文章编号：0253-2239(2010)02-0399-06

压缩图像的三维混沌加密算法

李 娟 冯 勇 杨旭强
(哈尔滨工业大学电气工程及自动化学院，黑龙江 哈尔滨 150001)

摘要 为保证数字图像的安全性，提出了一种压缩图像的三维混沌加密算法。该算法是通过对已压缩的数据流进行加密而实现的。首先采用基于小波的 Contourlet 变换的类等级树集合分割(SPIHT)编码算法对明文图像进行压缩，得到压缩数据流，然后将压缩数据流映射为一个三维位矩阵；利用 Lorenz 混沌映射产生混沌序列，并对其进行预处理得到比特值序列，根据比特值序列对上述三维位矩阵进行置乱和替代操作；将置乱和替代后的位矩阵重新映射为数据流，并对其进行解码和反变换操作，得到加密后的压缩图像。实验结果表明，产生的比特值序列具有较好的随机性，加密算法的密钥空间很大，对密钥非常敏感，子密钥和明文有关，能有效抵抗已知明文攻击，结合压缩技术，能有效提高存储和传输效率。

关键词 图像处理；加密算法；压缩图像；混沌映射
中图分类号 TP309.7 **文献标识码** A **doi**：10.3788/AOS20103002.0399

3D Chaotic Encryption Scheme for Compressed Image

Li Juan Feng Yong Yang Xuqiang
(*Department of Electrical Engineering, Harbin Institute of Technology, Harbin, Heilongjiang* 150001, *China*)

Abstract In order to ensure the security of digital image effectively, a 3D chaotic encryption scheme for compressed image is proposed. The scheme is realized by encrypting the datum stream achieved from compressing the original image. Firstly, the wavelet-based contourlet coding using an SPIHT-like algorithm is utilized on the plain image, and as a result, the compressed datum stream could be achieved which is then mapped to a 3D bit matrix. Afterward, a chaotic sequence is generated by Lorenz chaotic map, and it is preprocessed to a bit sequence which is used to permute and substitute the elements of the 3D bit matrix achieved above. In the end, the processed 3D matrix is mapped back to datum stream, and the encrypted compressed image could be achieved if decoding and inverse transform are performed on the datum stream. Experimental results show that the bit sequence generated by the chaotic sequence has a good randomicity and the proposed encryption scheme not only has a large key space but also is very sensitive to the security key. Moreover, its sub-key is relative to the plain image which could effectively resist the known-plaintext attack, and since the algorithm is carried out in the compressed domain it could increase the efficiency of storage and transmission.

Key words image processing; encryption scheme; compressed image; chaotic map

1 引 言

随着网络技术和数字图像技术的飞速发展，数字图像逐渐成为人们获取信息的重要来源，并成为人们生活的重要组成部分。为了提高传输大量图像信息的效率、保护数字图像的安全性，数字图像压缩和加密技术成为当前国内外研究的热点。根据加密对象的不同，可将图像加密方法分为两类：一类是在压缩域内对已压缩的数据流进行加密，另一类是对原始数据进行加密。前者的加密方法是对图像数据的变换系数矩阵进行处理，如果其中任何一个系数发生变化，就会引起图像原空间中的所有像素点发生变化。将图像压缩和加密技术有机结合，不仅实

收稿日期：2009-04-09；**收到修改稿日期**：2009-04-29
基金项目：国家自然科学基金(60474016 和 60774040)资助课题。
作者简介：李 娟(1982—)，女，博士研究生，主要从事图像处理方面的研究。E-mail：lijuan2001422@163.com
导师简介：冯 勇(1962—)，男，博士，教授，主要从事图像处理、混沌、滑模控制等方面的研究。E-mail：yfeng@hit.edu.cn

现了数据压缩，减小存储量和提高网络传输效率，而且具有较好的压缩效果，是图像加密技术一个重要的发展方向。目前常见的图像压缩算法主要有基于DCT变换和小波变换的压缩算法等[1~4]。Eslami等以Contourlet变换[5~7]为基础，相继提出了Contourlet域图像压缩编码方法[8]，如基于小波变换的Contourlet变换(WBCT)[9]和基于高频Contourlet变换等。混沌加密技术最早出现在19世纪80年代末，1998年Fridrich首次将混沌加密方法应用到图像加密中[10]，混沌加密以其良好的安全性、快速性已引起越来越多人的关注[11~14]。混沌在二维相平面上的不规则性，使得混沌系统非常适合用于图像加密。以灰度图像为例来说明提出的压缩图像的三维混沌加密算法。为了不影响压缩效果，对压缩后的数据流进行加密处理。首先利用基于WBCT的类SPIHT编码算法[9]得到压缩数据流；为了对其进行加密处理，将得到的压缩数据流映射为三维位矩阵；利用Lorenz混沌映射产生混沌序列，并对其进行预处理，根据预处理后的混沌序列对其进行置乱和替代操作；最后进行解码和逆变换实现压缩图像的加密。解密是图像加密的逆过程。

2 图像压缩算法

2.1 基于WBCT的压缩编码算法

为得到压缩后的数据流，采用压缩编码算法对明文图像进行压缩。由于提出的加密算法是将由0，1组成的数据流映射为三维位矩阵，并对该矩阵进行置乱和替代操作而实现加密的。因此所选择的压缩算法对源图像进行压缩编码后必须能产生由0，1组成的编码流，而SPIHT编码算法能够满足这一要求。并且，利用该压缩编码算法对源图像进行压缩，可得到较高的峰值信噪比(PSNR)，同时具有计算复杂度低、位速率容易控制等优点，因此选择SPIHT编码算法对源图像进行压缩处理。另外，之所以选择在WBCT域对图像进行压缩编码，是因为Contourlet变换是一种基于图像的几何性变换，能有效地表示轮廓和纹理丰富的图像，它弥补了小波变换在这方面的不足。由于拉普拉斯金字塔(Llaplacian pyramid，LP)分解存在数据冗余问题，不利于图像压缩编码，因此R. Eslami等[9]于2004年提出了一种基于WBCT的类SPIHT编码算法。下面简要介绍该编码算法。

WBCT的基本思想是用小波变换的Mallat塔式分解代替Contourlet变换中的LP分解，然后用方向滤波器组(dirctional filterband，DFB)分别对Mallat分解中的非LL子带进行卷积处理，原理如图1所示。图1中共进行了3次Mallat小波分解，第一次小波分解的高频(LH，HL和HH)子带方向分解数(层方向数)为4，共16×3个方向子带，第二、三次小波分解的层方向数都为3，共8×3×2个方向子带，LL子带层方向数为0(不分解)。

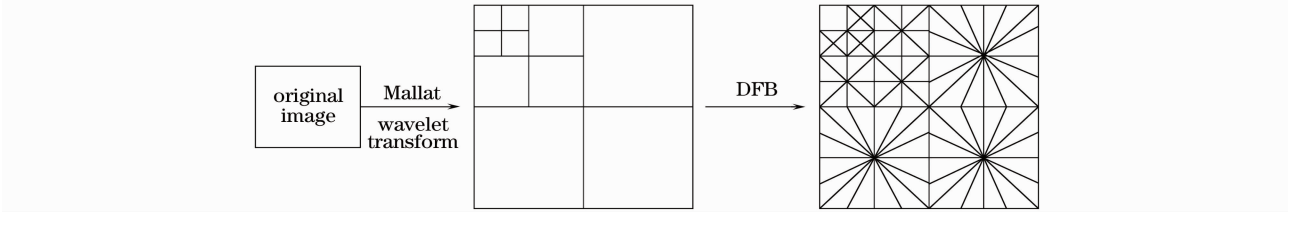

图1 WBCT原理示意图

Fig. 1 Sketch map of WBCT

由于WBCT各个方向子带的排列是横向和纵向分开，因此基于WBCT的类SPIHT编码算法的相邻两级方向子带系数对应关系如图2所示。为了更高效地进行SPIHT编码，按照图3所示调整子带之间数据放置结构，原先的方向子带排列如左图，阴影部分为纵向子带，同样标称的子带为同一个上一级小波子带的对应高频子带分解，将它们的排列重新安排为右图所示。

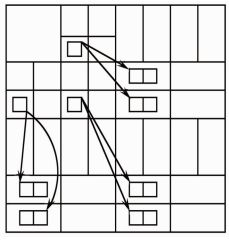

图2 相邻两级方向子带的系数对应关系

Fig. 2 Corresponding relation of coefficients of directional subbands in two adjacent levels

2.2 压缩数据流的预处理

假设明文图像的数据矩阵为$\boldsymbol{A}$，利用上述压缩算法对其进行编码，得到由0，1组成的压缩数据流

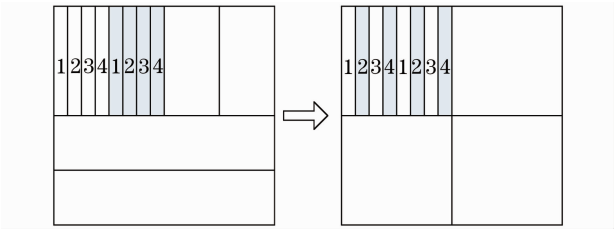

图 3　子带排列变化说明图

Fig. 3　Change of the permutation of subbands

$\boldsymbol{L}$,长度为 l。为方便对压缩数据流进行置乱和替代操作,需要对其进行预处理,将 $\boldsymbol{L}$ 映射为一个三维位矩阵 $\boldsymbol{B}$。令 $N = f(\sqrt[3]{l})$,其中 $f(x)$ 表示对 x 向下取整。如果 $N = \sqrt[3]{l}$,则三维位矩阵 $\boldsymbol{B}$ 的维数为 $N \times N \times N$,否则其维数为 $N \times N \times (N+1)$。若 $l < N \times N \times (N+1)$,则矩阵 $\boldsymbol{B}$ 的元素通过补零填充。假设压缩数据流的长度 $l = 71$,则由其映射得到的三维数据矩阵 $\boldsymbol{B}$ 如图 4 所示。矩阵 $\boldsymbol{B}$ 的维数是 $4 \times 4 \times 5$,图中的元素为数据流 $\boldsymbol{L}$ 中元素的序号。

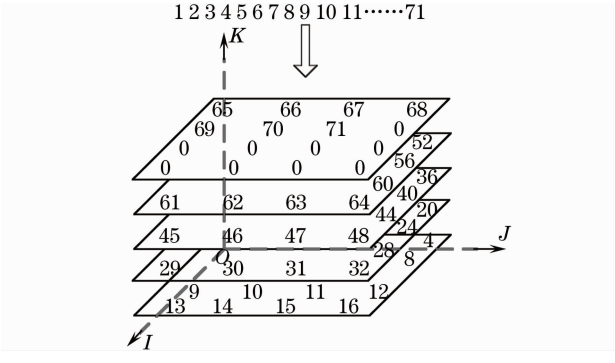

图 4　将数据流映射为三维位矩阵的示意图

Fig. 4　Datum stream is mapped to a 3D bit matrix

3　图像加密算法

提出的加密算法是通过预处理后的混沌序列对位矩阵 $\boldsymbol{B}$ 进行置乱和替代操作实现的,并选择 Lorenz 混沌映射产生所需的混沌序列。

3.1　混沌序列的预处理

Lorenz 混沌映射的动力学方程如下:

$$\begin{cases} \dot{x} = a(y-x) \\ \dot{y} = cx - xz - y, \\ \dot{z} = xy - bz \end{cases} \tag{1}$$

当 $a = 10, b = 8/3, c > 24.74$ 时,系统进入混沌状态。对 Lorenz 混沌映射模型进行迭代,得到的实数值混沌序列为 $\{x_k, k = 1,2,\cdots,p\}$,$\{y_k, k = 1,2,\cdots,p\}$ 和 $\{z_k, k = 1,2,\cdots,p\}$,迭代精度取为双精度。以 $\{x_k, k = 1,2,\cdots,p\}$ 为例来说明将实数值混沌序列改写为比特序列的方法。首先将混沌序列改写为 16 bit 的位序列:

$$|x_i| = b_1(x_i)b_2(x_i)b_3(x_i)b_4(x_i)\cdots b_{16}(x_i). \tag{2}$$

式中 $b_j(x_i)$ 是 $|x_i|$ 第 j 位整数。所得到的序列为 $\{b_j(x_i), j = 1,2,\cdots,16; i = 1,2,\cdots,p\}$。然后将 $b_j(x_i)$ 改写为比特值序列 $\{b'(x)_k, k = 1,2,\cdots,16 \times p\}$:

$$b'(x)_k = \begin{cases} 1 & r[b_j(x_i),2] = 1 \\ 0 & r[b_j(x_i),2] = 0 \end{cases}. \quad (k = 1, 2, \cdots, 16 \times p) \tag{3}$$

式中 $r(x,y)$ 表示 x 除以 y 后的余数。同理,可以得到由 $\{y_k, k = 1,2,\cdots,p\}$,$\{z_k, k = 1,2,\cdots,p\}$ 改写的比特值序列 $\{b'(y)_k, k = 1,2,\cdots,16 \times p\}$,$\{b'(z)_k, k = 1,2,\cdots,16 \times p\}$。对这 3 个比特值序列进行处理:

$$\begin{cases} b'(x,y)_k = b'(x)_k \oplus b'(y)_k, \\ b'(x,z)_k = b'(x)_k \oplus b'(z)_k, (k = 1,2,\cdots,16 \times p). \\ b'(y,z)_k = b'(y)_k \oplus b'(z)_k, \end{cases} \tag{4}$$

式中⊕表示进行异或操作,可以得到另外 3 个比特值序列 $\{b'(x,y)_k, k = 1,2,\cdots,16 \times p\}$,$\{b'(x,z)_k, k = 1,2,\cdots,16 \times p\}$ $\{b'(y,z)_k, k = 1,2,\cdots,16 \times p\}$,它们将被用于加密在 2.2 节得到的三维位矩阵。

3.2　加密算法设计

所提出的加密算法的密钥设计为 key:$[c, x_0, y_0, z_0, N_1, N_2, N_3, M, \text{sub-key}]$,其中参数 c 为 Lorenz 混沌映射的参数,x_0, y_0, z_0 为 Lorenz 混沌映射的初始值,N_1, N_2, N_3, M 为正整数,$M \in [0, 1000]$,sub-key 是由正整数组成的字符串。提出的加密过程如下:

1)将由压缩编码算法得到的三维位矩阵 $\boldsymbol{B}$ 看作是由 I 轴上的 N 个二维矩阵 $\{\boldsymbol{B}_i, i = 1,2,\cdots,N\}$ 组成,$\boldsymbol{B}_i$ 的维数是 $(N+1) \times N$,如图 5 所示;

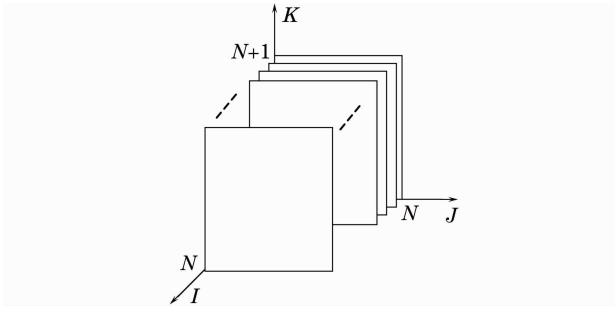

图 5　矩阵 $\boldsymbol{B}$ 由 N 个二维矩阵组成

Fig. 5　Matrix $\boldsymbol{B}$ is composed of N 2D matrices

2)令 $n = [1000 + N \times N \times (N+1)]$,以 a, b, c 为参数,x_0, y_0, z_0 为初始值,对 Lorenz 映射模型迭代 p 次可得到 3 个实数值混沌序列 $\{x_k, k = 1,2,\cdots,$

$p\}$,$\{y_k,k=1,2,\cdots,p\}$ 和$\{z_k,k=1,2,\cdots,p\}$,迭代精度为双精度;

3)令 $n_1=n-(M+N/16)+1$,$n_2=n-M$,取上述实数值混沌序列的一部分$\{x_k,k=n_1,n_1+1,\cdots,n_2\}$,$\{y_k,k=n_1,n_1+1,\cdots,n_2\}$ 和$\{z_k,k=n_1,n_1+1,\cdots,n_2\}$。按照上节的混沌序列的预处理方法将其转换成比特值序列$\{b'(x,y)_k,k=1,2,\cdots,N\}$,$\{b'(x,z)_k,k=1,2,\cdots,N\}$ 和$\{b'(y,z)_k,k=1,2,\cdots,N\}$。

4)根据比特值序列 $\{b'(x,y)_k,k=1,2,\cdots,N\}$ 实现对$\{\boldsymbol{B}_i,i=1,2,\cdots,N\}$ 的列元素的置乱和替代操作,算法如下:假设当前操作的二维矩阵为 $\boldsymbol{B}_i$,若 $b'(x,y)_k$ 为 0,则

$$\begin{cases} T=\boldsymbol{B}_i(k,j=1,2,\cdots,N) \\ \boldsymbol{B}_i(k,j=1,2,\cdots,N)=\boldsymbol{B}_i[(N+1)-k+1,j=1,2,\cdots,N], \\ \boldsymbol{B}_i[(N+1)-k+1,j=1,2,\cdots,N]=T \end{cases} \tag{5}$$

否则

$$\begin{cases} T=\boldsymbol{B}_i(k,j=1,2,\cdots,N) \\ \boldsymbol{B}_i(k,j=1,2,\cdots,N)=T\oplus\boldsymbol{B}_i[(N+1)-k+1,j=1,2,\cdots,N] \end{cases}. \tag{6}$$

5)为使密钥值与明文相关,利用子密钥 N_1 更新 M 的值:首先令 $N'_1=r(N_1,N+1)$,取 $\boldsymbol{B}_i(i>1)$ 平面上的第 N'_1 行的第 1~8 个比特值,将其转换成一个字节,若其值为 m,将 $M+m$ 赋值于 M;

6)重复步骤 3)~5),直到 I 轴上的所有二维矩阵都进行了相同操作,完成一次 I 轴上二维矩阵的置乱和替代操作;

7)将三维位矩阵 $\boldsymbol{B}$ 看作是由 J 轴上的 N 个二维矩阵$\{\boldsymbol{B}_j,j=1,2,\cdots,N\}$组成,$\boldsymbol{B}_j$ 的维数是$(N+1)\times N$,或者是 K 轴上的$(N+1)$个二维矩阵$\{\boldsymbol{B}_k,k=1,2,\cdots,N+1\}$组成,$\boldsymbol{B}_k$ 的维数是$(N+1)\times N$。J 轴和 K 轴上二维矩阵的置乱和替代操作与 I 轴类似,不同的是步骤 4)和 5)。在步骤 4),$\boldsymbol{B}_j$ 是利用 $b'(x,z)_k$ 实现置乱和替代的,$\boldsymbol{B}_k$ 则是利用 $b'(y,z)_k$ 实现的;在步骤 5),J 轴上的二维矩阵是利用子密钥 N_2 更新 M 的值,而 K 轴利用子密钥 N_3 更新 M 的值。

子密钥 sub-key 表示循环置乱和替代操作的次数。假设 sub-key:12345,则表示首先对 I 轴上二维矩阵进行 1 次置乱和替代操作,然后对 J 轴上二维矩阵进行 2 次置乱和替代操作,对 K 轴上二维矩阵进行3次置乱和替代操作,再对 I 轴上二维矩阵进行 4 次置乱和替代操作,对 J 轴上二维矩阵进行 5 次置乱和替代操作。

4 仿真结果

4.1 比特值序列的随机性检验

为了检验由实数值混沌序列所产生的比特值序列的随机性,对三组比特值序列进行了频数检验、序偶检验、扑克检验和游程检验。其中频数检验就是用来测试密钥序列中和的个数是否大致相同;序偶检验用于检验一段序列中相邻比特组成的序偶的分布特性;扑克检验是用来测试各种不同排列方式出现的次数是否均匀;游程检验又被称为脚检验,是一种非参数检验法,用来检验序列中是否存在自相关。检验结果如表 1 所示。

表 1 随机性测试结果

Table 1 Results of random test

Test object	Frequency test	Ordered-pair test	Poker test	Runs test
Test value corresponding to 5% significance level	3.84	5.99	279.2	1.96
$\{b'(x,y)_k,k=1,2,\cdots,N\}$	0.1111	2.1570	264.5714	0.0074
$\{b'(x,z)_k,k=1,2,\cdots,N\}$	0.3600	3.5868	228	1.0949
$\{b'(y,z)_k,k=1,2,\cdots,N\}$	0.1111	2.1387	246.2857	0.2600

由表 1 可知,所产生的比特值序列通过了随机性检验,具有较好的随机性能。利用该比特值序列对位矩阵进行置乱和替代操作,能够保证加密算法的安全性。

4.2 加密性能分析

为了测试所提出的加密算法,针对 256 pixel×256 pixel 的 Lenna 灰度图像进行加、解密仿真实验。图 6 为源图像,密钥为 key:[28.35,0.11,

0.21,0.32,30,42,61,20,12345],图 7 为加密后的重建图像,图 8 为正确解密的重建图像。其中压缩图像的压缩比率为 8.76,重建图像相对于源图像的峰值信噪比(PSNR)为 30.48 dB。

图 6　源图像

Fig. 6　Original image

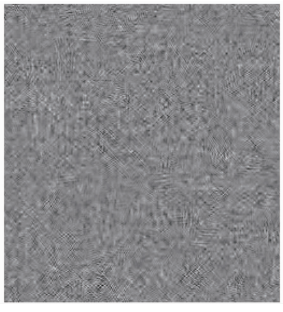

图 7　加密后的重建图像

Fig. 7　Encrypted reconstructed image

图 8　正确解密的重建图像

Fig. 8　Correctly decrypted reconstructed image

抵抗穷举攻击的有效方法是要求密码系统有足够大的密钥空间并且具有非常大的密钥敏感度,抵抗已知明文攻击的有效方法是令加密算法的密钥和明文相关。将所提出的加密方法和两种典型的图像加密算法在密钥空间、密钥是否与明文相关两个方面进行比较,结果如表 2 所示。由该表可以看出,所提出的加密方案的密钥空间只和密钥长度有关。理论上,在计算速度允许的前提下,子密钥 sub-key 的长度没有限制,因此该加密算法的密钥空间可以无限大,保证了加密的安全性。加密算法的密钥和明文有关,从而能有效抵抗已知明文攻击。

表 2　提出的加密方法与两种典型加密方法的比较

Table 2　Compare the encryption method proposed with other two typical encryption methods

Encryption method	Key space	Whether the security key is relate with plain-image
Image encryption proposed by this paper	Relate with the key length	Yes
3D Cat Map[15]	2^{128}	No
Image encryption based on chaotic maps[16]	2^{260}	No

为了测试密钥的敏感度,令 key_1:[28.35,0.11,0.21,0.32,31,42,61,20,12345],key_2:[28.351,0.11,0.21,0.32,30,42,61,20,12345],key_1,key_2 与 key 仅有微小差别,利用 key_1,key_2 对图 7 进行解密,解密图像如图 9 所示。由图 9 可知,key_1,key_2 均不能正确解密图像,即使解密密钥与正确的解密密钥仅有微小差别。由此看出,提出的加密算法对密钥非常敏感。

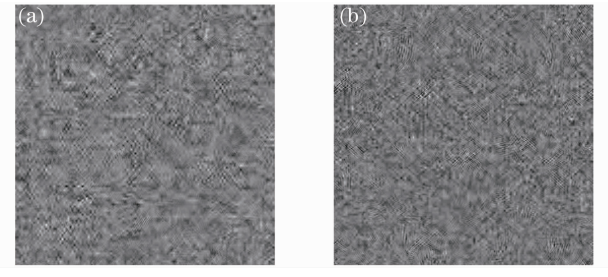

图 9　错误解密图像。(a)用 key_1 解密的图像;(b)用 key_2 解密的图像

Fig. 9　Incorrectly decrypted image. (a) Image decrypted by key_1; (b) Image decrypted by key_2

为了测试所提出加密算法的加密速度,针对不同大小的源图像,利用相同的加密和解密密钥进行加密以及解密实验,所用的时间如表 3 所示,表中的时间包括对图像进行编码和解码的时间。测试平台的硬件配置为:计算机的 CPU 主频为 1.8 GHz,内存2 GB;使用的编程软件是 VC6.0。

表 3　加密和解密时间

Table 3　Encryption and decryption times

Image size /pixel	Encryption /s	decryption /s
128×128	0.0340	0.0349
256×256	0.1718	0.1312
512×512	0.5623	0.6837

5 结 论

提出了一种压缩图像的三维混沌加密算法。该加密方案是对压缩后的数据流进行置乱和替代操作，因此并不影响压缩性能。将压缩和加密算法相结合，既能保证传输图像的安全性，又提高了图像的传输和存储效率。加密方案对密钥非常敏感，而且密钥空间与密钥长度有关，在理论上可以无穷大，抵抗穷举攻击能力较强。子密钥的设计使得加密密钥和明文有关，因此有效地提高抵抗已知明文攻击的能力。

参 考 文 献

1 Li Yunsong, Ma Jing, Wu Chengke. Three-dimensional orientation prediction-based wavelet transform for interference multi-spectral images compression[J]. *Acta Optica Sinica*, 2008, **28**(12): 2281～2287
李云松，马 静，吴成柯. 基于方向角预测三维小波变换的干涉多光谱图像压缩[J]. 光学学报，2008，**28**(12)：2281～2287

2 Wu Yingqian, Fang Tao, Shi Pengfei. Compression of hyperspectral images based on trellis coded quantization[J]. *Acta Optica Sinica*, 2004, **24**(12): 1633～1637
吴颖谦，方 涛，施鹏飞. 基于网格编码量化的超光谱图像压缩[J]. 光学学报，2004，**24**(12)：1633～1637

3 Jing Huang, Rihong Zhu, Jianxin Li *et al*.. Hyperspectral image compression using three-dimensional significance tree splitting [J]. *Chin. Opt. Lett.*, 2007, **5**(7): 393～396

4 Jiaxi Wu, Chengke Wu. Multispectral image compression using three-dimensional transform zeroblock coding[J]. *Chin. Opt. Lett.*, 2004, **2**(6): 325～327

5 R. Eslami, H. Radha. The contourlet transform for image denoising using cycle spinning[J]. *Conference Record of the Thirty-Seventh Asilomar Conference on Signals, Systems, and Computers. Pacific Grove*, USA. 2003, **2**: 1982～1986

6 Minh N. Do, Martin Vetterli. The contourlet transform: An efficient directional multiresolution image representation[J]. *IEEE Transactions on Image Processing*, 2005, **14**(12): 2091～2105

7 Liang Dong, Yin Bing, Yu Mei *et al*.. An algorithm for color image digital watermarking using the nonsubsampled contourlet transform[J]. *Acta Optica Sinica*, 2008, **28**(8): 1469～1474
梁 栋，殷 兵，于 梅 等. 基于非抽样 Contourlet 变换的彩色图像数字水印算法[J]. 光学学报，2008，**28**(8)：1469～1474

8 Yanjun Yan, Rajani Muraleedharan, Xiang Ye. Contourlet based image compression for wireless communication in face recognition system[C]. IEEE International Conference on Commutations, 2008. 505～509

9 R. Eslami, H. Radha. Wavelet-based contourlet coding using an SPIHT-like algorithm[C]. IEEE International Conference on Image Processing, 2004: 784～788

10 Fridrich. Symmetric ciphers based on two-dimensional chaotic maps[J]. *Int. J. Bifurcation and Chaos*, 1998, **8**(6): 1259～1284

11 Y. Mao, G. Chen, S. Lian. A novel fast image encryption scheme based on 3D chaotic baker maps[J]. *Int. J. Bifurc. Chaos*, 2004, **14**(10): 3613～3624

12 M. Salleh, S. Ibrahim, I. F. Isnin. Enhanced chaotic image encryption algorithm based on baker′s map[C]. IEEE Conference Circuits and System, 2003, 508～511

13 Kwok-Wo Wong, Bernie Sin-Hung Kwok, Wing-Shing Law. A fast image encryption scheme based on chaotic standard map[J]. *Phys. Lett. A*, 2008, **372**(15): 2645～2652

14 Bo Mi, Xiaofeng Liao, Yong Chen. A novel chaotic encryption scheme based on arithmetic coding[J]. *Chaos, Solitons and Fractals*, 2008, **38**(5): 1523～1531

15 Guanrong Chen, Yaobin Mao, Charles K. Chui. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. *Chaos, Solitons and Fractals*. 2004, **21**(3): 749～761

16 S. Behnia, A. Akhshani, H. Mahmodi *et al*.. A novel algorithm for image encryption based on mixture of chaotic maps[J]. *Chaos, Solitons and Fractals*, 2008, **35**(5): 408～419