用范围。

3. 公钥密码体制

1976 年美国斯坦福大学的 W. Diffie 和他的导师 M. Hellman 发表了“密码学新方向”的论文[7]，第一次提出公钥密码体制的概念，从此开创了一个密码的新时代[8-10]。

公钥密码体制的基本思想是，将对称密码体制的密钥 k 一分为二[6]，即加密密钥 k_e（公钥）和解密密钥 k_d（私钥），使 $k_e \neq k_d$，而且由计算复杂性确保由加密密钥 k_e 不能推出解密密钥 k_d。这样，即使将 k_e 公开也不会暴露 k_d，因此可以将 k_e 公开而只对 k_d 保密，从而从根本上克服了对称密码在密钥管理上的困难。

根据公钥密码体制的基本思想可知，一个公钥密码算法应当满足以下三个条件[6]：

（1）使用私钥 k_d 可以解密由公钥 k_e 加密的密文，即解密算法 D_{k_d} 与加密算法 E_{k_e} 对所有明文 M 都满足：

$$D_{k_d}(E_{k_e}(M)) = M \tag{1.3}$$

（2）在计算上不能由 k_e 推导出 k_d。

（3）加密运算 E_{k_e} 和解密运算 D_{k_d} 都是高效的。

满足了以上三个条件，即可构成一个公钥密码体制，它可以确保信息的秘密

性。但是，如果还要确保信息的真实性，则还需满足下面的条件：

对于所有明文 M 都有：

$$E_{k_e}(D_{k_d}(M)) = M \tag{1.4}$$

这是公钥密码体制能够实现数字签名、确保信息真实性的基本条件。

1.1.2 信息隐藏

信息隐藏作为信息安全中的另一重要核心技术，是 20 世纪 90 年代从国外逐步兴起的，目前已引起了众多信息安全领域科研人员的研究兴趣。它是利用多媒体信号本身存在的冗余，将秘密信息隐藏在宿主信号中，在不影响宿主信号的感觉效果和使用价值的前提下，达到不被感知系统察觉的目的[11-14]。信息隐藏最重要的特点在于它不仅隐藏了信息的内容，而且隐藏了通信的存在，因而在信息安全领域显示出广阔的应用和发展前景[11-14]。

1. 信息隐藏系统

一个通用的信息隐藏系统如图 1.2 所示，系统主要包括一个嵌入运算和一个提取运算。其中嵌入运算是指信息隐藏者利用嵌入密钥，将秘密信息添加到原始宿主信息中，从而生成合成信息。提取运算是指利用提取密钥从接收到的合成信息中恢复出秘密信息。嵌入密钥和提取密钥用于控制隐藏过程，使得检测和恢复过程仅限于那些知道密钥的人。

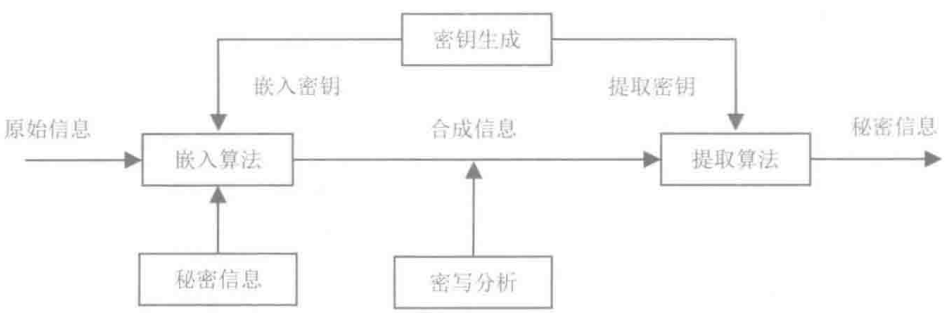


图 1.2 信息隐藏的一般框架

其中，在信息隐藏系统中的密写分析是指试图发现隐秘信息，进而对其破译的操作或运算[14]。也就是说，在这个信息隐藏系统模型中，还存在着一个隐藏分析者。它通常位于隐藏对象传输的信道上。

2. 信息隐藏分类

近来，人们提出了许多信息隐藏技术，其中大多数技术都是基于替换方法或修改方法的[13]，即用一个秘密信息替换或修改宿主信息中的冗余部分。信息隐藏技

术主要用来实现以下几类保护：防窃听、防篡改、防伪造、防抵赖。一般来说，按照保护对象，信息隐藏技术主要分为隐匿技术和版权标记技术[12,13]。前者主要用于保密通信，它所要保护的是秘密信息本身，后者主要用于保护隐秘载体，详细的分类如图 1.3 所示。在这些技术中，密写术和版权保护技术是目前研究较为广泛和热门的课题。

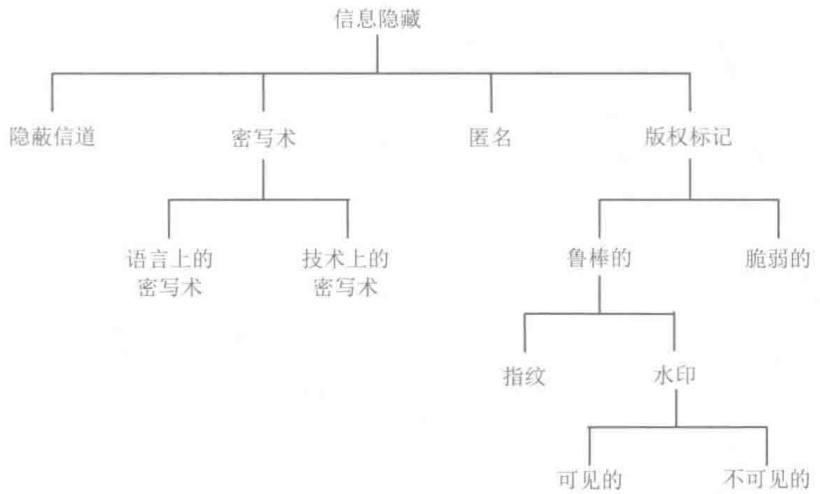


图 1.3　信息隐藏技术按保护对象的分类

3. 信息隐藏的特征

信息隐藏虽然有许多不同的分支，但各个分支具有许多共同的特征[13]。

（1）不可感知性。对于信息隐藏技术，最重要的要求是隐藏信息的不可感知性。如果在信息嵌入过程中使载体引入了人为的痕迹，给载体的质量带来了可视性或可听性的明显下降，就会减少已嵌入信息的载体的价值，破坏信息隐藏系统的安全性。当然，个别特殊场合会使用可见水印。

（2）鲁棒性。信息隐藏技术应保证在隐秘载体受到一定的扰动后，仍然能从中恢复隐藏信息。对多媒体数据通常要做有损压缩处理，以缩小文件数据量，节省存储空间和传输时间。另外，信息在传输过程中也可能会受到噪声、滤波、人为破坏等干扰，因此具有一定的鲁棒性是必须的。

（3）稳健性。信息隐藏中的水印技术必须具有高度的稳健性，任何删除水印的行为都会损害数字产品的质量，使之失去价值。密写技术则不一定要求这样强的稳健性，甚至很脆弱。

（4）嵌入容量和强度。在保证不可感知性和载体一定的前提下，应尽量在载体中嵌入更多的信息，提高信息的传输效率。另外，也希望嵌入信息的强度较高，

这可以增强信息隐藏系统的鲁棒性，但是这会减弱信息隐藏的不可感知性和安全性，所以两个方面需要权衡考虑。

（5）密钥与安全性。在隐秘载体被发现后，隐藏信息的安全就转化为像信息加密技术一样对密钥的保护。因而，密码学中对密钥的基本要求也适用于信息隐藏技术，如必须有足够大的密钥空间等。在设计一个信息隐藏系统时，密钥的产生、发放、管理等都需综合考虑。

（6）自恢复性。经过一些操作或变换后，可能使原数据产生较大的破坏，但是，如果只从留下的片段数据仍能恢复隐藏信息，而且恢复过程不需要宿主载体，这就是所谓的自恢复性。

1.1.3 身份认证

通信和数据系统的安全性常取决于能否正确验证通信用户或终端的身份。身份认证又可以称为身份识别，它的目的就是要证实用户或主体包括各种终端的真实身份是否与其所声称的身份相符的一个过程，通常是用交互式协议实现的。目前存在有非常多的身份认证协议，但由于身份认证通常与具体的应用系统高度集成，其标准化程度并不高，单独的身份认证系统也不多见。

1. 静态身份认证

静态身份认证通常指利用口令来进行的一种身份验证方法，如操作系统及诸如电子邮件系统等一些应用系统的登录和权限管理等。系统事先需要保存每个用户的二元信息组（ID_x, PWx），进入系统时用户输入其拥有的 ID_x 和 PWx，系统根据保存的用户信息和用户输入的信息相比较，从而判断用户身份的合法性。这种身份认证方法操作十分简单，无需任何附加设备，成本低、速度快，但同时又最不安全，因为其安全性仅仅基于用户口令的保密性，而用户口令一般较短，容易猜测且常以明文形式存储。另外，口令的明文传输使得系统攻击者很容易通过搭线窃听方法获取用户口令，很难防止重放攻击和来自内部人员的攻击。静态身份认证的安全性较低，很难满足复杂网络环境下的应用要求。

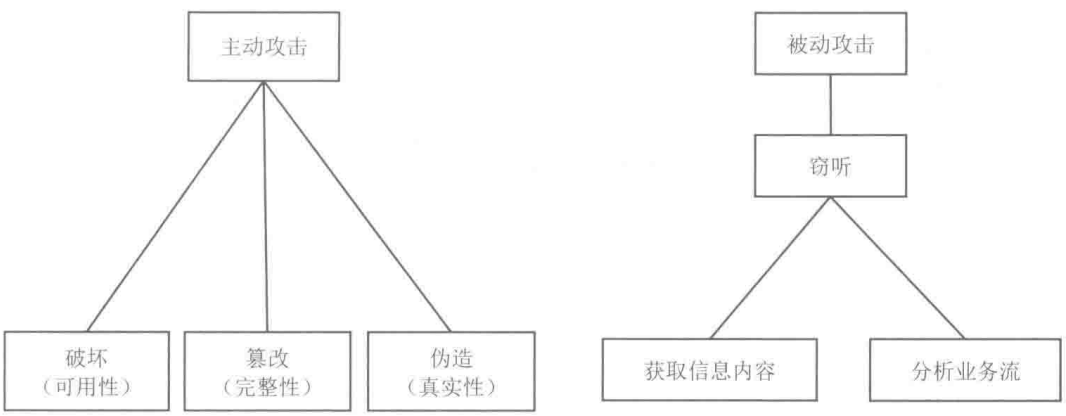
2. 动态身份认证

动态身份认证通常是指基于挑战应答模式的密码协议。其主要思想是，证明方通过某种方式展示拥有与他所声称的身份有关的秘密信息来向验证方证明他就是所声称的身份实体，但同时并不会将那个秘密信息本身透露给验证者，即实现零知识证明。在挑战应答模式下，这通常是通过验证方向证明方发送一个随机且通常保密的挑战信息，然后证明方根据该挑战信息以及其所掌握的与身份相关联的秘密信息，生成对应的响应信息“证据”发送给验证方，再

由验证方通过某种方式来验证该响应的正确性并以此来证实证明方的身份。挑战应答方式在每次认证过程中，证明方提供的“证据”都是一次性的，如果在通信过程中，他们的通信信息包括响应信息被侦听、窃听，那么协议的零知识证明特性将保证窃听者不能从窃取的信息中得到任何有用的信息，用于使验证者接受他是原证明方的身份。

1.2 传统信息安全技术面临的威胁

随着通信技术和计算机技术的快速发展，信息安全面临的威胁也多种多样，但是，归纳起来可以分为两类[4]：主动攻击和被动攻击，如图 1.4 所示。



（a）主动攻击　　（b）被动攻击

图 1.4　信息安全威胁的分类

主动攻击是指能够对所截获的信息进行修改甚至破坏的攻击。在这种攻击中，入侵者往往采取删除、篡改、伪造等手段向系统注入假信息，或者对传送中的信息进行某些破坏，使合法用户也无法提取秘密信息，以此来影响信息系统的正常运行。

绝对防止主动攻击是十分困难的，因为需要随时随地对通信设备和通信线路进行物理保护，因此抗击主动攻击的主要途径是检测，以及对此攻击造成的破坏进行恢复。

被动攻击是指攻击者通过搭线窃听等方式，截获保密系统的密文，并对其进行分析，以获得密钥或明文的攻击。被动攻击又可以分为两类：一类是获得信息的内容；另一类是进行业务流分析，即获取消息的格式、确定通信双方的位置和身份，以及通信的次数和消息的长度等，在某些特定情况下，这些信息对通信双