文章编号:1001 - 9081(2011)03 - 0771 - 03
doi:10.3724/SP.J.1087.2011.00771

基于混沌映射的图像 Contourlet 编码加密算法

顾国生,刘富春
(广东工业大学 计算机学院,广州 510006)
(guguosheng@gmail.com; liufch@gdut.edu.cn)

摘　要:针对图像 Contourlet 多级树集合分裂编码的安全性问题,利用混沌密码设计了一种新的图像加密算法。使用具有良好随机性、安全性的混沌映射构造置乱数组和混沌密钥流对图像进行加密,由两个步骤组成:基于有序扫描表的快速置乱算法;基于编码扫描输出比特的异或加密算法。经实验验证,该算法能对图像视觉内容达到良好的掩密效果,具有密钥敏感度高、加密速度快、安全性高的优点。

关键词:Contourlet 变换;加密;混沌映射
中图分类号: TP309.2　　**文献标志码**:A

Contourlet domain image encryption based on chaos mapping

GU Guo-sheng, LIU Fu-chun
(*Faculty of Computer, Guangdong University of Technology, Guangzhou Guangdong* 510006, *China*)

Abstract: Concerning the security of the Contourlet-based set partitioning in hierarchical trees compression method, a new image encryption algorithm based on chaos mapping was proposed. The presented algorithm contained two steps: ranked tables permutation using chaotic scrambling arrays; bit streams XOR processing using chaotic binary streams. The simulation results indicate that the cipher image satisfies requests for content masking. It also demonstrates that the proposed algorithm is sensitive to the initial values and has fast speed and high security.

Key words: Contourlet transform; encryption; chaos mapping

0　引言

随着 Internet 和多媒体技术的发展,数字图像成为了信息表示和传输的重要形式,其安全性越来越受到人们的重视。作为一种新的多尺度几何分析工具,轮廓波(Contourlet)变换[1]近年来开始在图像编码和分析领域得到了广泛的关注与应用。这是由于轮廓波变换不但具有小波变换的多分辨分析和时频局部能力,而且具备了比小波变换更优异的各向异性,能更有效地捕获图像的边缘、轮廓和纹理等高维奇异几何特征。

在轮廓波变换的基础上,Eslami 等人提出了基于小波的轮廓波变换(Wavelet Based Contourlet Transform, WBCT)[2-3],结合小波变换和方向滤波构造图像编码算法。文献[4]中提出了对图像小波变换高频子带进一步作 Contourlet 分解,然后作类多级树集合分裂编码(Set Partitioning in Hierarchical Trees, SPIHT)的算法,获得了比小波 SPIHT 好的编码效果。文献[5 - 6]中则完全参照小波 SPIHT 编码算法过程提出了基于 Contourlet 变换域零树结构的 SPIHT(Contourlet-Based SPIHT, CSPIHT)编码算法,获得了优异的编码效率。与此同时,基于 Contourlet 变换的图像编码加密算法也日渐受到关注。

在数字图像的各种加密算法中,混沌密码技术[7-8]由于其具有高效安全的特点,即对初始参数敏感依赖,可完全重现性、遍历性、非周期性以及类噪声等优良特性,特别适合于保密通信和图像加密领域的应用。文献[9]中将 WBCT 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对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,得到加密码流。

针对 CSPIHT 编码算法,本文提出一种在 Contourlet 变换域与编码结构相结合的加密算法。根据 Shannon 信息理论对数据加密安全性的扩散和置换的两个基本要求,本文加密算法主要由两部分构成:基于 CSPIHT 算法空间方向树有序扫描表的置乱过程,用于实现扩散的要求;基于编码输出比特的异或加密过程,用于实现置换的要求。

在设计扩散和置换两个过程中,充分利用混沌系统的密钥敏感性,保证了加密图像视觉内容的不可见性和数据安全性,并通过仿真实验进行了验证。

1　混沌映射

数值混沌映射[7-8]具有非常适合于作为密码系统的特性:遍历性、混合性、非周期性以及对初值的敏感依赖特性等。近 10 年来混沌理论在数据安全保密方面得到广泛的应用。

常用的数值混沌系统包括:

一维 Logistic 映射:

$$f(x) = \mu x(1-x);\ x \in (0,1) \tag{1}$$

当 $3.99465 < \mu \leqslant 4$ 时,该映射处于混沌状态。

具有一次耦合项形式的二维 Logistic 映射:

$$\begin{cases} x_{n+1} = 4\mu_1 x_n(1-x_n) + \gamma y_n \\ y_{n+1} = 4\mu_2 y_n(1-y_n) + \gamma x_n \end{cases} \tag{2}$$

在 $\mu_1 = \mu_2 = 0.89$, $\gamma = 0.1$ 时系统是混沌的。

混沌映射阶数越高,安全性也越高,相应的计算复杂度也越高。

2　离散 Contourlet 变换

2002 年 Do 等人[1]提出了一种新的多分辨分析框架——

收稿日期:2010 - 09 - 16;**修回日期**:2010 - 11 - 23。　**基金项目**:国家自然科学基金资助项目(60974019)。

作者简介:顾国生(1978 -),男,广东云浮人,讲师,主要研究方向:信息安全、多媒体应用;　刘富春(1971 -),男,江西赣县人,副教授,主要研究方向:系统控制、计算机理论。

Contourlet 变换，也称为金字塔型方向滤波器组（Pyramidal Directional Filter Bank，PDFB）。Contourlet 变换具有良好的多分辨率、局部化和方向性等优良性质，与小波相比更适合于捕捉高维奇异点信息。

二维离散 Contourlet 变换由两个独立的步骤完成，分别是拉普拉斯金字塔（Laplacian Pyramid，LP）和方向滤波器组（Directional Filter Bank，DFB）变换。图 1 显示了使用离散 Contourlet 变换进行二维图像分解的过程。

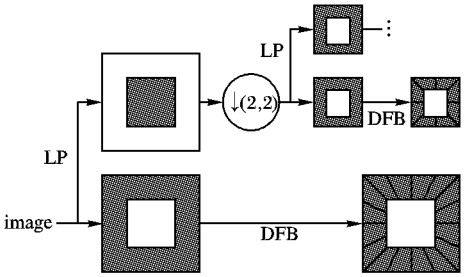

图 1 离散 Contourlet 变换分解示意图

Contoulet 变换首先使用 LP 滤波器[10]对原图像进行子带分解，捕获二维图像信号中存在的奇异点。一次 LP 分解将原始图像信号分解为原信号的低频逼近分量和原信号与低频信号的差值，即高频分量。这一过程在低频逼近图像上可重复进行，从而将原图像分解为多分辨分解图像。

LP 变换后，Contourlet 变换接着使用方向滤波器组 DFB 对 LP 变换中获得的高频分量进行方向变换，将同方向上的奇异点进行汇集，得到 Contourlet 变换系数。

数字图像经过 Contourlet 变换后的子带系数分布规律和小波变换有许多相似之处。在 Contourlet 系数矩阵中，系数幅值总体而言从低频子带到高频子带是逐渐衰减的。文献[5-6]中指出，如果对 DFB 选择适当的方向分解数（如进行 l 层分解，每一层高频子带 DFB 分解的方向数设定为下一层分解的方向数的 2 倍，由高至低分别含有 4 个方向子带，8 个方向子带，16 个方向子带，…，2^l 个方向子带），则构建出的 Contourlet 系数矩阵具有“零树”特征，因此可参照小波变换进行嵌入式位平面编码，获得优异的编码效率。图 2 给出了这种分解方式下系数矩阵所形成的零树结构。

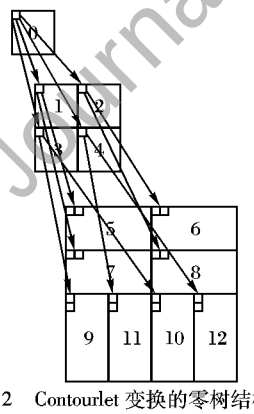

图 2 Contourlet 变换的零树结构

文献[5-6]中参照 SPIHT 算法（基于小波零树结构）编码过程，基于上述的 Contourlet 零树（Spatial Orientation Tree，SOT）结构提出了 CSPIHT 算法。和 SPIHT 算法类似，CSPIHT 编码算法构造了 3 个链表：不重要系数链表（List of Insignificant Pixels，LIP）、不重要集合链表（List of Insignificant Sets，LIS）和重要系数链表（List of Significant Pixels，LSP），用于存放编码过程数据。

3 图像加密算法

为了便于描述加密算法，引入如下符号表示：

$O(i,j)$ 表示节点 (i,j) 所有孩子的坐标集；

$D(i,j)$ 表示节点 (i,j) 所有子孙（包括孩子）的坐标集；

H 表示低频子带所有树根的集合；

$L(i,j)=D(i,j)-O(i,j)$，即节点 (i,j) 所有非直系子孙的坐标集。

最初坐标集由 $LIS=\varnothing$、$LIP=\{(i,j)\mid(i,j)\in H\}$ 及 $LIS=\{D(i,j)\mid(i,j)\in H$且具有非零子孙$\}$ 组成，初始阈值 $T=2^{\lfloor \mathrm{lb}(\max(|c(i,j)|)) \rfloor}$。

根据 Shannon 信息理论的扩散和置换两个基本要求，图像加密算法将由两部分构成，加密过程融合在 CSPIHT 编码过程中。

3.1 置乱算法

置乱算法作用于编码中的两个环节，实现 Shannon 信息理论的扩散要求。

1）对初始化的 LIP 表的置乱。

CSPIHT 编码开始时，LIP 表被初始化为顺序扫描低频子带系数即所有树根的坐标集 $LIP=\{(i,j)\mid(i,j)\in H\}$。如果 (i,j) 是重要系数，输出重要性比特‘1’及其符号位，并将 (i,j) 移到 LSP 表尾部；否则输出‘0’。

设初始 LIP 表的元素个数为 m，记为 $\{\tau_i\}_{i=1}^{m}$。用混沌映射构造一个长度为 m 的置乱数组 $\{\varphi_i\}_{i=1}^{m}$，对初始 LIP 表 $\{\tau_i\}_{i=1}^{m}$ 进行置乱。置乱步骤为：将 $\{\varphi_i\}_{i=1}^{m}$ 进行升序排列，得到 $\{\varphi_{j_i}\}_{i=1}^{m}$。对 $i=1,2,\cdots,m$，根据排序前后对应的位置编号将元素 τ_i 移动到位置 j_i。

注意到，初始 LIP 表的元素置乱还直接影响并改变了对应的系数重要性符号编码及其相应后续的 D、L 型表项分集处理顺序（见下述的步骤 2））。因此，对初始 LIP 表的置乱实质上是实现了对以 LIP 表中元素对应的低频系数为根的子树之间的置乱。

2）对 LIS 表的 D、L 型表项分集数据的置乱。

当 D 型表项 $D(i,j)$ 是对当前阈值是重要的，将输出重要性比特‘1’，并根据分集规则将 $D(i,j)$ 分解成 $L(i,j)$ 和 4 个单节点 $(k,l)\in O(i,j)$，若 $L(i,j)\neq\varnothing$，移到 LIS 表尾部，并处理 4 个子节点：若 (k,l) 是重要系数，添加到 LSP 表尾部，并输出‘1’及其符号位；否则添加到 LIP 表尾部，输出‘0’。用混沌映射构造一个长度为 4 的置乱数组，对这 4 个子节点进行置乱。和步骤 1）类似的分析，对 $D(i,j)$ 4 个子节点的置乱实质上是对以这 4 个子节点为根的子树进行置乱。

当 L 型表项 $L(i,j)$ 是对当前阈值是重要的，将输出重要性比特‘1’，并将 $L(i,j)$ 从 LIS 表中移出，分解成 4 个 D 型表项 (k,l)，$(k,l)\in O(i,j)$，并将它们添加到 LIS 表的尾部；否则输出‘0’。使用混沌映射构造一个长度为 4 的置乱数组，对这 4 个 D 型表项 (k,l) 进行置乱。同上，对 4 个表项的置乱实质上是对以每个 (k,l) 为根的子树进行置乱。

3.2 异或加密算法

CSPIHT 在编码第 i 轮（$i=1,2,\cdots,n$）扫描中，处理完 LIP 表、LIS 表后，对 LSP 表的扫描输出非本轮扫描新添加系数的第 i 个位平面比特。

于是，编码过程中对 LIP、LIS、LSP 这 3 个链表扫描，产生了 6 种类型的比特数据：LIP 系数重要性比特及系数符号比特；D 型表项重要性比特、其孩子系数重要性比特及符号位比

特;L 型表项重要性比特;LSP 系数位平面比特。本文使用高效的异或运算设计加密算法。设编码输出的比特序列为 X_i $(i=1,2,\cdots,s)$,采用混沌函数生成一个二值混沌序列 C_i $(i=1,2,\cdots,s)$,与输出比特序列作异或加密运算,实现 Shannon 信息理论的置换要求。

$$X'_i = X_i \oplus C_i;\ i = 1,2,\cdots,s \tag{3}$$

注意到在解码过程中,将会使用这些比特逆向构造空间方向树。特别地,如果加密改变了其中的 LIP 系数重要性比特、D 型表项重要性比特和 L 型表项重要性比特,则不但影响了它们自身的值,还改变了它们相应子树的分布和重构过程,也连锁地改变了后续比特的含义。因此,如果需要进一步降低加密的开销,则可以选择此部分比特进行加密,就已经可以达到良好的加密效果。

4　仿真实验与分析

采用 256×256 的灰度图像 Lena 作为测试图像。图 3 给出了利用本文算法对 Lena 图像进行完全加密的结果。从图 3(b)来看,加密后的图像已经无法识别出原图像的任何信息。图 3(c)和(d)给出了加密前后图像的灰度统计直方图。由图 3(c)和(d)可知,原图和密图的灰度统计直方图完全不同,并且密图直方图中的灰度均匀分布,完全消除了原图像中的灰度统计分布特征,这说明加密算法有效实现了 Shannon 信息加密理论扩散和置换的两个要求。

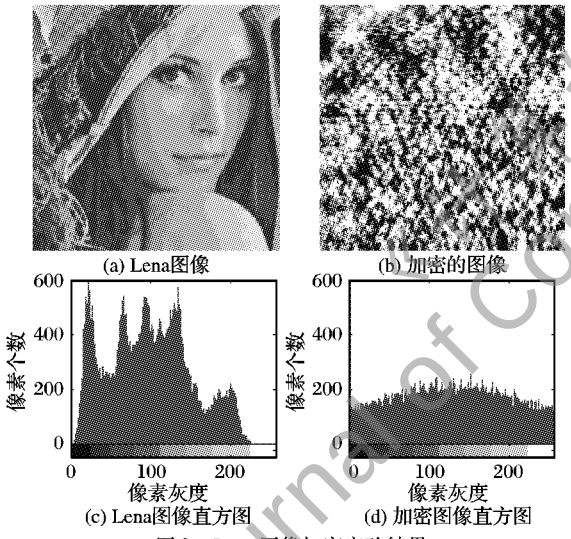

图 3　Lena 图像加密实验结果

根据实验结果对算法的性能进行分析。

1)安全性分析。

本文算法由基于扫描有序表数据的置乱和扫描输出比特加密两部分组成,实现了 Shannon 理论的置换和扩散两个要求。由于采用对初始参数极其敏感的混沌密钥流来构建置乱矩阵和流密码,算法安全性由选用的混沌密码保证。混沌初始参数敏感性是指给定的初始密钥尽管有很微小的差别,但所产生的混沌序列却有特别大的差别,因此密钥稍有偏差则不能正确解密图像。图 4(a)是使用正确的混沌密钥所获得的解密图像,而图 4(b)是使用错误密钥(将混沌参数由0.1改为 0.100 01,仅相差 10^{-5})所获得的解密图像。可以看到,得益于混沌初始参数的敏感性,图 4(b)不能还原出任何原图像的信息。

用均方误差(Mean Square Error, MSE)衡量解密图像和原图像之间的差别,分别使用不同初始参数的敏感性统计实验结果列于图 5。从图 5 可知,正确密钥 0.1 对应的 MSE 值为 0,即图像被正确解密,其他错误密钥(分别与正确密钥相差 10^{-2}、10^{-3}、10^{-4}、10^{-5})的解密图像与原图像的 MSE 值均很大,超过 10^5,说明无法正确解密。

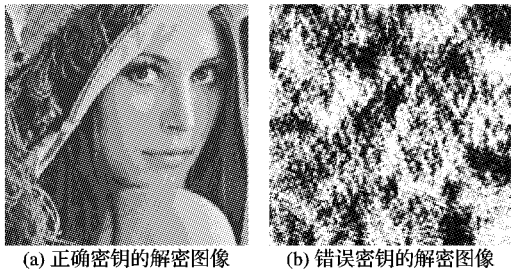

图 4　Lena 图像解密实验结果

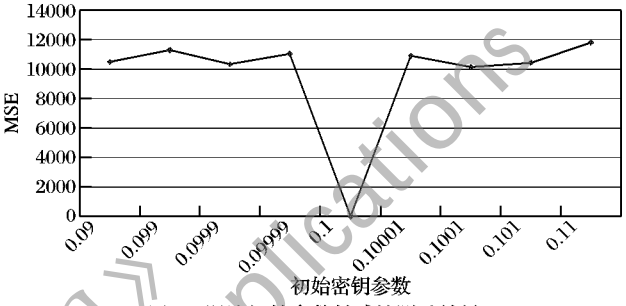

图 5　混沌初始参数敏感性测试结果

2)对编码效率影响分析。

对扫描有序表数据的置乱过程实质上是仅改变了相应节点为根的子树扫描顺序,没有增加新的数据,因此对编码效率没有影响。而对扫描输出比特的异或加密运算,也不会对编码效率造成影响。

3)对编码时间影响分析。

本文的加密算法中的置乱单元中,采用高效的混沌映射,可快速构建置乱矩阵。例如,将 256×256 的 Lena 标准图像按图 2 方式分解,初始 LIP 表的置乱仅需要使用 1 个长度为 32×32=1 024 的置乱数组,对 D 型表项和 L 型表项数据的置乱均使用长度为 4 的置乱数组。置乱数组规模小,效率很高。搭配采用高效异或运算的替换单元,对编码时间影响较小。

设编码时间影响率为 γ,不包含加密过程时(即原 CSPIHT 算法)熵编码编码时间为 T_1,包含加密时熵编码时间为 T_2,则:

$$\gamma = \frac{T_2 - T_1}{T_1} \tag{4}$$

表 1 给出了本文算法对多幅标准图像编码时间影响的实验结果。

表 1　置乱算法对编码时间的影响

实验图像	编码时间影响率 γ/%
Lena	9.5
Barbara	8.7
Baboon	8.3
Cameraman	9.2
Goldhill	10.6
Indor2	7.5
Peppers	8.8

5　结语

本文提出了一种在 Contourlet 变换域与编码过程相结合的加密算法。根据CSPIHT算法中Contourlet变换空间方向

(下转第 777 页)

表 1　三种方案在最坏情况下需要搜索路由器个数(完全部署)

方案	$d=5$		$d=10$		$d=15$		$d=20$		$d=25$		$d=30$	
	$N_i=64$	$N_i=128$	$N_i=64$	$N_i=128$	$N_i=64$	$N_i=128$	$N_i=64$	$N_i=128$	$N_i=64$	$N_i=128$	$N_i=64$	$N_i=128$
本文方案	1	1	3	3	5	5	6	6	8	8	10	10
Gong 等人[8]的方案	126	254	315	635	441	889	630	1 270	756	1 524	945	1 905
SPIE	315	635	630	1 270	945	1 905	1 260	2 540	1 575	3 175	1 890	3 810

表 2　三种方案在最坏情况下需要搜索路由器个数(一半部署)

方案	$d=5$		$d=10$		$d=15$		$d=20$		$d=25$		$d=30$	
	$N_i=64$	$N_i=128$	$N_i=64$	$N_i=128$	$N_i=64$	$N_i=128$	$N_i=64$	$N_i=128$	$N_i=64$	$N_i=128$	$N_i=64$	$N_i=128$
本文方案	126	254	315	635	441	862	630	1 270	756	1 524	945	1 905
Gong 等人[8]的方案	3 969	16 129	7 938	32 258	—	—	—	—	—	—	—	—
SPIE	7 938	32 258	19 845	80 645	—	—	—	—	—	—	—	—

4.3　渐进性部署

从重构速度和误报率可以看出,本文方案在未完全部署的情况下仍然保持良好的性能。但 Gong 等人[8]的方案在未完全部署下对重构速度产生了严重的影响,而且误报率也非常大。SPIE 方案虽然不会产生严重的误报,但重构速度比 Gong 等人[8]方案还要慢很多。

5　结语

本文主要在 Gong 等人[8]的方案基础上,对交替使用日志记录和包标记的方法进行改进,提出了使用路由器的接口信息来标志一个路由器,缩短了原方法中的标记长度,并灵活地根据路由器部署追踪方案情况来选择是否做日志记录操作,从而提高了重构的速度,降低了误报率,并能更好地适应渐进式的部署。日后的研究工作包括:1)如何在标记信息中加入认证的信息,以防止欺骗的信息写入;2)如何减少日志操作的次数以降低路由器存储负担。

参考文献:

[1] SAVAGE S, WETHERALL D, KARLIN A, *et al*. Practical network support for IP traceback [C]// Proceedings of the ACM SIGCOMM 2000 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication. New York: ACM Press, 2000: 295 - 306.

[2] 曲海鹏,冯登国,苏璞睿. 基于有序标记的 IP 包追踪方案[J]. 电子学报,2006,34(1):173 - 176.

[3] 徐劲松. 一种改进的路由包标记追踪方案[J]. 计算机应用,2009,29(5):1316 - 1320.

[4] 徐劲松. 一种改进的数据包追踪方案——CDPM[J]. 计算机应用,2009,29(12):3185 - 3187.

[5] XIANG Y, ZHOU W L, GUO M Y. Flexible deterministic packet marking: An IP traceback system to find the real source of attacks [J]. IEEE Transactions on Parallel and Distributed System, 2009, 20(5): 567 - 580.

[6] CHANG H Y, NARAYAN R, WU S F, *et al*. DECIDUOUS: Decentralized source identification for network-based intrusions [C]// Proceedings of the Sixth IFIP/IEEE International Symposium on Integrated Network Management. Boston, USA: [s. n.], 1999: 701 - 714.

[7] SNOEREN A C, PARTRIDGE C, SANCHEZ L A, *et al*. Hash-based IP traceback [C]// Proceedings of the ACM SIGCOMM 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication. New York: ACM Press, 2001: 3 - 14.

[8] GONG C, SARAC K. A more practical approach for single-packet IP traceback using packet logging and marking [J]. IEEE Transactions on Parallel and Distributed System, 2008, 19(10): 1310 - 1324.

[9] CHEN R L, PARK J M, MARCHANY R, *et al*. RIM: Router interface marking for IP traceback [C]// Global Telecommunications Conference. San Francisco, USA: [s. n.], 2006: 1 - 5.

[10] MUTHUPRASANNA M, MANIMARAN G, MANZOR M, *et al*. Coloring the Internet: IP traceback [C]// Proceedings of the 12th International Conference on Parallel and Distributed Systems. Minnesota, USA: [s. n.], 2006: 589 - 598.

(上接第 773 页)

树的有序表扫描结构,构造快速置乱方法,根并对扫描输出比特执行异或加密算法,由此获得的密文图像能实现对视觉内容的有效掩蔽。通过实验仿真证明了该算法的安全性和有效性。

参考文献:

[1] DO M N, VETTERLI M. Contourlets: A directional multiresolution image representation [C]// Proceedings of the 2002 IEEE International Conference on Image Processing. New York: IEEE Computer Society, 2002: 357 - 360.

[2] ESLAMI R, RADHA H. Wavelet-based contourlet coding using an SPIHT-like algorithm [C]// Proceedings of the IEEE Conference on Information Science and Systems. Piscateway, USA: [s. n.], 2004: 784 - 788.

[3] ESLAMI R, RADHA H. Wavelet-based contourlet transform and its application to image coding [C]// Proceedings of IEEE International Conference on Image Processing. Piscateway, USA: [s. n.], 2004: 3189 - 3192.

[4] VASUKI A, VANATHI P T. Progressive image compression using contourlet transform [J]. International Journal of Recent Trends in Engineering, 2009, 2(5): 193 - 197.

[5] 肖羽,王相海. 基于 Contourlet 的中低码率图像质量可分级编码算法[J]. 计算机研究与发展,2008,45(6):1020 - 1028.

[6] 肖羽,王相海. 一种基于 Contourlet 的图像低码率 SPIHT 算法[J]. 计算机科学,2007,34(11):196 - 200.

[7] KOCAREV L, JAKIMOVSKI G. Chaos and cryptography: From chaotic maps to encryption algorithms [J]. IEEE Transactions on Circuits and System, 2001, 48(2): 163 - 169.

[8] LI S J, MOU X Q, CAI Y L. Chaotic cryptography in digital world: state-of-the-art, problems and solutions [EB/OL]. [2010 - 05 - 01]. http://www.hooklee.com.

[9] 李娟,冯勇,杨旭强. 压缩图像的三维混沌加密算法[J]. 光学学报,2010,30(2):399 - 404.

[10] BURT P J, ADELSON E H. The Laplacian pyramid as a compact image code [J]. IEEE Transactions on Communications, 1983, 31(4):532 - 5401.