【本文献信息】郭雨,柏森,阳溢,等. 基于复用技术和数论的图像加密压缩同步算法[J]. 电视技术,2013,37(5).

基于复用技术和数论的图像加密压缩同步算法

郭　雨,柏　森,阳　溢,唐鉴波
(1. 重庆通信学院,重庆 400035;2. 应急通信重庆市重点实验室,重庆 400035)

【摘　要】在前人应用数论对图像进行同时压缩和加密研究的基础之上,结合图像复用技术,提出了一种改进算法。算法首先将4幅相同尺寸但内容不同的图像利用图像复用技术复合成1幅图像,再对复合的图像应用数论方法进行加密和压缩。仿真实验结果表明,算法具有较好的加密效果和压缩比。

【关键词】图像加密;图像压缩;中国剩余定理;图像复用技术
【中图分类号】TN919.81　　【文献标志码】A

Simultaneous Image Compression and Encryption Using Number Theory and Image Multiplexing

GUO Yu,BAI Sen,YANG Yi,TANG Jianbo
(1. Chongqing Communication Institute,Chongqing 400035,China;2. Chongqing Key Laboratory of Emergency Communication,Chongqing 400035,China)

【Abstract】On the basis of the study of simultaneous image compression and encryption using number theory,combined with image multiplexing technique,an improved algorithm is proposed. Firstly,four different images with the same size are multiplexed into one image. Then,uses number theory knowledge,the multiplexing image is encrypted and compressed. The simulation experiment results show that the proposed algorithm has a good encryption effect and compression ratio.

【Key words】image encryption;image compression;Chinese remainder theorem;image multiplexing

传统的图像压缩和加密过程往往是分开的,这样不但增加了算法的复杂度,并且由于加密破坏了图像的相关性,还会降低图像的压缩性能。因此,发展一种能够同时对图像进行压缩和加密处理的算法就成了新的需要。对图像同时进行加密和压缩,既能够解决图像传输中带宽利用率的问题,又可以解决传输安全的问题。基于数论的图像同时压缩和加密算法[1](Number Theory based Image Compression Encryption,NTICE)正是这样的一种技术。

文献[2]中提到的方法是先压缩,后加密。由于先对图像进行压缩,没有破坏图像相关性,因此可以得到较高的压缩比,但由于其加密和压缩是两个独立的部分,增加了算法复杂度,降低了运算效率。文献[3]提出了一种基于骑士巡游的图像加密和压缩同时进行的方法。此方法可以得到较好的压缩比和加密效果,但是严格来说,此方法是先加密,后压缩。文献[1]中首先使用了NTICE算法对RGB彩色模型的彩色图像进行加密和压缩。文献[4]为了进一步提高NTICE算法的安全性和压缩效率,通过将两幅不同的图像的高4比特位和低4比特位互换的方法,使两幅图像复合成为一幅图像后,再对复合图像使用NTICE算法进行加密和压缩处理。文献[4]为多幅图像同时加密和压缩提供了一个思路。

为保证图像传输的安全性和传输效率,本文在前人应用数论知识对图像进行同步压缩和加密研究的基础之上,结合图像复用技术[6-7],提出了一种改进算法。本文首先利用图像复用技术将4幅图像复合1幅图像,再对复合图像使用NTICE算法进行压缩和加密。经由上述算法对图像进行压缩和加密,图像的压缩率和安全性都得到了一定程度的提升。

1　中国剩余定理及NTICE算法加密和压缩的原理

中国剩余定理(Chinese Remainder Theorem,CRT)解决了同余方程组的求解问题。具体表述如下。

设有以下同余方程组:

$$\begin{cases} x \equiv a_1 (\bmod n_1) \\ x \equiv a_2 (\bmod n_2) \\ \quad \vdots \\ x \equiv a_k (\bmod n_k) \end{cases} \tag{1}$$

设$n_1,n_2,\cdots,n_k(k \geqslant 1)$为$k$个两两互素的正整数,令

$$P = n_1 n_2 \cdots n_k = n_1 P_1 = n_2 P_2 = \cdots = n_k P_k \tag{2}$$

式中:$P_i = \dfrac{P}{n_i}(i = 1,2,\cdots,k)$。

则同余方程组的一般解为

基金项目:国家自然科学基金项目(61272043)

$$x \equiv a_1c_1P_1 + a_2c_2P_2 + \cdots + a_kc_kP_k \pmod{P} \quad (3)$$

式中：c_i 是满足同余方程(4)的一个特解。

$$P_ix \equiv 1 \pmod{n_i} \quad (4)$$

式中：$i = 1,2,\cdots,k$。其求解方法可以采用“大衍求一数”或“辗转相除法”，具体方法见文献[5]。

NTICE 算法是 CRT 的一种应用。把像素值作为同余方程组的余数 a_k，而将两两互素的密钥分别作为同余方程组的模数 n_k，从而求解出同余方程组的通解 x。可以得知，多个像素值经过同余方程组的求解，最终变成了一个正整数，也就是通解，达到了图像压缩的目的。若将图像还原，只需将通解 x 代入式(1)就可得到原始像素值。若此时模数 n_k 不正确，即解密密钥错误，就无法还原出原始像素值，达到了加密的目的。

2 基于图像复用技术和数论的图像加密压缩同步算法

2.1 算法思想

由于图像的像素之间存在着强相关性，在应用 NTICE 算法对图像加密时，如果正确的解密密钥和错误的解密密钥相差不是很大时，使用错误密钥解密仍可得到部分原始图像。为了进一步提高安全性和压缩比，本文首先对 4 幅 $m \times n$ 大小的图像进行 DCT 变换，得到 4 个 $m \times n$ 大小的 DCT 系数矩阵，再按照一定的规则将 4 个 DCT 系数矩阵结合成 1 个 $m \times n$ 大小的 DCT 系数矩阵，再对生成的 DCT 系数矩阵进行 DCT 逆变换，得到复合图像，最后对复合图像使用 NTICE 算法进行同步加密和压缩，得到加密和压缩后的数据流。解密过程是上述算法的逆过程。算法过程如图 1 所示。

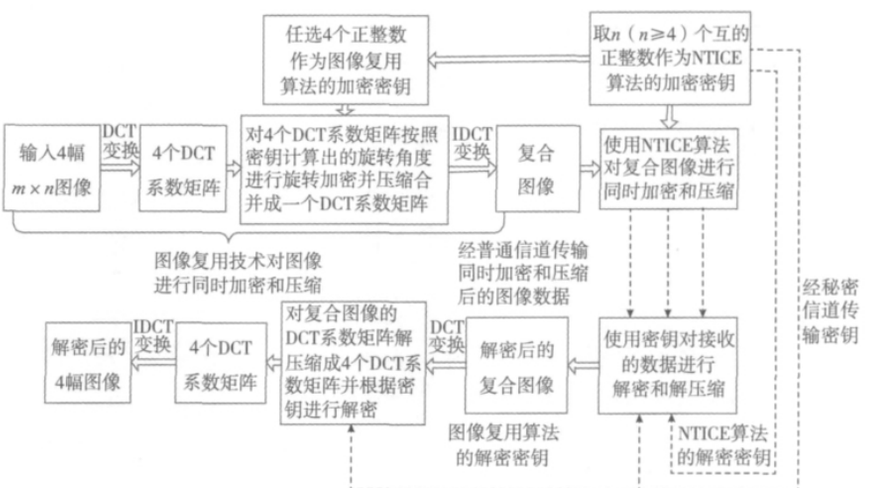


图 1 本文算法示意图

2.2 图像复用技术算法原理与步骤

文献[6]和文献[7]中的图像复用技术可以提高图像压缩效率，但是复用后的图像仍可以显示其中的部分原始图像信息。本文在其基础上进行了改进，复用后的图像不显示原始图像信息，安全性得到了一定的提升。其示意图如图 2 所示，步骤如下。

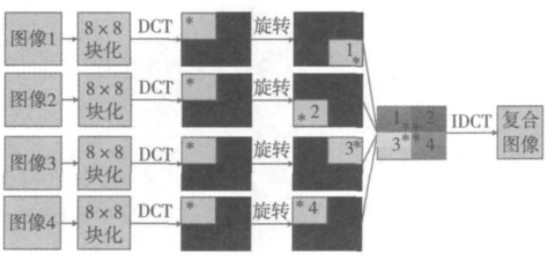


图 2 图像复用技术示意图

1) 分别对 4 幅 $m \times n$ 大小的图像 I_1, I_2, I_3, I_4 以 8×8 为大小进行分块，将每幅图像都分别分成 $i \times j$ 块，得到 4 个块化矩阵，其中 $i = \lfloor m/8 \rfloor$，$j = \lfloor n/8 \rfloor$。再分别对每一个块化矩阵的每一个 8×8 小块进行 DCT 变换，得到 4 个 DCT 系数块化矩阵 $\boldsymbol{S}_1, \boldsymbol{S}_2, \boldsymbol{S}_3, \boldsymbol{S}_4$。

2) 为了提高加密图像的安全性，本文采用如下方法进行旋转加密。令 $k_1 = n_1 \bmod 4$，$k_2 = n_2 \bmod 4$，$k_3 = n_3 \bmod 4$，$k_4 = n_4 \bmod 4$，其中 n_1, n_2, n_3, n_4 分别为 NTICE 算法中作为密钥的 k 个正整数中的任意 4 个正整数。当 $k_1 = 0,1,2,3$ 时，将 $\boldsymbol{S}_1$ 的每个 8×8 小块相应地逆时针旋转 180°，90°，270°，0°。也可采用其他组合方式，只要满足 4 个旋转角度与 k_1 可能出现的 4 个数值一一对应即可。同理，k_2, k_3, k_4 分别决定 $\boldsymbol{S}_2$，$\boldsymbol{S}_3$，$\boldsymbol{S}_4$ 的每个 8×8 小块的旋转角度。图 2 展示了 DCT 系数矩阵的一个 8×8 小块由上到下分别按照逆时针旋转 180°，90°，270°，0° 的方法示意图。

3) 将旋转后的 S_1 每个 8×8 小块的低频 1/4 部分置于复合图像的块化系数矩阵 S 对应块的左上 1/4 部分;将旋转后 S_2 每个 8×8 小块的低频 1/4 部分置于复合图像的块化系数矩阵 S 对应块的右上 1/4 部分;将旋转后 S_3 每个 8×8 小块的低频 1/4 部分置于复合图像的块化系数矩阵 S 对应块的左下 1/4 部分;将旋转后 S_4 每个 8×8 小块的低频 1/4 部分置于复合图像的块化系数矩阵 S 对应块的右下 1/4 部分。

4) 将 S 每个 8×8 块进行 DCT 逆变换,得到复合图像。由于复合图像的 DCT 系数是由原始 4 幅图像的 DCT 系数经旋转合并成的,因此复合图像不再显示出原始的图像信息,且 4 幅图像经运算后变成 1 幅图像,所以图像复用算法是一种同步进行加密和压缩的算法。

5) 在接收端,按照上述过程的逆过程,还原出原始的 4 幅图像。

2.3 NTICE 算法原理与步骤

NTICE 算法的示意图如图 3 所示。

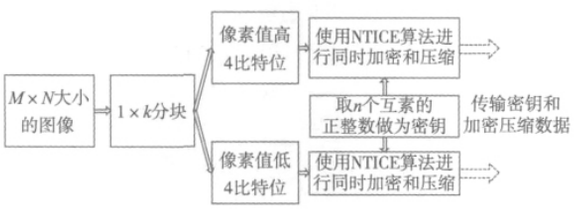


图 3 基于 NTICE 算法的图像加密压缩同步方法示意图

1) 读取原始图像 I,图像大小为 $m\times n$,对图像进行 $1\times k$ 分块,其中图像的列数可以被 k 整除,即 $n\equiv0(\bmod k)$。

2) 对划分好的像素块中的每个像素 r_i 按照式(5)分别得到像素值的高 4 比特位的十进制数值和低 4 比特的十进制数值。

$$\begin{cases} a_i = \lfloor r_i/16 \rfloor, i = 1,2,\cdots,k \\ a'_i = r_i \bmod 16, i = 1,2,\cdots,k \end{cases} \tag{5}$$

式中:a_i 表示像素值的高 4 比特位的十进制数值;a'_i 表示像素值的低 4 比特位的十进制数值。

3) 取 k 个两两互素的正整数 n_i($n_i \geqslant 16$)作为密钥。令 $P = \prod_{i=1}^{k} n_i$,$P_i = P/n_i$,构造两个同余方程组,即

$$\begin{cases} x \equiv a_1(\bmod n_1) \\ x \equiv a_2(\bmod n_2) \\ \quad\vdots \\ x \equiv a_k(\bmod n_k) \end{cases}, \begin{cases} x' \equiv a'_1(\bmod n_1) \\ x' \equiv a'_2(\bmod n_2) \\ \quad\vdots \\ x' \equiv a'_k(\bmod n_k) \end{cases} \tag{6}$$

4) 根据中国剩余定理解同余方程组,分别计算每一个一次同余式 $P_i x \equiv 1(\bmod n_i)$ 的一个特解 c_i。由于中国剩余定理的一次同余式计算仅与 P_i 和 n_i 有关,与像素值无关,因此像素值的高 4 比特位 a_1 和低 4 比特位 a'_1 的一次同余式的特解 c_i 是相同的,即无论像素值怎么变化,特解都不会变化。根据这一性质,可以在计算得出特解 c_i 之后,将其存储起来,而不用每次都进行计算,以提高计算效率。

5) 根据式(7),分别得出像素值高 4 比特和低 4 比特的加密后的数据,也就是式(6)的通解 TR 和 TR'。计算出所有 TR 后,统计相同的 TR 的个数。将不同的 TR 按照出现频率的大小,依次由高到低排列后,采用 Huffman 方法进行编码。TR' 采用同 TR 的方法进行编码。由上述叙述可以看出 TR 和 TR' 既是加密后的数据,又是压缩后的数据,达到了同时加密和压缩的目的。

$$\begin{cases} TR \equiv a_1c_1P_1 + a_2c_2P_2 + \cdots + a_kc_kP_k(\bmod P) \\ TR' \equiv a'_1c_1P_1 + a'_2c_2P_2 + \cdots + a'_kc_kP_k(\bmod P) \end{cases} \tag{7}$$

如果仅保留图像像素值的高 4 比特位的数据,而将其低 4 比特位的数据置为 0,也可以得到较好的图像显示效果。因此对解压缩后图像质量要求较高时,可以采用无损压缩模式,既同时传输高 4 比特位的加密数据 TR 和低 4 比特位的加密数据 TR';对解压缩后的图像质量要求不高时,可以采用有损压缩模式,仅传输高 4 比特位的加密数据 TR。

6) 在接收端还原图像,只需要将接收到的数据解码得到通解 TR 和 TR',并将通解 TR 和 TR' 代入式(8)

$$\begin{cases} ar_i \equiv TR(\bmod m_i), i = 1,2,\cdots,k \\ ar'_i \equiv TR'(\bmod m_i), i = 1,2,\cdots,k \end{cases} \tag{8}$$

式中:m_i 是解密密钥;ar_i 和 ar' 是解密后图像像素值的高 4 比特位和低 4 比特位。

7) 将像素的高 4 比特位和低 4 比特位合并,重建图像 S_i,计算公式为

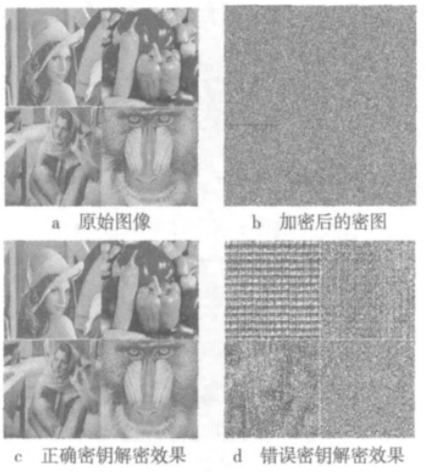
$$S_i = ar_i \times 16 + ar_i^{\text{prime}} \tag{9}$$

3 算法仿真与结果

3.1 加密效果性能分析

本文主要是针对灰度图像进行仿真实验,对彩色图像进行同时加密和压缩时,可以将彩色图像按照 RGB 颜色模型分解成三基色的 3 个矩阵,然后按照灰度图像加密和压缩方法,分别对 3 个矩阵进行加密和压缩。本文使用 MTALAB 软件对 4 幅 520×520 大小的测试图像进行仿真实验。设置密钥长度为 10,即选取 10 个两两互素的正整数(18,25,43,31,29,37,17,23,41,19)作为密钥。其正确密钥解密效果图和错误密钥(22,21,19,44,31,32,39,17,

41,23) 的解密效果图如图 4 所示。



a 原始图像　b 加密后的密图
c 正确密钥解密效果　d 错误密钥解密效果

图 4　正确密钥和错误密钥解密效果图

3.2　压缩比(CR)

压缩比是评价图像压缩算法的一个重要指标,它指的是原始图像每个像素的平均比特数 c_1 同编码后每个像素的平均比特数 c_2 的比值,压缩比越大表示压缩效果越好[8],定义为

$$CR = \frac{c_1}{c_2} \tag{10}$$

压缩比测试中,采用无损压缩模式,密钥长度分别选为 10 和 8,即分别选取 10 个两两互素的正整数和 8 个两两互素的正整数作为密钥。其中峰值信噪比(PSNR)是进行解压缩后的重建图像与原始图像进行比较得到的。

由表 1 可知,密钥长度为 10(29,37,17,23,41,19,18,25,43,31) 的压缩比要比密钥长度为 8(29,37,17,23,41,19,18,25) 效果好。这是因为随着密钥长度增加,一个通解 TR 可以表示更多的像素。由于目前缺乏关于多幅图像同时进行加密和压缩的资料,所以无法与其他文献进行压缩比的比较。

表 1　无损加密和压缩的压缩比

密钥长度	原始 4 幅图像占用空间大小/kbyte	加密压缩后图像占用空间大小/kbyte	CR	$PSNR$/dB
8	1 060	463.64	2.29	31.86
10	1 060	422.50	2.51	31.75

如果在对重建图像质量要求不是非常高,可以仅传输原始复合图像像素值的高 4 位比特的加密数据 TR,进行有损加密和压缩来得到较高的压缩比。由表 2 和图 5 可以看出,有损加密和压缩的重建图像的质量和 $PSNR$ 有所下降,但仍可较为清晰地显示出图像内容,显示效果仍在可接受范围之内。

表 2　有损加密和压缩的压缩比

密钥长度	原始 4 幅图像占用空间大小/kbyte	加密压缩后图像占用空间大小/kbyte	CR	$PSNR$/dB
8	1 060	199.58	5.31	27.14
10	1 060	211.25	5.02	27.12

a 原始图像　b 有损的重建图像

图 5　有损加密和压缩的重建图像

3.3　安全性分析

3.3.1　密钥空间容量分析

一个好的加密算法应该是对密钥非常敏感的,且密钥空间要足够大以抵抗穷举攻击[9]。本算法安全性取决于密钥 n_i(由两两互素的正整数组成的)。本算法中,取每个正整数的长度为 6 bit,那么当取 10 个两两互素的正整数作为密钥时,密钥总长度为 60 bit。由于作为密钥的正整数顺序之间可以互相变化,总的变化数目是作为密钥的正整数个数的阶乘 l。本算法为了进一步增加安全性,在图像复合时,将图像的旋转方向也作为密钥。令 $k_1 = n_1 \bmod 4$,$k_2 = n_2 \bmod 4$,$k_3 = n_3 \bmod 4$,$k_4 = n_4 \bmod 4$,其中 n_1,n_2,n_3,n_4 分别为加密密钥的任意 4 个正整数,共有 A_{10}^4 种($A_{10}^4 = 10 \times 9 \times 8 \times 7$)不同的选择。当 $k_1 = 0$,1,2,3 时,分别对应逆时针旋转 0°,90°,180°,270° 这 4 个不同的旋转方向,那么不同的组合方式有 4! 种情况。其他位置的图像 DCT 系数矩阵旋转方向如上述方法所述,那么旋转图像的密钥数目为 $A_{10}^4 \times 4!^4$。综上所述,在假设攻击者不知道加密算法的情况下,本算法总的密钥空间最大为 $2^{60 \times l} \times A_{10}^4 \times 4!^4$。在本算法中,当解密密钥与原始加密密钥的欧氏距离极为接近时,仍可获知部分原始图像信息,即存在着少量的弱密钥。可以采用如图 6 所示的模型进行加密予以解决,首先将分块后的像素值的高 4 比特转化成二进制比特流(模型中像素块长度为 10,所以共有 40 bit),上文中提到密钥共有 60 bit,选取密钥序列的前 40 bit 与像素值的前 40 bit 进行异或加密,得到加密后的像素值序列,再用本文算法对加密后的像素值序列进行同时加密和压缩。像素值的低 4 比特同上。

3.3.2　密钥雪崩效应分析

从密钥更换的有效性考虑,图像加密算法对密钥的

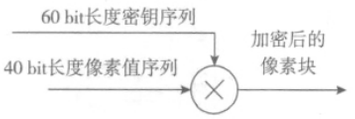


图6 加密模型

变换应是敏感的，即密钥具有所谓的雪崩现象[10]。由于本文密钥是两两互素的正整数，具有特殊性，所以测试密钥雪崩效应时，在保证测试密钥是两两互素的正整数的前提下，选取与初始密钥欧氏距离最小的两两互素的正整数作为测试密钥。设初始密钥 key1 为 18，25，43，31，29，37，17，23，41，19，改变后的密钥 key2 为 16，25，43，31，29，37，17，23，41，19。测试结果如图7所示。

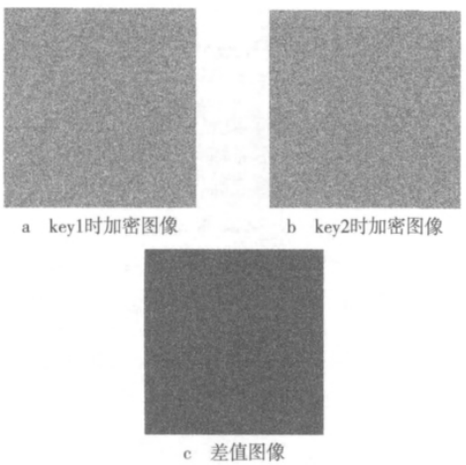


图7 密文对密钥的敏感性测试

从图7中可以看出，当密钥发生细微改变时，会导致密文产生较大的变化，此加密算法对密钥有较好的敏感性。

3.3.3 明文雪崩效应

加密算法应该对明文的变化是敏感的，即明文对密文存在着雪崩现象[10]。通常攻击者可以通过对图像作微小的改变来观察加密效果，这样可能发现加密图像与原始图像的某种关系，但是如果对原始图像做细微改变，导致加密图像有很大变化，这样差分攻击将失去作用[9]。首先对4幅原始图像进行加密，然后改变4幅原图像某一个像素点的值（如：$I(i,j) = I(i,j) + 1$），再用同样密钥进行加密，比较两个密文对应位置的像素值（如图8）。由图8可以看出，明文发生细微改变，密文多数都改变，具有较强的抗差分攻击能力。

4 结束语

本文在前人用数论对图像进行压缩和加密研究的基础之上，结合图像复用技术，提出了一个改进的算法。经实验证明，本文算法具有较大的密钥量和较好的压缩比。在图像压缩和加密技术快速发展的今天，具有较好的应用前景。

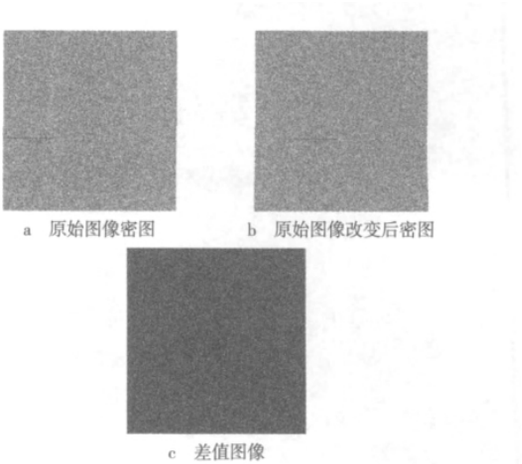


图8 密文对明文的敏感性测试

参考文献：

[1] JAGANNATHAN V，MAHADEVAN A，HARIHARAN R，et al. Simultaneous color image compression and encryption using number theory [C] // Proc. ICIS 2005. [S. l.]: IEEE Press，2005: 1-6.

[2] 侯启槟，王阳生，黄向生，等. 结合 EZW 和 AES 的图像加密机制 [J]. 中国科学院研究生院学报，2004，21(1)：119-124.

[3] 刘博文，柏森，刘程浩，等. 基于骑士巡游的灰度图像加密压缩算法 [J]. 电视技术，2012，36(9)：10-13.

[4] JAGANNATHAN V，MAHADEVAN A，HARIHARAN R，et al. Number theory based image compression encryption and application to image multiplexing [J]. Signal Processing，Communications and Networking，2007(11)：59-64.

[5] 胡冠章. 应用近世代数 [M]. 北京：清华大学出版社，1999.

[6] ALFALOU A，ELBOUZ M，JRIDI M，et al. A new simultaneous compression & encryption method for images suitable to recognize form by optical correlation [C] //Proc. SPIE 2009. Berlin，Germany：IEEE Press，2009：1117.

[7] LOUSSERT A，ALFAOU A，SAWDA E L R，et al. Enhances system for image's compression and encryption by addition of biometric characteristics [J]. International Journal of Software Engineering and Its Applications，2008，2(2)：111-118.

[8] 姚敏. 数字图像处理 [M]. 北京：机械工业出版社，2006.

[9] 吴成茂，候文滨. 基于 SMS4 分组密码的彩色图像加密方法 [J]. 西安邮电学院学报，2011，16(5)：1-6.

[10] 陈果，廖晓峰. 一种基于混沌映射的图像加密算法 [J]. 计算机应用，2005，25(S1)：121-123.

作者简介：

郭 雨（1989— ）硕士生，主研图像和视频加密、信息隐藏；

柏 森（1963— ）硕士生导师，主研信息隐藏、信息加密、数字水印；

阳 溢（1987— ）硕士生，主研图像、视频信息隐藏；

唐鉴波（1989— ）硕士生，主研图像去雾。

责任编辑：时 雯 收稿日期：2012-08-13