加密图像置乱性能分析*)

徐江峰[1] 杨 有[2]

(郑州大学信息工程学院 郑州 450052)[1](重庆师范大学数学与计算机科学学院 重庆 400047)[2]

摘 要 在对近年来的图像加密技术进行分析和研究的基础上,给出了几个图像置乱评价参数——不动点比、信息熵、灰度平均变化值及自相关度,并利用这些参数对传统的图像加密算法的置乱性能进行了模拟实验分析。分析及试验结果表明,综合利用这些参数可以有效地对加密图像的置乱度及安全性进行分析和评价。

关键词 图像加密,置乱性能,信息熵,安全性分析

Analysis of Scrambling Performance of Encrypted Image

XU Jiang-Feng[1] YANG You[2]

(School of Information and Engineering, Zhengzhou University, Zhengzhou 450052)[1]

(College of Mathematics and Computer Science, Chongqing Normal University, Chongqing 400047)[2]

Abstract With the rapidly development of network and multimedia technology, more and more image data transfer on Internet. In order to protect the privacy and to make the image data transfer more safely, a lot of schemes of image encryption are presented. To evaluate and analyze the scrambling perfermance and security of these schemes, some parameters such as the percentage of unchanged point, the information entropy, the average of pixel values change and the self-correlation of image are given. The simulation results of the experiment indicate that these parameters can be effectively ued to evaluate scrambling performance and the security of encrypted image.

Keywords Image encryption, Scrambling performance, Information entropy, Analysis of security

1 引言

人类接受的信息大部分都来自视觉,或称为图像信息,其中包括图像、图形(动画)、视频等,它们是人类最重要的信息获取和交流方式。由于 Internet 传输数据方便快捷,不受地域限制,因此通过 Internet 传输的数据越来越多。随着宽带网的快速发展,利用 Internet 传输的各种图像信息也将越来越多。在这些图像信息中,有很多是要求发送方和接受方进行保密通信的,如军用卫星所拍摄的图片、军用设施图纸、新式武器图、金融机构系统图及涉及个人隐私或部门秘密的图像数据等,因而图像数据的保护越来越重要。

近几十年来,现代加密技术得到了快速发展,出现了许多性能良好的加密算法,如:DES、AES、RSA 等,但这些方案并不适合于图像加密,因为它们的应用对象主要是一维数据,而图像是二维或三维的,并且与一般的文本数据相比,图像中包含的数据量大且冗余高。因此,有许多专用的图像加密方案被提出[1~3]。信息加密的目的是提高信息存储及传输的安全性,由于加密策略的不同,不同加密方案的安全性是不同的,有些方案具有很高的安全性,但有些方案安全性并不高,提出之后很快就被破解[4~5]。为了使加密后的数据具有较高的安全性,加密中使用的方案应该具有很强的安全性,不管是对文本数据还是图像数据都是如此。图像加密的本质是像素置乱,不同加密方案得到的加密图像置乱程度是不一样的,置乱程度越高安全性越高。然而对于众多的图像加密方案,如何对其置乱度进行分析与比较呢?

针对上述问题,本文在对近年来的图像加密技术进行分析之后,给出了几个图像置乱评价参数——不动点比、信息熵、灰度平均变化值及自相关度,并利用这些参数对传统的图像加密算法的置乱性能进行了模拟实验分析。分析及试验结果表明,综合应用这些参数可以有效地对图像加密算法的置乱度及安全性能进行分析与评价。

2 图像加密技术

常用的图像置乱及加密技术主要以下几类[1]:

2.1 基于矩阵变换/像素置换的加密技术

这种方法的基本原理是对图像像素的位置进行矩阵变换,安全性基于转换矩阵,其中 Arnold 变换和幻方变换是常用的变换方法。该类变换只对图像中的像素位置进行置乱,并不改变像素值。因而,这种变换的安全性较低,攻击者在知道加密算法和密文时,很容易得到明文。即使采用复杂的变换或随机变换矩阵,该类加密安全性同样不高,因为攻击者采用已知明文或选择明文的攻击方法就容易得到加密用的变换矩阵。

2.2 基于随机序列的加密技术

该类加密的基本思想是利用伪随机序列生成器产生像素变换的二进制序列,而后根据该序列改变图像中的像素值,从而实现加密。文[6]给出了一个基于混合细胞自动机(hybrid cellular automata)的二进制图像加密方案,方案中首先利用混合细胞自动机产生伪随机序列,再把图像转换成一维序列,最后把两个序列进行按位异或后得到的序列转换为图像,从而实现图像加密。

2.3 基于压缩编码的加密技术

该类加密的基本思想是首先对图像进行压缩,而后再进行加密。基于四叉树编码和 SCAN 语言的图像加密和基于

*)本课题得到国家自然科学基金(60074034)的支持。徐江峰 博士,副教授,研究领域:网络安全及混沌加密通信。杨 有 博士研究生,讲师,研究领域:嵌入式微小型信息处理系统。

压缩编码的图像加密都属于该类加密技术，只不过前者进行的是无损压缩，而后者进行的是有损压缩。采用此类加密技术，可以减少加密后图像传输的数据量，加快传输速度，但需要首先对原图像进行预处理。

2.4 基于混沌的图像加密技术

混沌由于具有与密码学非常近似的一些特性，近年来被广泛地应用于密码研究中。基于混沌的图像加密是 Fridrich 在 1997 年首先提出的，1998 年 Fridrich 又发表了一篇基于二维混沌映射的图像加密方案[7]，该方案首先使用二维的 Baker 映射进行像素位置的变换，而后又把该映射扩展成三维映射，对每个像素的值也进行了变换。在文[8]中 Chen 等人给出了一个基于三维 CAT 映射的图像加密方案，此方案利用三维 CAT 映射置乱图像像素位置，而利用其它混沌映射去混淆原图像与加密图像的关系。文[9]给出了一个基于连续混沌系统的图像加密方案，方案中利用多维连续混沌系统与 Hash 函数产生图像像素置乱矩阵和像素值变换矩阵。

3 图像置乱性能分析

对于不同的加密方案，根据像素位置及像素值的变换情况，可以划分为：(1)仅像素位置变换的图像加密；(2)仅图像灰度值变换的图像加密；(3)像素位置及灰度值都发生变换的图像加密。不同类型的变换，其置乱程度及加密安全性是不同的。下面给出的一些置乱评价参数——不动点比、信息熵、灰度平均变化值和自相关度，将可以用来对加密图像的置乱性能进行分析和评价。

在以下分析中，设 $G=(g_{ij})_{M\times N}$ 表示大小为 $M\times N$、灰度级为 L 的原图像，$C=(c_{ij})_{M\times N}$ 是 G 置乱后的图像，其中 g_{ij}、c_{ij} 分别表示图像 G 和 C 中像素点 (i,j) 的灰度值。

3.1 不动点比

定义 1 对于图像 G 和 C 中的像素点 (i,j)，若 $g_{ij}=c_{ij}$，则称像素点 (i,j) 为 C 相对于 G 的不动点。

定义 2 图像 C 相对于图像 G 的不动点总数占 C 中像素点总数的百分比，称为 C 相对于 G 的不动点比，其表示式为

$$BDD(C,G)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}f(i,j)}{MN}\times 100\% \tag{1}$$

其中 $f(i,j)=\begin{cases}1 & \text{若 } g_{ij}=c_{i,j}\\ 0 & \text{否则}\end{cases}$。

图像加密的目的是让加密图像与原图像尽可能“不同”，使加密图像“面目全非”。显然，一般情况下，两个图像的不动点比越小，加密图像与原图像区别就越大，置乱效果就越好。然而，在许多情况下，该参数只能有效地反映出两个图像对应点变化的数目情况，却不能反映出灰度值的变化程度。例如，若把图像 G 的每个像素点都加上常数 k，则 BDD(G,C)=0，不动点比是最低的，但是加密图像的置乱度并不高，安全性也很差。所以，该参数需要与下面参数一起才能正确反映出图像的置乱度。

3.2 信息熵

信息熵是 Shannon 在其信息论中提出的一个描述信息不确定性的概念[10]，也可以用来描述图像信息的不确定性。

定义 3 若 x_i 表示 L 级灰度图像的第 i 个灰度值，$P(x_i)$ 为图像中第 i 个灰度所占比例，且 $\sum_{i=1}^{L}p(x_i)=1$，则图像 G 的信息熵定义为

$$H(G)=-\sum_{i=1}^{L}p(x_i)\log_2 p(x_i) \tag{2}$$

根据上述定义，若图像 G 中所有点的灰度值都相同，则 $H(G)=0$；若图像中每个灰度所占比例完全相同，即 $p(x_1)=p(x_2)=\cdots=p(x_L)=1/L$，则 $H(G)=-\sum_{i=1}^{L}[\frac{1}{L}\times\log_2(\frac{1}{L})]=-L\times\frac{1}{L}\times(-\log_2 L)=\log_2 L$。因而，信息熵可以度量出图像中灰度值的分布情况，灰度分布越均匀，图像信息熵越大，反之信息熵就越小。

3.3 灰度平均变化值

图像加密后，许多点灰度值都会发生变化，不动点比从数量上反映了灰度变化情况，但不能反映出灰度变化的程度，因此并不能度量出加密图像的完全度。为了更好地度量加密图像中灰度变化程度，下面给出灰度变化平均值 GAVE。

定义 4 若图像 C 是图像 G 加密后的图像，则

$$GAVE(C,G)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|c_{ij}-g_{ij}|}{MN} \tag{3}$$

称为 C 相对于 G 的灰度变化平均值。其中 $M\times N$ 表示两个图像的大小。

根据定义，该参数在 G 与 C 相同时取最小值 0，而当加密图像为原图像的逆，即 $c_{ij}=L-g_{ij}$ 时，取最大值 L。显然，这两种情况的图像置乱效果及加密安全性都是最差的。因此，对于一个加密图像，并不是该值越大加密图像的置乱度及安全度就越高，而是两个图像灰度差变化越均匀，图像置乱性能越好。

3.4 图像的自相关度

图像数据与文本数据的最大区别是图像数据存在很强的相关性，许多相邻像素点具有相同的灰度或较小的差值。如果一个像素点及其相邻点，在置乱后仍然相邻，则很容易受到区域分析的攻击，降低加密图像的安全性。下面我们首先给出像素点 (i,j) 的 r-m 相关集的概念，而后再定义图像的 r-m 自相关度。

定义 6 设图像 $G=(g_{ij})_{M\times N}$ 是一个灰度级为 L 的图像，(i,j) 是其中的一个像素点，r、m 均为整数，且 $0<r\leqslant\frac{M}{2}$，$0\leqslant m<L$，则 $G_{i,j}^{r,m}=\{g_{k,l}\,|\,|i-k|\leqslant r,|j-l|\leqslant r,|g_{i,j}-g_{k,l}|\leqslant m\}$ 称为点 (i,j) 的 r-m 相关集，r 和 m 分别称为像素点间距和灰度差。

定义 7 设图像 $G=(g_{i,j})_{M\times N}$ 及集合 $G_{i,j}^{r,m}$ 如上所述，则图像 G 的 r-m 自相关性定义为

$$R^{r,m}(G)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|G_{i,j}^{r,m}|}{\sum_{i=1}^{M}\sum_{j=1}^{N}|G_{i,j}^{r,L}|}\times 100\%$$

其中 $|G_{i,j}^{r,m}|$ 表示集合 $G_{i,j}^{r,m}$ 的元素个数。

根据定义，该参数给出的是图像 G 中相邻区域内像素点的相关程度。在 r 与 m 不发生变化时，参数 R 值越小，图像 G 中像素点相关性越小，反之相关性就越大。

上述参数，虽然都从某些反面放映了图像的置乱度，但是都不能单一地确定图像的置乱度及安全性。例如：如果一个加密图像只是原图像改变像素位置的结果，那么其不动点数目、灰度变化平均值都可能具有较高的值，但是其信息熵是不会改变的，自相关度的改变也很小。因此，要评价加密图像的置乱性能或安全性需要对得到的参数结果进行综合分析。

4 模拟试验结果与分析

矩阵变换是图像加密中经常采用的加密方法之一，而基于混沌的图像的加密则是近几年图像加密研究中的热点。为了分析上文给出的图像置乱评价参数的性能，下面对基于

Aronold 变换、幻方变换、三维 Cat 映射及连续混沌系统的加密图像的置乱度及安全性进行分析。试验中加密原图像为 Lena. bmp(图 1. a)。

4.1 加密方案描述

(1)Aronold 变换

Arnold 变换是一种纯粹的像素位置变换，它通过下述变换实现图像加密

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$$

其中 $A=\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ 是变换矩阵。该变换通过把原图像中像素点 $\begin{pmatrix} x \\ y \end{pmatrix}$ 的像素值放到加密图像中像素点 $\begin{pmatrix} x' \\ y' \end{pmatrix}$ 实现加密。试验中，我们选用 $A=\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$，经过多轮迭代后加密图像为 Lena_A. bmp(图 1. b)。

(2)幻方变换

幻方变换与 Arnold 变换类似，也是利用变换矩阵来实现图像的加密。试验中选用的变换矩阵为 $A=\begin{pmatrix} 16 & 2 & 3 & 13 \\ 5 & 11 & 10 & 8 \\ 9 & 7 & 6 & 12 \\ 4 & 14 & 15 & 1 \end{pmatrix}$。加密步骤为：(i)把 lena. bmp 分成 64×64 个大小为 4×4 图像块，(ii)对每个图像块根据变换矩阵 A 进行置乱，消除相邻元素的相关性，(iii)对块置乱后的图像进行再进行行和列置换，消除元素相邻行和列的相关性。利用上述方法，经过一次迭代和两次迭代得到的加密图像为 Lena_HF1. bmp(图 1. c)和 Lena_HF2. bmp(图 1. d)。

(3)基于三维 Cat 映射的混沌加密

基于三维 Cat 映射的混沌加密方案是 Chen 等人于 2004 年提出的[8]，其加密思想为：(i)输入 128 位的密钥，分成 8 组，产生 3 维 CAT 映射参数及 Logistic 映射的初始条件和图像迭代操作初始值；(ii)把二维图像转换成若干个正方体图像；(iii)利用 3 维 CAT 映射把正方体图像置乱；(iii)利用 Logistic 映射产生图像迭代中的参数，并利用异或操作把置乱后的图像进行混淆；(iv)把置乱及混淆过的图像转换成二维的，形成加密图像。

从加密方案中可以看出，该方案经过多次混淆与置乱实现了图像加密，因而加密图像不但改变了原图像的像素位置，还改变了其灰度值。在密钥为“1234567890123456”和“1234567890123457”时，图像加密结果分别为 Lena_Cat1. bmp(图 1. e)和 Lena_Cat2. bmp(图 1. f)。

(4)基于连续混沌系统的图像加密

基于连续混沌系统的图像加密是文[9]中给出的一个新的图像加密方案，其基本思想是：首先利用对混沌初始条件极其敏感的 Hash 函数得到的置乱序列对图像进行行列置乱，而后再利用灰度置乱矩阵改变图像的灰度值，从而实现图像加密。

利用 Lorenz 混沌系统，在初条件分别为 $X_0=[-3.34321 \quad -1.98731 \quad 23.58721]$ 及 $X_0=[-3.34321 \quad -1.98731 \quad 23.58721]+10^{-10}$ 时加密得到的图像分别为 Lena_L1. bmp(图 1. g)和 Lena_L2. bmp(图 1. h)。

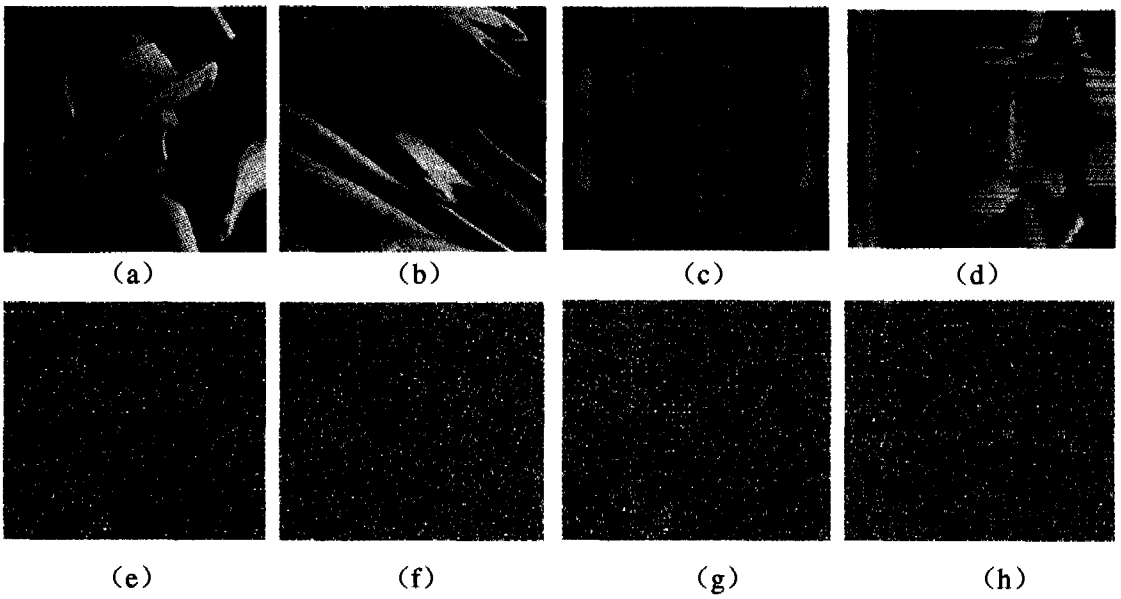

图 1 分析试验图像

4.2 置乱参数分析

(1)不动点比

根据不动点比的定义，各加密图像相对图像 Lena. bmp 的不动点比见表 1。

表 1 加密图像不动点比

图像	Lena_A	Lena_HF1	Lena_HF2	Lena_Cat1	Lena_Cat2	Lena_L1	Lena_L2
不动点比(%)	0.5127	1.8890	20.6787	0.4074	0.3921	0.3570	0.4058

从表中可以看出，除加密图像 Lena_HF2. bmp 具有较大的不动点比外，其余加密图像的不动点比都很低，这说明上述加密方案都极大地置乱了原始图像的像素点。进一步的试验还表明，对于幻方变换，在经过偶数次加密变换后，图像的不动点比都很大，而奇数次变换后的不动点比却很小，因此要想利用幻方变换加密图像，应把奇数次变换后的结果作为图像

加密结果。上述试验中，原图像的灰度级为256。若对于二值图像，理想的不动点比应该接近50%。

(2)信息熵

信息熵反映的是图像中的灰度分布情况，分布越均匀，信息熵越大，包含的不确定信息就越多。原图像与加密图像的信息熵见表2。

表2 加密图像信息熵

图像	Lena	Lena_A	Lena_HF1	Lena_Cat1	Lena_Cat2	Lena_L1	Lena_L2
信息熵	7.4462	7.4462	7.4462	7.9974	7.9971	7.9971	7.9970

从表2可以看出，基于Aronold变换及幻方变换的图像加密，加密图像的信息熵与原图像完全一样，这说明图像加密没有改变图像灰度值，只是进行了位置移动，攻击者只要恢复了像素点的位置也就可以破解加密图像。而基于混沌系统的两个图像加密方案，加密图像的信息熵基本上都等于256级灰度图像信息熵的最大值(8)，由此可知加密图像的灰度分布是非常均匀的，攻击者要想通过对像素值变化的统计分析对加密方案进行攻击，将是极其困难的。

(3)灰度平均变化值

不动点比从数量上反映了加密图像与原图像的象素变换情况，而灰度平均变化值则反映了变化的程度。加密图像灰度平均变化值见表3。

表3 加密图像灰度平均变化值

图像	Lena_A	Lena_HF1	Lena_HF2	Lena_Cat1	Lena_Cat2	Lena_L1	Lena_L2
灰度平均变化值	55.66	45.86	32.95	72.85	73.28	72.84	73.26

上述试验结果表明，基于混沌系统的两个图像加密方案，灰度变化平均值非常接近，远大于基于矩阵变换加密图像的灰度变化平均值，置乱效果良好。对基于混沌系统的两个加密方进一步分析表明，两个对应的加密图像灰度平均变化值分别为85.20和84.89，高于它们与原图像的灰度平均变化值。这一结果表明，基于混沌系统的加密图像对混沌初始条件是非常敏感的，初始条件的微小变化，加密图像就会发生极大改变。

(4)自相关度

图像数据与文本数据的主要区别是信息量大、数据自相关度高。加密图像应该降低图像的自相关度。在下面的试验中，计算了点间距 $r=1,2,3$，灰度差 $m=0,5$ 时的加密图像自相关度，结果见表4及表5。

表4 加密图像自相关度(m=0)

图像	Lena	Lena_A	Lena_HF1	Lena_HF2	Lena_Cat1	Lena_Cat2	Lena_L1	Lena_L2
r=1	0.2014	0.1908	0.1170	0.1559	0.1152	0.1151	0.1151	0.1152
r=2	0.1164	0.1078	0.0617	0.0781	0.0440	0.0440	0.0441	0.0442
r=3	0.0861	0.0786	0.0345	0.0563	0.0245	0.0244	0.0245	0.0246

表5 加密图像自相关度(m=5)

图像	Lena	Lena_A	Lena_HF1	Lena_HF2	Lena_Cat1	Lena_Cat2	Lena_L1	Lena_L2
r=1	0.6799	0.6387	0.1711	0.4473	0.1491	0.1492	0.1480	0.1498
r=2	0.5754	0.5309	0.2251	0.3388	0.0812	0.0807	0.0804	0.0814
r=3	0.5116	0.4660	0.1459	0.3121	0.0623	0.0620	0.0618	0.0627

从表中可以看出，在 $m=0$ 时，原图像和加密图像的自相关度都不高，并且加密图像的自相关度只是原图像的1/3～1/2。在 $m=5$ 时，除Lena_A.bmp和Lena_Hf2.bmp外，其余加密图像的自相关度都明显减小，并且在 $r=2$ 和 $r=3$ 时，两个基于混沌系统的加密图像的自相关度只是原图像的1/8～1/7。利用其它图像进行实验，得到的结果同样如此。这说明基于混沌系统的两个图像加密方案极大地降低了原图像的自相关度，具有很好的置乱效果。

结束语 近年来，图像加密技术的研究吸引了许多学者的注意，提出了许多图像加密方案。本文在对这些加密方案进行研究和分析的基础上，给出了多个置乱性能评价参数，并利用这些参数对几个图像加密算法进行了置乱性能分析。试验结果及理论分析表明，本文给出的几个加密图像置乱评价参数是实用的、有效的，可以用来对图像加密算法的置乱度及安全性能进行综合评价。对几个加密方案的分析结果还表明，仅采用像素位置置乱对图像进行加密，安全性是比较差的，而两个基于混沌系统的图像加密方案无论从不动点比和相关性，还是信息熵和灰度变化值都有很好的加密效果，并且加密图像对密钥都是非常敏感的，可以有效地用来对图像进行加密。

参考文献

1 李昌刚，韩正之，张浩然. 图像加密技术综述[J]. 计算机研究与发展，2002，39(10)：1317～1324

2 丁玮，闫伟齐，齐东旭. 基于Arnold变换的数字图像置乱技术[J]. 计算机辅助设计与图形学学报，2001，13(4)：338～341

3 李国富. 基于正交拉丁方的数字图像置乱方法[J]. 北方工业大学学报，2001，13(1)：14～16

4 Alvarez G，Montoya F，Romera M，Pastor G. Cryptanalysis of a chaotic secure communication system[J]. Physics Letters A，2003，306：200～205

5 Li S J，Zheng X. Cryptanlysis of a chaotic image encryption method[C]. Proceedings of ISCAS，2002，2：708～711

6 Martín del Rey A. A Novel Cryptosystem for Binary Images[J]. Studies in Informatics and Control，2004，13(1)：5～14

7 Fridrich J. Symmetric ciphers based on two-dimmesional，chaotic maps[J]. International Journal of Bifurcation and Chaos，1998，8(6)：1259～1284

8 Chen G，Mao Y B，Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos，Solitons and Fractals，2004，21：749～761

9 徐江峰，尚晋，胡静. 基于连续混沌系统和Hash函数的图像加密算法[J]. 计算机应用，2004，24(12)：61～63

10 Shannon C E. Communication theory of secrecy system[J]. Bell System Technical Journal，1949，28：656～715