一种基于共轭混沌映射的图像加密算法*)

韦鹏程[1,2] 张 伟[1,2] 杨华千[1,2]
(重庆大学计算机科学与工程学院 重庆 400044)[1]
(重庆教育学院计算机与现代教育技术系 重庆 400067)[2]

摘 要 本文应用离散混沌动力系统,针对图像数据的存储特点,设计了一种基于共轭混沌映射 Logistic 映射和 Tent 映射的图像加密算法。利用共轭映射产生密钥流改变原图像的灰度值;运用一类标准混沌映射,构造了一种具有强非线性藕合结构的置换方式,从而改变像素点的位置。同时,对提出的算法进行仿真实验和安全性分析,结果表明该算法具有安全性高和加密速度快等特点。

关键词 共轭混沌映射,Logistic 映射,Tent 映射,图像加密

An Image Encryption Algorithm Based on Coupled Chaotic Map

WEI Peng-Cheng[1,2] ZHANG Wei[1,2] YANG Hua-Qian[1,2]
(Department of Computer Science and Engineering, Chongqing University, Chongqing 400044)[1]
(Department of Computer and Modern Education Technology, Chongqing Education College, Chongqing 400067)[2]

Abstract In this paper, an image encryption algorithm based on the coupled digital chaotic map is proposed. Firstly, Grey substitution is designed via the key stream using the coupled chaotic , then use standard chaotic map to construct permutation pixels scheme. The algorithm comprises permutation and grey value substitution. Through experimental tests are carried out with detailed analysis, demonstrating the high security and fast encryption speed of the new scheme.

Keywords Coupled chaotic map, Logistic map, Tent map, Image encryption

1 引言

随着 Internet 技术和多媒体技术的飞速发展,多媒体通信逐渐成为人们进行信息交流的重要手段。越来越多的领域需要图像信息进行保密传输,如电话会议、有线电视、医学图像等。

传统的加密算法一般是基于文本数据设计的,它把一段有意义的数据流(称为明文)转换成看起来没有意义的数据(成为密文),如 DES 和 RSA[1]。由于将明文数据加密成密文数据,使得在网络传递过程中非法拦截者无法从中获得信息,从而达到保密的目的。虽然,我们可以把多媒体数据作为文本数据流一样看待,使用传统的加密算法进行加密;但是,然而,由于图像本身具有一些比如数据量大、像素点之间高相关性和高冗余性等特点,多媒体数据流具有的特性与文本数据的特性有很大不同。因此,目前的传统加密方法如 DES , 3-DES 或 RSA 等也很难满足多媒体应用中的实时性等要求。新型的多媒体应用需要新的数据加密技术。近年来,在这方面的研究取得了一些成果,主要针对视频数据和图像数据[8~10]。

图像加密技术有三种思想方法:灰度值替代,像素位置变换以及二者的组合[2~4]。灰度值替代是利用密钥改变源图像的灰度,可以逐点改变,也可以把源图像分成几块,逐块进行替代操作;像素位置变换是改变源图像中像素点的排列顺序;组合方法是加密过程中既有灰度值替代,又有像素位置的变换。在所有的加密算法中,都需要一个随机数产生器。离散的混沌系统由于容易实现,具有良好的统计特性,从而可以作为随机数发生器。混沌系统对参数和初始条件极其敏感,如果把系统的参数或初值作为密钥,混沌系统就成为一个具有优良密码特性的密码系统。混沌系统在二维相平面内的不规则性使得混沌系统更适合用于图像加密。

本文应用离散混沌动力系统,针对图像数据的存储特点,设计了一种基于共轭混沌映射 Logistic 映射和 Tent 映射的图像加密算法。这是一种把灰度值替代和像素位置变换相结合的方法。利用共轭混沌映射产生密钥流改变原图像的灰度值;运用一类标准混沌映射,构造了一种具有强非线性藕合结构的置换方式,从而改变像素点的位置。这种方法只进行一次这种置换操作,能够对所有的明文进行加密,从而提高了加密效率。所有的密钥都由混沌离散映射产生,因此算法没有因为增加了密钥设置而影响加密/解密的效率和速度。

2 混沌映射的拓扑共轭

混沌现象是一种有界的内在的随机过程,具有时间遍历性,这种过程既非周期性,又不收敛。任意相近的两点经过若干次混沌迭代之后,就会呈现指数发散,所以根据混沌序列很难确定混沌系统的初值和参数。另外,混沌轨道极其不规则,经过系统局部扩展、压缩、折叠之后,系统的输出类似于随机噪声。这些特点,都使得混沌映射很适合用来设计密码系统。

由于很多混沌映射具有拓扑共轭性质[5],比如 Logistic

*)基金项目:重庆市科委自然科学基金资助项目(CSTC,2005B2286),重庆市教委资助项目(No. kj051501),重庆教育学院重点项目。**韦鹏程** 博士研究生,主要研究方向为信息安全,混沌理论;**张 伟** 教授,博士后,主要研究方向为信息安全、计算智能与数据挖掘;**杨华千** 博士研究生,主要研究方向:信息安全,混沌数字水印。

映射就与改进的 Logistic 映射、Tent 映射以及 Chebyshev 映射等具有拓扑共轭关系。而这种拓扑共轭关系是一种等价关系，因此就可以重点地研究和分析其中的某几类混沌映射的性能。

定义 1 设 $x=h(\theta)$ 是连续、可逆的函数。对映射 $f(x)$ 作变换

$$g(\theta)=h^{-1}(f(h(\theta))) \tag{1}$$

或简记为 $g=h^{-1}\circ f\circ h$，则称(1)式为映射 $f(x)$ 到 $g(\theta)$ 的拓扑共轭变换。

当 f 与 g 拓扑共轭时，记为 $f\sim g$。拓扑共轭关系是一种等价关系，它满足下面三条性质：

① 反身性：f 与 f 是拓扑共轭的，即 $f\sim f$；

② 对称性：若 $f\sim g$，则 $g\sim f$；

③ 传递性：若 $f\sim g$，$g\sim\varphi$，则 $f\sim\varphi$。

具有拓扑共轭关系的两个映射实际上是不同坐标表示下的同一种映射，因此拓扑共轭变换具有一些不变性质。

性质 1 如果映射 $f(x)$ 和 $g(\theta)$ 具有拓扑共轭关系，则

$$g^{(n)}=h^{-1}\circ f^{(n)}\circ h$$

即 f 的迭代与 g 的迭代仍然存在拓扑等价关系。

推论 1 设有一对满足拓扑共轭变换的映射 f 和 g，如果 f 有 n 周期轨道，则 g 也有 n 周期轨道，且两者具有相同的稳定性，即 Lyapunov 指数。

对于 Logistic 映射：

$$f(x)=4x(1-x),x\in[0,1] \tag{2}$$

与 Tent 映射：

$$g(x)=\begin{cases}2x, & x\in[0,1/2]\\ 2(1-x), & x\in(1/2,1]\end{cases} \tag{3}$$

是具有拓扑共轭关系。

证明：考虑如下映射：

$$h(x)=\sin^2\frac{\pi x}{2},x\in[0,1]$$

易见 $h(x)$ 是[0,1]到[0,1]上的单调可逆映射，且

$$f\circ h(x)=4\sin^2\frac{\pi x}{2}(1-\sin^2\frac{\pi x}{2})=\sin^2\pi x$$

$$h\circ g(x)=\begin{cases}\sin^2\dfrac{\pi x\cdot 2x}{2}=\sin^2\pi x,x\in[0,\dfrac{1}{2}]\\ \sin^2\dfrac{\pi x\cdot 2(1-x)}{2}=\sin^2\pi x,x\in[\dfrac{1}{2},1]\end{cases}$$

即 $f\circ h(x)=h\circ g(x)=\sin^2\pi x$，于是有 $g(x)=h^{-1}\circ f\circ h(x)$，根据定义 1 可知 $f(x)$ 与 $g(x)$ 是拓扑共轭的。

拓扑共轭映射的密度分布也有着密切的关系。由“点数守恒”条件

$$\rho_T(\theta)\mathrm{d}\theta=\rho_L(x)\mathrm{d}x$$

得到：

$$\rho_L(x)=\rho_T(h^{-1}(x))\left|\frac{\mathrm{d}h^{-1}(x)}{\mathrm{d}x}\right|$$

注意 Tent 映射具有唯一不变的密度分布函数 $\rho_T(x)=1$，因为分布函数与初值无关，所以该映射一定是遍历(ergodic)的。又

$$h^{-1}(x)=\frac{2}{\pi}\arcsin\sqrt{x},x\in[0,1]$$

于是由式(3.17)得到 Logistic 映射的密度分布函数为

$$\rho_f(x)=\frac{1}{\pi\sqrt{x(1-x)}},x\in[0,1]$$

此外 Tent 映射的 Lyapunov 指数为 ln2，由拓扑共轭的性质可知道 Logistic 映射的 Lyapunov 指数也为 ln2。与下式(Lyapunov 指数定义)计算结果相同。

$$\lambda_L=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n}\ln|f'(x_i)|=\ln 2$$

利用概率密度函数，可以容易地计算出 Logistic 映射所产生的混沌序列一些统计特性：平均值：

$$\bar{x}=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N=i}x_i=\int_{-1}^{1}x\rho(x)=0 \tag{3}$$

对于自相关函数 $ac(m)$，当自相关间隔 $m=0$ 时，

$$\begin{aligned}ac(m)&=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N=1}x_1^2-\bar{x}^2\\&=\int_{-1}^{1}x^2\rho(x)-0=\int_{-1}^{1}\frac{x^2}{\pi\sqrt{1-x^2}}\mathrm{d}x\\&=\frac{1}{\pi[\arcsin x-0.5(\pi\sqrt{1-x^2}+\arcsin x)]}\Bigg|_{-1}^{1}=0.5\end{aligned} \tag{4}$$

当自相关间隔 $m\neq 0$ 时，

$$\begin{aligned}ac(m)&=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N=i}x_ix_{i+m}-\bar{x}^2=\int_{-1}^{1}xf^m(x)\rho(x)\mathrm{d}x-0\\&=0\end{aligned} \tag{5}$$

式中 $f^m(x)=f(f\cdots f(x)\cdots)$。

独立选取 2 个不同的初始值 x_{01} 和 x_{02}，它们分别产生 2 个混沌序列的互相关函数为：

$$\begin{aligned}ac_{12}(m)&=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N=i}x_{1i}x_{2i+m}-\bar{x}^2=\int_{-1}^{1}\int_{-1}^{1}x_1f^m(x_1)\rho\\&(x_1)\rho(x_2)\mathrm{d}x_1\mathrm{d}x_2-0=0\end{aligned} \tag{6}$$

式中 $f^m(x)=f(f\cdots f(x)\cdots)$。

从以上的统计特性可以看出，Logistic 映射在参数 $\mu=4.000$ 时产生的混沌序列均值为 0，自相关 δ 是函数，互相关为 0，其概率统计特性与白噪声是一致的。

3 算法设计

3.1 图像加密的框架图

对于任一图像 I，设 I 的大小由 $N\times N$ 个像素点构成，且 $I(x,y)$ 表示像素点 (x,y) 的灰度值。图 1 为基于共轭混沌映射的图像加密算法框架图。

3.2 像素置换设计

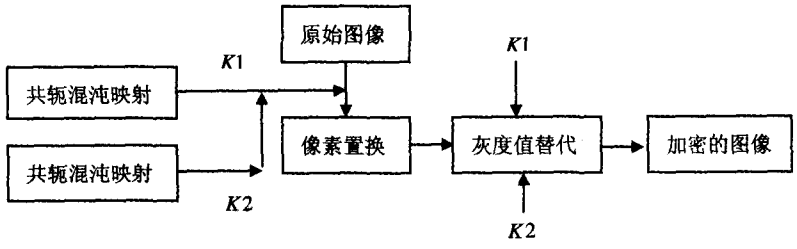


图 1 图像加密算法的框架图

借鉴混沌系统中的标准映射[4,6]

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} \mathrm{mod}(x_n + y_n, 2\pi) - \pi \\ y_n + p\sin(x_n + y_n) \end{pmatrix} \quad (7)$$

为了设计图像的置换变换，将式(8)推广成如下形式

$$i' = \mathrm{mod}(i + \Phi(j), M) \quad j' = \mathrm{mod}(j + \Phi(i'), N) \quad (8)$$

其中 i, j, i', j', M, N 是整数，

$$\Phi(j) = \mathrm{mod}(i, \lfloor j.k1_n + 0.5 \rfloor, N) \quad \Phi(i') = \mathrm{mod}(i', \lfloor i.k2_n + 0.5 \rfloor, M) \quad (9)$$

其中，$\lfloor x \rfloor$ 表示取 x 的整数部分，$k1_n, k2_n$ 为第 n 置换操作的密钥，n 为进行置换操作的次数。式(10)的逆为：

$$j = \mathrm{mod}(j' - \Phi(i'), N) \quad i = \mathrm{mod}(i' - \Phi(j'), M) \quad (10)$$

$k1_n, k2_n$ 是由共扼映射(2)和(3)产生的。利用式(8)可以对大小为 $M \times N$ 的图像进行置换加密操作，文[6]已经证明了式(8)的逆映射(10)的存在性，故可用(10)进行逆置换解密操作，所以算法是正确的。

3.3 灰度替代设计

设图像的灰度等级为 L，$I(i,j)$ 表示 (i,j) 位置的灰度值，$I'(i,j)$ 表示进行灰度替代之后 (i,j) 位置的灰度值，$k1_n, k2_n$ 是由共扼映射(2)和(3)产生的伪随机序列，令 $S_n = k1_n + K2_n$ 设计如下的灰度替代：

$$I'(i,j) = k1_n \oplus ((k2_n + I(i,j)) \bmod L), \quad \text{当 } S_n \text{ 为偶数}$$
$$I'(i,j) = k2_n \oplus ((k1_n + I(i,j)) \bmod L), \quad \text{当 } S_n \text{ 为奇数} \quad (11)$$

式(12)的逆变换为：

$$I(i,j) = k1_n \oplus ((I'(i,j) - k2_n) \bmod L) \quad \text{当 } S_n \text{ 为偶数}$$
$$I(i,j) = k2_n \oplus ((I'(i,j) - k1_n) \bmod L) \quad \text{当 } S_n \text{ 为奇数} \quad (12)$$

式(11)可以对大小为 $M \times N$ 的图像进行灰度替代的加密操作，可用(12)进行逆变灰度替代的解密操作，所以算法是正确的。

3.4 加密/解密算法

完成了灰度替代和置换设计之后，整个加密过程可以表示如下：

① 利用式(2)和(3)产生密钥流，利用式(8)进行置换设计变换；

② 利用式(2)和(3)产生密钥流，利用式(11)进行灰度替代变换；

③ 重复步骤①和② n 次。

解密过程是上述加密过程的逆过程：

① 利用式(2)和(3)产生密钥流，利用式(10)进行置换操作的逆；

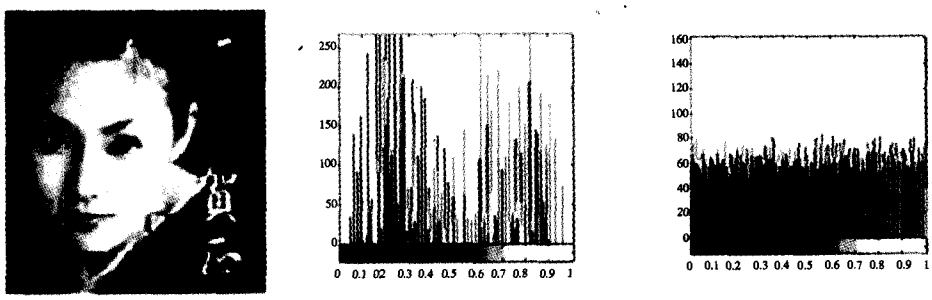
② 利用式(2)和(3)产生密钥流，利用式(12)进行灰度替代的逆操；

③ 重复步骤①和② n 次。

4 算法分析与模拟实验

4.1 密文分布分析

密文分布是一个密码系统最重要的特性之一，它将直接影响到密码系统的安全[7]。一个分布不均匀密文，往往是密码分析者进行唯密文攻击的首选入口。为更清晰地描述这一特性，我们用图像的直方图来表达。图像的直方图是图像的重要统计特征，它可以认为是图像灰度密度函数的近似。加密之前，图像 2(a)的直方图如同图 2(b)所示，加密之后，图像的直方图如图 2(c)所示。原图像的直方图分布不均匀，而密文图像的直方图分布极均匀，这说明通过加密算法，可以有效地改变图像各个像素之间的统计关系，使得密文图像能够有效抵抗统计分析和已知密文攻击。



(a) (b) (c)

图 2 (a)原图像；(b)原图像的直方图；(c)密文图像直方图

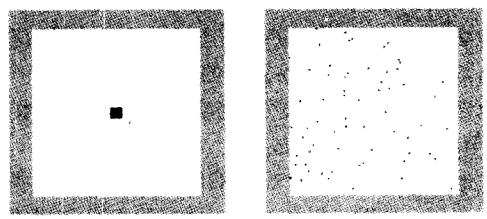
4.2 扩散性能分析

扩散是将每一位明文的影响尽可能地作用到较多的输出密文位中去，同时，还要尽量使得每一位密钥的影响也尽可能迅速地扩展到较多的密文位中去。其目的是有效隐藏明文的统计特性。置换设计(8)能有效地对明文进行扩散。我们用不动点数和像素相关性来衡量置换操作的性能。

(1)不动点数

不动点数[6]是置换操作前后，位置没有发生变化的像素点的数目。不动点越小，表明置换操作能够移动的像素点数目越多，加密效果越好。理想的置换操作能够移动所有的像素点，这样像素位置能够被有效地打乱。

对图 3 是加密扩散性测试。小黑点进行置换操作之后，小黑点经加密后均匀地分布到整幅图中，几乎所有的像素点都发生了变化。



(a) (b)

图 3 加密扩散性测试((a)黑点原图(b)黑点加密图)

(2)相邻像素的相关性

相邻像素的相关性[7]可反映图像像素扩散程度，相关性越大，扩散效果越差，相关性越小，扩散的效果越好。

(下转第 255 页)

14 Blieberger J. Discrete loops and worst case performance. Computer Languages, 1994,20(3):193～212
15 Kirner R. The Programming Language wcet C:[Technical report]. Vienna, Austria: Technische Universität Wien, 2002
16 Stappert F, Ermedahl A, Engblom J. Efficient Longest Executable Path Search for Programs with Complex Flows and Pipeline Effects. In: Proc. Int Conf. on Compilers, Architectures and Synthesis for Embedded Systems, Atlanta, Georgia, USA, 2001
17 Healy C A, Whalley D B. Automatic Detection and Exploitation of Branch Constraints for Timing Analysis. IEEE Transactions on Software Engineering, 2002. 763～781
18 Gustafsson J, Ermedahl A. Automatic derivation of path and loop annotations in object-oriented real-time programs. Parallel and Distributed Computing Practices, 1998, 1(2)
19 Gustafsson J. Worst Case Execution Time analysis of Object-Oriented Programs. In: Proc. 7th IEEE International Workshop on Object-Oriented Real-Time Dependable Systems (WORDS'02). January2002. 58～63

(上接第 239 页)

我们分别分析图像中水平相邻、垂直相邻和对角线相邻的两个像素相关性，因此，我们选择 1000 对相邻的像素点，然后用(13)，(14)公式来计算其相关性：

$$\mathrm{cov}(x,y)=E(x-E(x)(y-E(y)) \tag{13}$$

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}} \tag{14}$$

上两式中，x,y 代表图像中相邻的两个像素点的灰度值。且有，在数字计算中，用到以下离散公式：

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{15}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x)(y_i-E(y))$$

$$C(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{16}$$

表 1 为图像 2(a)加密前后相邻的像素灰度值的计算结果，从计算结果可知，图像加密后相关性相差很大。

表 1 图像加密前后的相邻像素灰度值的相关性比较

	加密前图像灰度值相关性	加密后图像灰度值相关性
水平方向	0.9674	0.00187
垂直方向	0.945	0.00097
对角线	0.9158	0.00082

从表 2 可以看出，置换操作之后，加密图像和原图像的相邻像素相关性发生了极大的变化，密文图像有很好的抵抗差分分析和线性分析的能力，保密性高。

4.3 混乱性能分析

混乱，是指密文和明文之间的统计特性的关系尽可能地复杂化，这也就是混沌映射通过迭代，将初始域扩散到整个相空间。灰度替换设计(11)能有效地对明文进行混乱。

灰度替代操作(11)实质上是对像素点进行混沌的加密操作，改变该点的像素值，从而打破明文中各点像素值之间的统计关系。图 4 是初始值的微小改变。将混沌系统的初值改变量 10^{-4} 时，对图像 2(a)加密后其密文间差值的分布情况。可以看出，灰度替换设计(11)能够使得图像中几乎所有的像素点的灰度值发生变化，是个比较理想的灰度替代操作。

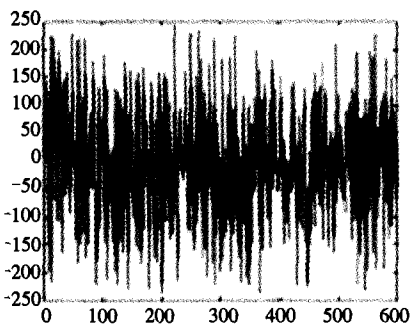


图 4 不同初值加密后的密文之间的差值

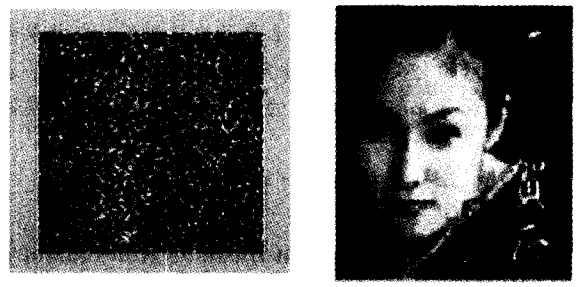


图 5 原图 2(a)的加密和解密图

4.4 算法正确性分析

由于算法中的像素置换操作和灰度替代操作都是可逆的，隐私算法具有可逆性，能够正确解密。因此在掌握正确密钥的情况下，能够对密文图像进行正确解密。图 5(a)和图 5(b)是图 2(a)的加密图和解密图。

结论 图像本身具有数据量大、像素点之间高相关性和高冗余性等特点，针对这些特点，本文应用离散混沌动力系统，设计了一种基于共轭混沌映射 Logistic 映射和 Tent 映射的图像加密算法。这是一种把灰度值替代和像素置换相结合的方法，实验表明，置换设计能有效地对明文进行扩散，灰度替换设计能有效地对明文进行混乱。算法符合密码学中加密算法准则，使得效率提高，便于实现。

参 考 文 献

1 Schneier B, 著. 吴世忠, 祝世雄, 张文政, 等译. 应用密码学. 机械工业出版社, 2001
2 Fridrich J. Image encryption based on chaotic maps. IEEE Int. Conf. Systm, Man&Cybernet ics Computational Cybernetics, Simulations, 1997. 1117～1120
3 Chuang T J, Lin J C. A new multiresolutiona pproach to still image encryption. Patern Recognition Image Anal , 1999, 9(3): 431～436
4 李昌刚, 韩正之, 张浩然. 一种随机密钥及"类标准映射"的图像加密. 计算机学报, 2003, 26 (4): 465～470
5 彭军. 混沌在网络信息安全中的应用研究:[博士论文]. 2003, 6: 27～40
6 樊春霞. 混沌保密通信系统的研究:[博士论文]. 2004, 10: 97～99
7 韦鹏程, 张伟, 杨华千. 一种多级混沌图像加密算法研究. 计算机科学, 2005, 32 (7): 172～175
8 Chang HKC, Liu JL. A linear quadtree compression scheme for image encryption. Signal Process Image Communation, 1997, 10 (4): 279～290
9 Chang C C, Hwang M S, Chen T S. A new encryption algorithm for image cryptosystems. J Syst Software, 2001, 58: 83～91
10 Cheng H, Li X B. Partial encryption of compressed images and videos. IEEE Trans Signal Process, 2000, 48(8): 2439～2451