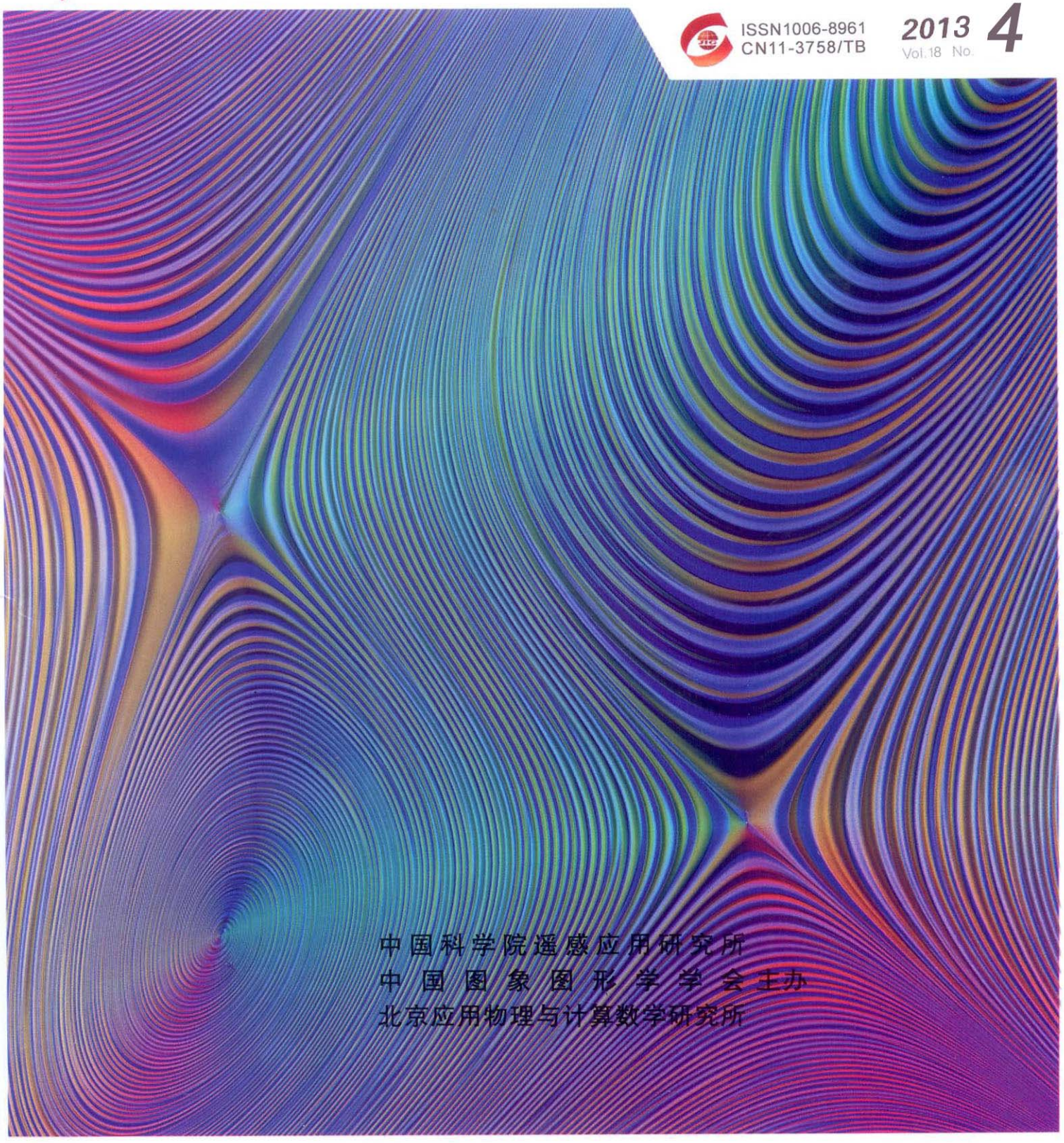
Journal of Image and Graphics

中国图象图形学报

ISSN1006-8961
CN11-3758/TB

2013 Vol.18 No. 4



中国科学院遥感应用研究所
中国图象图形学学会主办
北京应用物理与计算数学研究所

中国精品科技期刊

中国图象图形学报

Zhongguo Tuxiang Tuxing Xuebao

2013 年 4 月　第 18 卷　第 4 期(总第 204 期)

目　次

Journal of Image and Graphics

(**Monthly, Started in 1996**)

Vol. 18 No. 4 April 2013

Contents

中图法分类号: TP309.7 **文献标识码**: A **文章编号**: 1006-8961(2013)04-0376-06
论文引用格式: 李园园,张绍武. 小波变换和 SHA-1 的图像压缩加密[J]. 中国图象图形学报,2013,18(4):376-381.

小波变换和 SHA-1 相结合的图像压缩加密

李园园, 张绍武
西北工业大学自动化学院, 西安 710129

摘 要: 针对图像分层树集划分编码的安全性问题,提出一种将小波变换和 SHA-1(security hash algorithm-1)相结合的图像加密算法(DSCE)。首先将图像小波变换后的系数分为低频和高频两部分,然后将低频系数、初始密钥及图像像素和,通过 SHA-1 置乱加密 SPIHT 编码高频系数;将部分加密高频系数和初始密钥,通过 SHA-1 置乱加密 Huffman 编码低频系数,在压缩过程中实现低频和高频部分相互加密。仿真结果表明,DSCE 算法密钥空间大,对密钥和明文敏感,同时有效提高图像存储和传输效率。

关键词: SPIHT 编码;SHA-1;图像加密;混沌映射;离散小波变换

Image compression and encryption based on DWT and SHA-1

Li Yuanyuan, Zhang Shaowu
College of Automation, Northwest Polytechnical University, Xi'an 710129, China

Abstract: For the security of the set partition in hierarchical trees compression, an algorithm of joint image compression and encryption with discrete wavelet transform and secure Hash algorithm-1 (named as DSCE) is proposed in this paper. First, the wavelet transform coefficients of the plain image are divided into a high-frequency and a low-frequency part. Then, the low-frequency coefficients, the initial keys, and the sum of total pixels are the input data of the SHA-1 to output the 160-bit hash value. The 160-bit hash value is used to produce a sub-key and to perturb the initial keys. The high-frequency coefficients are permuted by a sub-key produced with the 160-bit hash value. The initial keys perturbed with 160-bit hash value are used to partially encrypt the high-frequency coefficients encoded with the SPIHT code. Third, the partial encrypted high-frequency coefficients and the initial keys are input to the SHA-1 to output another 160-bit hash value. The hash value is used to produce a sub-key to permute the low-frequency coefficients, and it is also used to perturb the initial keys to encrypt the low-frequency coefficients encoded with Huffman code. This new DSCE algorithm can implement the mutual encryption between low-frequency and high-frequency in the process of compression. The simulation results show that our algorithm not only has a large key space, but also is highly sensitive to both the key and plain-image. Moreover, it can increase the efficiency of image storage and transmission.

Key words: SPIHT coding; secure hash algorithm-1; image encryption; chaos mapping; discrete wavelet transform

收稿日期:2012-05-08;**修回日期**:2012-10-26
基金项目:国家自然科学基金项目(61170134)
第一作者简介:李园园 (1985—),女,西北工业大学控制理论与控制工程专业在读硕士研究生,主要从事图像压缩加密方面的研究。E-mail:sainan2@163.com
通讯作者:张绍武,E-mail:zhangsw@nwpu.edu.cn

0　引　言

随着多媒体内容更加丰富以及在公共网络中安全传输的需求不断增加,数字图像压缩和加密技术日益受到人们的关注。在图像压缩领域,人们突破传统信源编码理论,充分利用人的视觉特性、图像信源特性等,不断提高图像压缩性能。然而,这些算法在取得较好压缩效果的同时,却未充分考虑图像信息安全方面的问题。同时在图像加密领域,混沌系统因其具有对初值敏感、可完全重现及类随机等特性,特别适合图像通信和图像加密领域。近几年来,基于混沌序列的图像加密算法不断提出[1-4],但这些算法主要集中在直接对图像像素进行置乱和扩散,未考虑置乱和扩散对图像压缩性能的影响。

针对这一问题,图像压缩和加密相结合的方法得到了越来越多的关注。文献[5-7]将基于小波变换的压缩算法与加密算法相结合,在保障图像加密安全性的同时减少了加密数据量,但这种方法对明文图像不敏感。文献[8-9]提出了基于离散余弦变换(DCT)的图像压缩加密算法,取得了较好掩密效果。文献[9]采用 SHA-1(security hash algorithm-1)增加算法对明文的敏感性,但由于该方法采用基于块 DCT,在压缩比较高情况下会出现明显方块效应。而小波变换对图像变换是全局的,不会出现方块效应,同时经过小波变换后的图像采用 SPIHT 编码可以实现分层传输,可满足不同用户不同网络条件的需求。基于上述分析,提出一种基于小波变换和 SHA-1 的图像压缩加密算法(DSCE),并通过图像仿真实验验证 DSCE 算法有效性。

1　DSCE 图像压缩加密算法

DSCE 算法主要由 SHA-1 生成子密钥、压缩前小波系数置乱和压缩后数据流加密 3 部分构成。

1.1　SHA-1 生成子密钥

SHA-1 是目前使用最为广泛的一种散列函数[10-11],它可以对长度不超过 2^{64} 比特的消息进行计算,产生 160 位散列值。SHA-1 算法对输入信息较敏感性、运算效率较高。DSCE 算法采用 SHA-1 生成子密钥,扰动混沌映射的初始值及部分参数,增加算法对明文和密钥的敏感性。

采用的数字值混沌系统为 Logistic 映射和 Tent 映射,映射方程分别为

$$\begin{aligned} &x_{n+1}=\mu x_n(1-x_n)\\ &3.569\,94\cdots<\mu\leqslant 4,x_n\in(0,1)\end{aligned} \tag{1}$$

$$x_{n+1}=\begin{cases}\dfrac{x_n}{p} & 0<x_n<p\\ \dfrac{1-x_n}{1-p} & \text{其他}\end{cases} \tag{2}$$

$$p\in(0,1),x_n\in[0,1]$$

具体的子密钥生成过程如下:

1)选择部分已知信息和初始密钥作为 SHA-1 输入消息,将输出的 160 位散列值分为 5 组,记 d_1、d_2、d_3、d_4、d_5。

2)由式(3)生成子密钥 x_0^g,作为 Logistic 映射初始值。

$$x_0^g=\mathrm{mod}\left(\sum_{i=1}^{5}d_i/2^{32},1\right) \tag{3}$$

式中,mod(·,·)表示模运算。

3)给定初始密钥 x_0、p_0、c_0,由式(4)扰动初始密钥生成子密钥 x_0',p_0',c_0',分别作为 Tent 映射初始值、控制参数以及初始密文块。

$$\begin{cases}x_0'=\mathrm{mod}(x_0+(d_1\oplus d_2)/2^{32},1)\\ p_0'=\mathrm{mod}(p_0+(d_3\oplus d_4)/2^{32},1)\\ c_0'=c_0\oplus d_5\end{cases} \tag{4}$$

式中,⊕表示异或运算。

1.2　小波系数置乱

在不同加密阶段,DSCE 算法对小波分解后的高频系数和低频系数分别进行置乱。对于低频系数,直接采用 Logistic 映射构造置乱表进行置乱;对于高频系数,为了保证 SPIHT 编码性能,对同一方向不同分解层小波系数采用同一置乱矩阵进行置乱,确保不破坏小波多尺度分解树形结构。具体过程如下:

1)对 $N\times N(N=2^n)$ 图像进行 l 级小波变换,变换后子频带 LL_l 的大小为 $M\times M$,其中 $M=2^{n-l}$。

2)令 $\mu=4$,以 $x_{0\mathrm{H}}^g$ 为初始值(下标 H 表示高频),通过迭代 Logistic 模型产生混沌序列值,取迭代 1 000 次后 p 个迭代值 $\boldsymbol{X}^g=\{x_1^g,x_2^g,\cdots,x_p^g\}$,从 $\boldsymbol{X}^g$ 序列中取 $x_{3t}^g(t=1,2,\cdots,(p-1)/3)$ 进行递增排序,得到排序后对应的下标映射序列,构造置乱表 T_{HL}。用同样的方法从 $\boldsymbol{X}$ 序列中取 x_{3t+1}^g、x_{3t+2}^g 构造置乱表 T_{LH}、T_{HH}。

3)将第 $k(1\leqslant k\leqslant l)$ 级分解的子频带 HL_k、LH_k、

HH_k 均分成 $M \times M$ 小块，块的大小为 $m \times m$，其中 $m = 2^{l-k}$。对子频带 HL_k、LH_k、HH_k 以块为单位分别用 T_{HL}、T_{LH}、T_{HH}进行置乱。

1.3 压缩数据流加密

采用 Tent 映射对压缩后码流进行混淆扩散加密。假设明文压缩后的数据流为 R，Tent 映射初值和控制参数分别为 x'_0、p'_0，初始密文块为 c'_0。压缩数据流加密过程如下：

1）首先将 R 分成若干个长度为 32 的子块 r，q 为序列 R 的分块数。

2）以 x'_0、p'_0为初值和控制参数，迭代 Tent 模型 q 次，由式(5)处理每次迭代值 x'_k，最后得到序列 $\{m_k, k = 1, 2, \cdots, q\}$，其中 m_k 为 y_k 的 32 位二进制数表示形式。

$$y_k = \mathrm{mod}(round(x'_k \times 10^{16}), 2^{32}) \tag{5}$$

式中，$round(\cdot)$表示取整运算。

3）以 c'_0为初始密文块，通过式(6)对序列 R 进行两轮加密，得到密文序列 R'。

$$c_i = CycR[(\mathrm{mod}((r_i \oplus m_i + c_{i-1}), 2^{32}), LSB_5(m_{(1+\mathrm{mod}(c'_{i-1}, q))})] \tag{6}$$

式中，r_i、c_i 分别为第 i 个明文子块及对应的密文子块。$CycR[s, b]$表示将二进制序列 s 右移 b 位，$LSB_5(s)$表示取序列 s 中最低 5 位的值。

1.4 DSCE 算法步骤

设初始密钥 Key 为$[x_{0H}、p_{0H}、x_{0L}、p_{0L}、c_0]$（下标 H 表示高频，L 表示低频）。图 1 为 DSCE 算法框图。

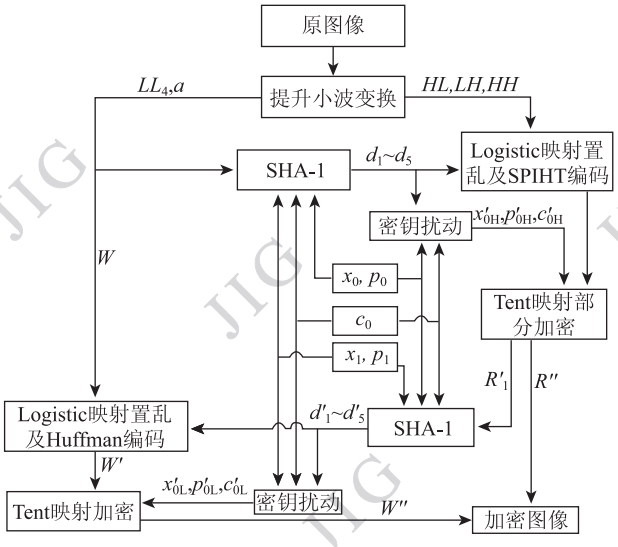


图 1 DSCE 算法框图

Fig. 1 The schematic diagram of DSCE algorithm

计算步骤如下：

1）计算图像像素值和，其模 256 结果记为 a。同时对原图像进行 4 层提升小波变换，低子频带 LL_4 系数按列扫描转化为序列 L，L 和 a 构成序列 W，其余的小波系数按水平、垂直、对角 3 个方向分为 HL、LH、HH 3 部分，每部分仍保持原有级间相似性。

2）将序列 W 和初始密钥 Key 作为 SHA-1 的输入消息，由式(3)(4)生成子密钥 x^g_{0H}、x'_{0H}、p'_{0H}、c'_{0H}，以 x^g_{0H}为初始值对高频部分进行置乱，计算 HL、LH、HH 3 部分能量 E_1、E_2、E_3。根据压缩比确定总的码字 N，按照式(7)为 3 个方向分配码字 N_1、N_2、N_3[12]。

$$N_i = \frac{E_i}{E} \times (N - N_0), i = 1, 2, 3 \tag{7}$$

式中，E 为高频部分总能量，N_0 为子频带 LL_4 安全编码所需码字，一般由经验值确定。根据分配的码字，对 3 个方向分别进行 SPIHT 编码，将编码后的数据流记为序列 HL'、LH'、HH'。

3）分别提取序列 HL'、LH'、HH'部分数据，构成临时序列 R_1，以 x'_{0H}、p'_{0H}为 Tent 映射初始值和控制参数，c'_{0H}为初始密文块，采用式(6)加密 R_1，得到密文序列 R'_1。重新分配 R'_1到序列 HL'、LH'、HH'中，连接 3 个序列构成高频系数的密文序列 R''。

4）将密文序列 R'_1及密钥 Key 作为 SHA-1 函数输入信息，由式(3)(4)生成子密钥 x^g_{0L}、x'_{0L}、p'_{0L}、c'_{0L}，令 $\mu = 4$，以 x^g_{0L}为初始值迭代 Logistic 模型构造置乱表 T_{LL}对序列 W 进行置乱。对置乱后的序列进行 Huffman 编码，得到序列 W'。

5）以 x'_{0L}、p'_{0L}为 Tent 映射初值和控制参数，c'_{0L}为初始密文块，用式(6)加密 W'，得到加密序列 W''。最后由序列 W''及 R''组成密文图像。

解密过程是加密算法的逆运算。为了保证正确解密，解密过程中除了需要密钥 Key 外，还需要序列 W''及 HL''、LH''、HH''的长度。首先，分别提取序列 HL''、LH''、HH''部分数据和密钥作为 SHA-1 输入信息，生成子密钥 x^g_{0L}、x'_{0L}、p'_{0L}、c'_{0L}，解密低频部分；然后将低频部分及密钥作为 SHA-1 输入信息，以相同的方法解密高频部分。重新排列小波系数后进行逆小波变换得到重构图像。

2 仿真实验结果与分析

基于 Matlab R2008a 平台，选取 Barb、Frog、Sail-

boat、Aerial 和 Goldhill 5 幅 512 × 512 标准灰度图像作为测试图像。初始密钥 x_{0H} = 0.405 000 869 748 94、p_{0H} = 0.630 979 255 024 04、x_{0L} = 0.421 150 774 180 42、p_{0L} = 0.594 355 626 212 63、c_0 = 3 853 080 679,图 2 为 DSCE 算法对 Barb 图像加密结果(图像压缩比为 10)。从图 2(b)可以看出,经过 DSCE 算法加密后图像根本无法辨认,不会泄露原图像的结构和纹理信息,主观视觉性安全性高。其他 4 幅图像亦有类似加密效果。

(a) 原图像　　(b) 加密后重建图像

图 2　Barb 原图像及加密后重建图像

Fig. 2　Original image and encrypted reconstructed image of Barb

2.1　压缩性能分析

DSCE 算法对压缩性能的影响主要表现在小波高频部分的置乱,改变了 SPIHT 编码节点的扫描顺序,在相同压缩比条件下,使重构图像的质量有所不同。为了验证 DSCE 算法对压缩质量的影响,在压缩比分别为 4 和 10 的条件下,分别采用 DSCE 算法和无加密编码算法(低频部分采用 Huffman 编码,高频部分采用 SPIHT 编码)对 5 幅测试图像进行仿真实验,实验结果如表 1 所示(其中 CR 表示压缩比)。由表 1 可以看出,DSCE 算法与无加密编码算法的压缩性能基本相等,这主要是因为 DSCE 算法在置乱阶段未破坏小波多尺度分解的树型结构。同时还会发现,当 CR = 10 时,对于 Frog 图像,DSCE 算法的 PSNR 略高于无加密编码算法,其原因在于 SPIHT 算法在同一频带内以"Z"字方式扫描编码,并不能保证在未置乱的情况下先扫描的系数绝对大于后扫描的系数,可能会出现置乱后编码更优的情况,但大部分情况下两种算法的 PSNR 基本相同。

为了进一步验证 DSCE 算法压缩性能,相同压缩比条件下,DSCE 算法与 Yuen 算法[9]对比结果如图 3 所示。从图 3 可以看出,压缩比较低时,Yuen 算法的 PSNR 高于 DSCE 算法,但随着压缩比提高,

表 1　DSCE 算法加密过程对压缩性能的影响

Table 1　The compression performance influenced by encryption process of DSCE algorithm

测试图像	PSNR/dB			
	CR = 4		*CR* = 10	
	DSCE 算法	无加密	DSCE 算法	无加密
Barb	38.51	38.51	31.60	31.61
Goldhill	38.02	38.02	32.38	32.38
Sailboat	36.22	36.22	30.95	30.97
Aerial	35.73	35.73	28.12	28.12
Frog	29.64	29.65	25.39	25.38

DSCE 算法压缩性能优于 Yuen 算法。其原因主要在于两种加密算法内部所采用的压缩方法不同,Yuen 算法主要采用 Huffman 编码压缩图像 DCT 变换后的系数,Huffman 编码是一种无损编码算法,数据压缩的理论极限是其信息熵,因而在低压缩比条件下,图像具有较高的 PSNR,但随着压缩比提高,系数的量化步长需不断增加,重构图像的 PSNR 将显著下降;而 DSCE 算法通过计算 DWT 变换后 *HL*、*LH*、*HH* 3 个方向上的能量,根据式(7)分为每个方向分配码字,利用 SPIHT 渐进编码的特性,在高压缩比条件下使得重构的图像具有较好的 PSNR 和主观视觉特性,因而,DSCE 算法适用于压缩比要求较高的场合。同时随着压缩比不断提高,Yuen 算法重构图像出现较明显的分块效应,而 DSCE 算法视觉效果明显优于 Yuen 算法。图 4 为压缩比为 6.94,两种算法 Barb 图像解密的局部放大图,图4(b)中的圆圈为较明显的分块部分。

2.2　编码时间分析

DSCE 算法采用混沌映射构建置乱矩阵,可并行对 3 个方向进行置乱,对于高频系数,仅对编码后的部分数据量进行加密,对编码时间影响较小。

设不包含加密过程的编码时间为 T_1,包含加密过程的时间为 T_2,编码时间影响率为

$$\delta = \frac{T_2 - T_1}{T_1} \tag{8}$$

加密过程对编码时间影响的实验结果如表 2 所示,由表 2 可以看出,随着压缩比的降低,加密过程对编码时间影响降低,这主要是因为算法运算时间主要由编码时间决定。

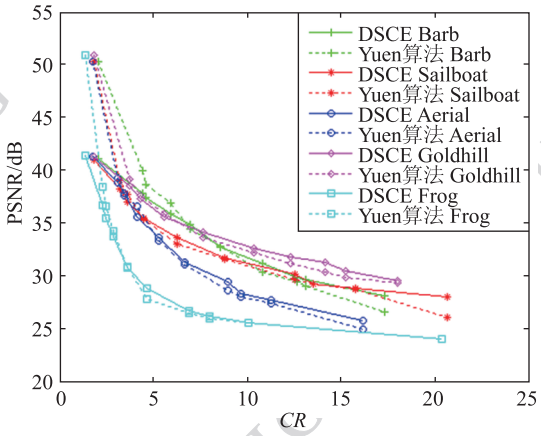
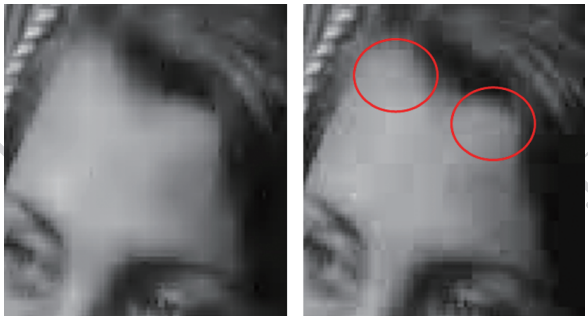


图 3 两种加密算法的压缩性能

Fig. 3 The compression performance of two encryption algorithms



(a) DSCE算法 (b) Yuen算法

图 4 Barb 图像解密的局部放大图($CR=6.94$)

Fig. 4 The local enlarged view of decrypted Barb image ($CR=6.94$)

表 2 加密对编码时间影响

Table 2 The encoding time influenced by Encryption

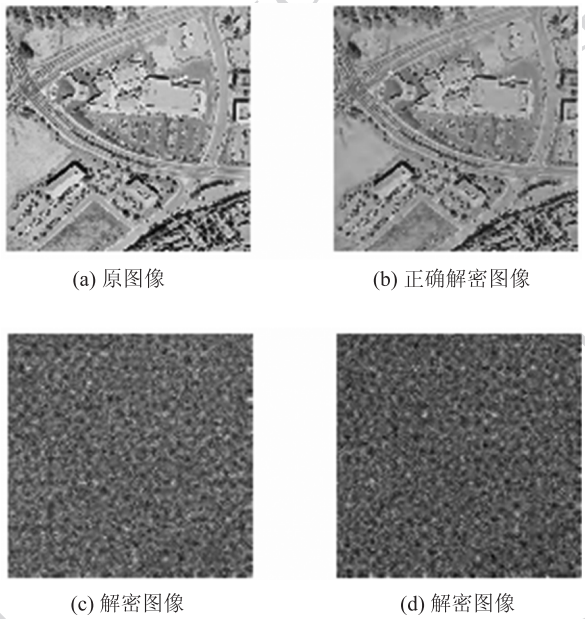
测试图像	编码时间影响率 δ/%	
	$CR=4$	$CR=10$
Barb	7.2	7.3
Goldhill	6.7	8.0
Sailboat	6.7	7.4
Aerial	7.0	7.2
Frog	7.8	8.6

2.3 密钥空间分析

DSCE 算法共需要 5 个初始密钥:x_{0H}、x_{0L}、p_{0H}、p_{0L}、c_0,其中前 4 个密钥为双精度类型,每个双精度密钥产生的双精度空间约为 10^{15}。同时 DSCE 算法采用 SHA-1 算法输出散列值生成子密钥用于小波系数置乱,原图像不同子密钥将发生很大变化,因而 DSCE 算法具有较大的密钥空间,能有效抵抗穷举攻击。

2.4 密钥敏感性分析

为了验证系统对密钥的敏感性,采用具有微小差异的密钥对原图像进行加密,比较输出码流的变化率。分别将密钥 x_{0H}、x_{0L}、p_{0H}、p_{0L}小数点后第 15 位由 0 变为 1,其他密钥保持不变,对图像进行加密,输出比特流变化率保持在 47.60%～47.73% 之间,较文献[9]的略低,其主要原因是本文仅加密高频系数部分码流。但由于本文高频系数采用 SPIHT 编码,在图像重构时前半部分码流的改变将直接影响后续码流,从而保证了加密安全性。图 5 给出了压缩比为 10,密钥 x_{0H}、p_{0H}分别进行微小改变(仅差 10^{-15})时,Aerial 加解密实验结果。由图 5 可以看出,解密结果是一幅杂乱无章的图像,对图像的视觉内容具有很好的掩密效果。



(a) 原图像 (b) 正确解密图像

(c) 解密图像 x_{0H}=0.405 000 869 748 941 (d) 解密图像 p_{0H}=0.630 979 255 024 041

图 5 Aerial 加解密实验结果

Fig. 5 Results of Aerial encryption and decryption

2.5 明文敏感性分析

保持密钥不变,随机改变原图像某一像素值,通过加密后比特流变化率来评价算法对明文的敏感性。对 Aerial 图像(压缩比为 10)进行了 50 次仿真实验,实验结果表明密文比特流变化率保持在 47.44%～47.50%。说明 DSCE 算法对明文图像很敏感,可有效抵抗差分攻击。

3　结　论

将小波变换和 SHA-1 散列函数相结合的图像压缩加密算法,首先对图像进行 4 层小波分解,将分解后的系数分为低频和高频两部分;将原图像像素和、低频系数及初始密钥通过 SHA-1 产生 160 位散列值,由散列值生成子密钥置乱高频系数,对置乱后高频系数进行 SPIHT 编码,同时由散列值扰动初始密钥对编码后数据流进行部分加密;将加密后部分高频系数和初始密钥作为 SHA-1 的输入消息,采用类似的方法置乱加密低频系数。在充分利用了 SHA-1 散列算法对输入信息敏感的同时,使得低频部分与高频部分相互加密,保证了图像信息的安全性。仿真结果表明,DSCE 算法基本上不影响图像压缩性能;能有效抵抗穷举攻击、已知明文攻击和差分攻击;与文献[9]相比,DSCE 算法适用于压缩比要求较高的场合。

参考文献(References)

[1] Pareek N K, Patidar V, Sud K K. Image encryption using chaotic logistic map[J]. Image and Vision Computing, 2006, 24(6): 926-934.

[2] Behnia S, Akshshani A, Mahmodi H, et al. A novel algorithm for image encryption based on mixture of chaotic maps[J]. Chaos, Solitons & Fractals, 2008, 35(2): 408-419.

[3] Wang Y, Wong K W, Liao X F, et al. A new chaos-based fast image encryption algorithm[J]. Applied Soft Computing, 2011, 11(1): 514-522.

[4] Wong K W, Kwok B S H, Law W S. A fast image encryption scheme based on chaotic standard map [J]. Physics Letter A, 2008, 372(15): 2645-2652.

[5] Li J, Feng Y, Yang X Q. 3D chaotic encryption scheme for compressed image[J]. Acta Optica Sinica, 2010, 30(2): 399-404. [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.]

[6] Ping L, Sun J, Zhou J. An algorithm for image encryption based on JPEG2000[J]. Application & project of video technologies, 2006, 7: 87-90. [平亮,孙军,周军. 一种基于 JPEG2000 标准的数字图像加密算法[J]. 电视技术,2006,7:87-90.]

[7] Gu G S, Liu F C. Contourlet domain image encryption based on chaos mapping[J]. Joumal of Computer Application, 2011, 30(3): 771-777. [顾国生,刘富春. 基于混沌映射的图像 Contourlet 编码加密算法[J]. 计算机应用, 2011, 30(3): 771-777.]

[8] Peng C, Liu L. Encryption algorithm for compressed images based on chaotic sequences [J]. Computer Engineering, 2008, 34(20): 177-180. [彭成,柳林. 基于混沌序列的压缩图像加密算法[J]. 计算机工程, 2008, 34(20): 177-180.]

[9] Yuen C H, Wong K W. A chao-based joint image compression and encryption scheme using DCT and SHA-1[J]. Applied Soft Computing, 2011, 11(8): 5092-5098.

[10] Denis T S, Johnson S. Cryptography for Developers[M]. Rockland, Florida, USA: Syngress Publishing, 2006: 203-207.

[11] Wang Y, Liao X, Xiao D, et al. One-way hash function construction based on 2D coupled map lattices[J]. Information Sciences, 2008, 178(5): 1391-1406.

[12] Liu Y J, Ma Y D, Wang J, et al. Multiwavelet image compression coding based on improved SPIHT[J]. Chinese Journal of Scientific Instrment, 2006, 27(sup.): 2168-2170. [刘映杰,马义德,王俊,等. 基于改进的 SPIHT 多小波图像压缩编码[J]. 仪器仪表学报,2006,27(增刊): 2168-2170.]