一种新的数字图像置乱方法

刘 兵,王 珂,周 勇
LIU Bing,WANG Ke,ZHOU Yong

中国矿业大学 计算机学院,江苏 徐州 221116
College of Computer Science and Technology,China University of Mining and Technology,Xuzhou,Jiangsu 221116,China
E-mail:liubing@cumt.edu.cn

LIU Bing,WANG Ke,ZHOU Yong.Novel digital image scrambling method.Computer Engineering and Applications,2010,46(6):181-184.

Abstract: Common image scrambling methods based on position space can't change the statistical property of an image,and these methods have to face with severe security problems because of using fixed form matrices.The paper presents a novel scrambling method based on color space and fast number theoretic transformation.It has the following advantages:The form of transformation matrix is unfixed,it is easy to calculate the invertible matrix,restoring image is lossless,and by choosing appropriate parameters this method can reach preferable scrambling effect after only one time iterating,so it has the less calculated capacity.The results show that the scrambled image is like white noise,new method improves the secrecy property of an image and reduces the attacker's notice.It is easy to realize and has application value in the field of image hiding.

Key words: information hiding;image scrambling;number theoretic transformation

摘 要:常见的基于位置空间的数字图像置乱方法存在不能改变图像统计特性的缺陷,同时置乱过程缺乏随机性,保密性不高。针对以上问题,提出了一种新的数字图像色彩空间置乱方法。该方法基于快速数论变换,置乱速度快,变换矩阵形式不固定,逆变换矩阵求解简单,恢复图像完全无损,且通过选取合适的参数,经过一次迭代就可以达到满意的置乱效果。实验结果表明,置乱后的图像接近白噪声,提高了保密信息的迷惑性,同时还原图像易于实现,有较好的实用性。

关键词:信息隐藏;图像置乱;数论变换
DOI:10.3778/j.issn.1002-8331.2010.06.053 **文章编号:**1002-8331(2010)06-0181-04 **文献标识码:**A **中图分类号:**TN911.73

1 引言

数字图像置乱技术是大幅图像信息隐藏问题的基础性工作,它既可以看做数字图像加密的一种途径,也可以用做数字图像隐藏、数字水印图像植入、数值计算恢复方法和数字图像分存的预处理和后处理过程[1-2],是一个值得深入研究的课题。

经典密码学对于一维数据流提供了很好的加解密算法,其中如 DES、AES 等著名密码系统已被应用于图像置乱[3-4],但是这些系统往往忽视二维数字图像的自相似性、大数据量等特殊性质,近几年对数字图像的置乱研究主要集中在图像的空间域(位置空间、色彩空间)和频域上进行,位置空间上的置乱研究较多,如文献[5-7]提出的 Arnold 变换、Fibonacci 变换及 Fibonacci-Q 变换;文献[8]提出的骑士巡游变换;文献[9]提出的基于仿射变换的置乱;此外还有基于幻方、空间填充曲线(FASS 曲线)和广义 Gray 码的置乱等。这些方法通过位置置乱分散了错误比特的分布,在提高数字水印的鲁棒性方面得到了很好的应用,但这些方法的缺点在于置乱形式固定,用于加密时算法和密钥不能有效地分开,这和现代密码体制的要求是不相容的,仍然属于古典密码体制的范畴[10]。文献[11]提出一种随机矩阵置乱变换的方法解决这个问题,但是算法对于不同位置的同一种颜色无法进行置乱,无论经过多少次迭代,这些不同位置点的颜色仍是一样的。因此寻找一种安全而又简便的置乱方法,一直是数字图像置乱研究的内容。针对以上问题,提出了一种基于二维数论变换的数字图像置乱方法,并通过实验验证了此方法的有效性。该方法置乱速度快,迭代次数少,置乱效果好,同时变换矩阵形式不固定,提高了保密信息的安全性。

2 二维数论变换及其快速算法

定义 1 设 $Z_p=\{0,1,\cdots,P-1\}$,在 Z_p 中定义加法和乘法是通常整数模 P 的加法和乘法,在这两种运算下,Z_p 成环,称模 P 剩余类环。

定义 2 设 a 是 Z_p 中的任一非零元素,如果有正整数 N 使

基金项目:中国矿业大学校青年科技基金(Youth Scientific Research Foundation of China University of Mining and Technology under Grant No. 2007A040)。

作者简介:刘兵(1981-),男,博士研究生,讲师,主要研究方向为图像压缩、信息隐藏、人工智能;王珂(1979-),男,博士研究生,讲师,主要研究方向为计算机网络、图像处理;周勇(1975-),男,博士,副教授,主要研究方向为智能信息处理。

收稿日期:2008-08-27 **修回日期:**2008-10-06

得 $a^N \equiv 1(\bmod P)$,则称 a 是环 Z_p 中的 N 次单位根。当 N 是使得上式成立的最小正整数时,则称 a 是 N 次本原单位根。

定义 3 设 P 为正整数,以 P 为模的整数环 Z_p:$Z_p=\{0,1,2,\cdots,p-1\}$。设 $x(n,m)\in Z_p$($n=0,1,\cdots,N-1$;$m=0,1,\cdots,M-1$),$\alpha,\beta\in Z_p$,则二维 NTT(Number Theoretic Transformation)定义为[12]:

$$X(r,s)\equiv\sum_{n=0}^{N-1}\sum_{m=0}^{M-1}x(n,m)\alpha^{rn}\beta^{sm}(\bmod p)(r=0,1,\cdots,N-1;S=0,1,\cdots,M-1) \tag{1}$$

逆变换为:

$$x(n,m)\equiv N^{-1}M^{-1}\sum_{r=0}^{N-1}\sum_{s=0}^{M-1}X(r,s)\alpha^{-rn}\beta^{-sm}(\bmod p)(n=0,1,\cdots,N-1;m=0,1,\cdots,M-1) \tag{2}$$

其中变换具有循环卷积特性,二维数论变换的矩阵表示形式如下:

$$\boldsymbol{X}\equiv\boldsymbol{T}_N\boldsymbol{x}\boldsymbol{T}_M(\bmod p)$$

$$\boldsymbol{x}\equiv\boldsymbol{T}_N^{-1}\boldsymbol{X}\boldsymbol{T}_M^{-1}(\bmod p)$$

$$\boldsymbol{T}_N\equiv\begin{bmatrix}1&1&\cdots&1\\1&\alpha&\cdots&\alpha^{N-1}\\\vdots&\vdots&&\vdots\\1&\alpha^{N-1}&\cdots&\alpha^{(N-1)^2}\end{bmatrix}(\bmod p)$$

$$\boldsymbol{T}_N^{-1}\equiv N^{-1}\begin{bmatrix}1&1&\cdots&1\\1&\alpha^{-1}&\cdots&\alpha^{-(N-1)}\\\vdots&\vdots&&\vdots\\1&\alpha^{-(N-1)}&\cdots&\alpha^{-(N-1)^2}\end{bmatrix}(\bmod p)$$

$$\boldsymbol{T}_M\equiv\begin{bmatrix}1&1&\cdots&1\\1&\beta&\cdots&\beta^{M-1}\\\vdots&\vdots&&\vdots\\1&\beta^{M-1}&\cdots&\beta^{(M-1)^2}\end{bmatrix}(\bmod p)$$

$$\boldsymbol{T}_M^{-1}\equiv M^{-1}\begin{bmatrix}1&1&\cdots&1\\1&\beta^{-1}&\cdots&\beta^{-(M-1)}\\\vdots&\vdots&&\vdots\\1&\beta^{-(M-1)}&\cdots&\beta^{-(M-1)^2}\end{bmatrix}(\bmod p)$$

可以推导出数论变换(NTT)有如下性质:

(1)线性性;(2)正交性;(3)周期性;(4)对称性;(5)位移定理;(6)循环卷积特性。

数论变换矩阵的元素可变,且二维数论变换矩阵有不同的组合,文献[12]给出了单位根 α 和 β 的求解算法,因篇幅所限略去。Z_p 上的数论变换若有快速计算的效果,通常需要满足三个条件:

(1)长度 N 适合具有快速傅里叶变换 FFT 类型的快速计算,对二进制的计算机来说,N 是 2 的方幂。

(2)由于需要进行大量乘 α 方幂的运算,所以,α 的二进制表示位数越少越好。当 α 是 2 或 2 的方幂时最好,此时乘 α 的一个方幂在计算机上仅为移位操作。

(3)为了便于模 P 的计算,把 P 表示成二进制位时,其位数越少越好。

设变换参数 $M,N=8,\alpha,x_n\in Z_p$($n=0,1,\cdots,N-1$),类似于快速傅里叶变换的按频率抽取的算法将变换矩阵分解,得到快速算法的蝶形流图如图 1 所示。

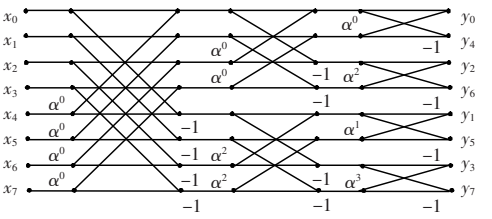


图 1　NTT 快速算法蝶形流图

把二维 NTT 看成将二维序列 $x(n,m)$的每一列先进行一维 N 点的快速数论变换,然后对中间结果矩阵的每一行进行一维 M 点的快速数论变换,则共有 M 个 N 点快速数论变换再加上 N 个 M 点快速数论变换。因此二维快速数论变换可以通过 $M+N$ 次一维快速数论变换实现。所需的乘法次数为(NMlbNM)/2,加法次数为 NMlbNM。如果 α 是 2 或 2 的幂,则只需(NMlbNM)/2 次移位操作。

以 Fermat 数(形如:$F_t=2^b+1,b=2^t$($t=1,2,3\cdots$))为模的数论变换称为 Fermat 数变换,其变换核一般可以为 2 或 2 的方幂,从而具有 FFT 类型的快速算法。此外以 Fermat 数的二进制表示式最为简单,所以使用快速算法时 Fermat 数变换最为常用。

3　基于 NTT 的数字图像色彩置乱

利用数论变换的可逆性与快速算法,同时为了增强保密图像的安全性,采用分块和迭代变换的思想,本章提出灰度图像的数论变换置乱算法并进行了实验验证,算法可推广到二值和彩色图像。

3.1　算法描述

为讨论方便,假设原始图像的大小为 2 的方幂。若原始图像大小不是 2 的方幂,可以通过填充 0 等方式实现。已知灰度图像像素灰度值的范围在 0~255 之间,为减少数论变换模运算的计算量,模 P 应尽可能小,此外为了使用数论变换快速算法,要求变换核为 2 或 2 的方幂。以 Fermat 数(形如:$F_t=2^b+1,b=2^t$($t=1,2,3\cdots$))为模的数论变换具有 FFT 类型的快速算法,同时 Fermat 数的二进制表示式最为简单,所以该文算法取大于 255 的最小 Fermat 数 257 进行模运算。

基于以上分析,算法流程如下:

图像置乱流程:

步骤 1　给定原始图像 P,读入图像信息,将灰度值存至矩阵 $\boldsymbol{F}$,$\boldsymbol{F}=(a_{ij})_{m\times m}$(假定 m 为 2 的方幂),$a_{ij}\in\{0,1,\cdots,255\}$。

步骤 2　将矩阵 $\boldsymbol{F}$ 分为 $N\times N$(N 为 2 的方幂)大小的子块,随机选取满足条件的单位根 α,对每一个子块进行二维快速数论变换,将结果存入原分块,得到置乱后矩阵 $\boldsymbol{F}'$。

步骤 3　进行 k 次迭代变换,用矩阵 $\boldsymbol{F}'$替换矩阵 $\boldsymbol{F}$ 重复步骤 2 的操作,得到 k 次迭代后的矩阵,记为 $\boldsymbol{F}^k$。

步骤 4　输出置乱图像 S。

图像还原流程:

步骤 1　读入图像 S,将灰度值存至矩阵 $\boldsymbol{F}$,$\boldsymbol{F}=(a_{ij})_{m\times m}$(假定 m 为 2 的方幂),$a_{ij}\in\{0,1,\cdots,255\}$。

步骤 2　将矩阵 $\boldsymbol{F}$ 分为 $N\times N$(N 为 2 的方幂)大小的子块,根据置乱中选择的单位根 α,对每一个子块进行二维逆数论变换,将结果存入原分块,得到置乱后矩阵 $\boldsymbol{F}'$。

步骤 3　进行 k 次迭代逆变换,用矩阵 $\boldsymbol{F}'$替换矩阵 $\boldsymbol{F}$ 重复

步骤 2 的操作,得到 k 次迭代后的矩阵,记为 $\boldsymbol{F}^k$。

步骤 4　输出还原图像 P。

3.2　分块大小与算法复杂度

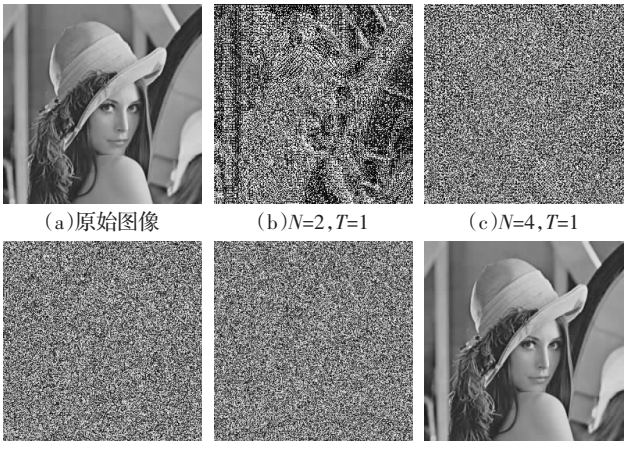
为了使数论变换具有快速演算的效果，要求变换长度 N 必须是高度复合的数。当 N 等于 2 的方幂时就能满足这样的要求。设原图像的数据矩阵的尺寸为 $M\times M$,假定 M 是 2 的幂,可以考虑选择一个小于 M 的数 N,N 也是 2 的幂。设 $M=KN$,从而K 也是 2 的幂，于是可将 $M\times M$ 的块分割为 k^2 个 $N\times N$ 的块,从而存储器容量的空间要求可节省 k^2 倍,计算时间将变为

$$T=k^2N^2\,\mathrm{lb}\,N=M^2(\mathrm{lb}\,M-\mathrm{lb}\,k)$$

即计算时间要求可以减少$((\mathrm{lb}\,M-\mathrm{lb}\,k)$倍,因此选择的 k 越大所需的空间和时间改进越多,而且对多处理器并行结构的支持也越大。但是考虑到数字图像局部相关性比较大的特点,当 N 小到一定程度时,在较小范围内的二维置乱变换会影响置乱的效果,所以实现时应进行折衷。

3.3　实验结果与分析

选取 256×256 大小的 lena.bmp 原始图像,采用上述算法,分别对 2×2、4×4、8×8 和 16×16 大小的分块在 Matlab7.0 上进行仿真实现。实验结果如图 2 所示,其中 N 表示分块大小,T 表示迭代次数。图 2(a)为原始图像,图 2(b)是分块大小为 2×2 时原始图像的置乱结果，从图中可以明显看出原始图像的轮廓,这说明分块太小,不能有效破坏图像相邻像素的相关性,置乱效果差。而图 2(c)、图 2(d)和图 2(e)肉眼看不出原图的轮廓,置乱效果较好。图 2(f)是恢复图像,通过验证,与原图像完全相同。



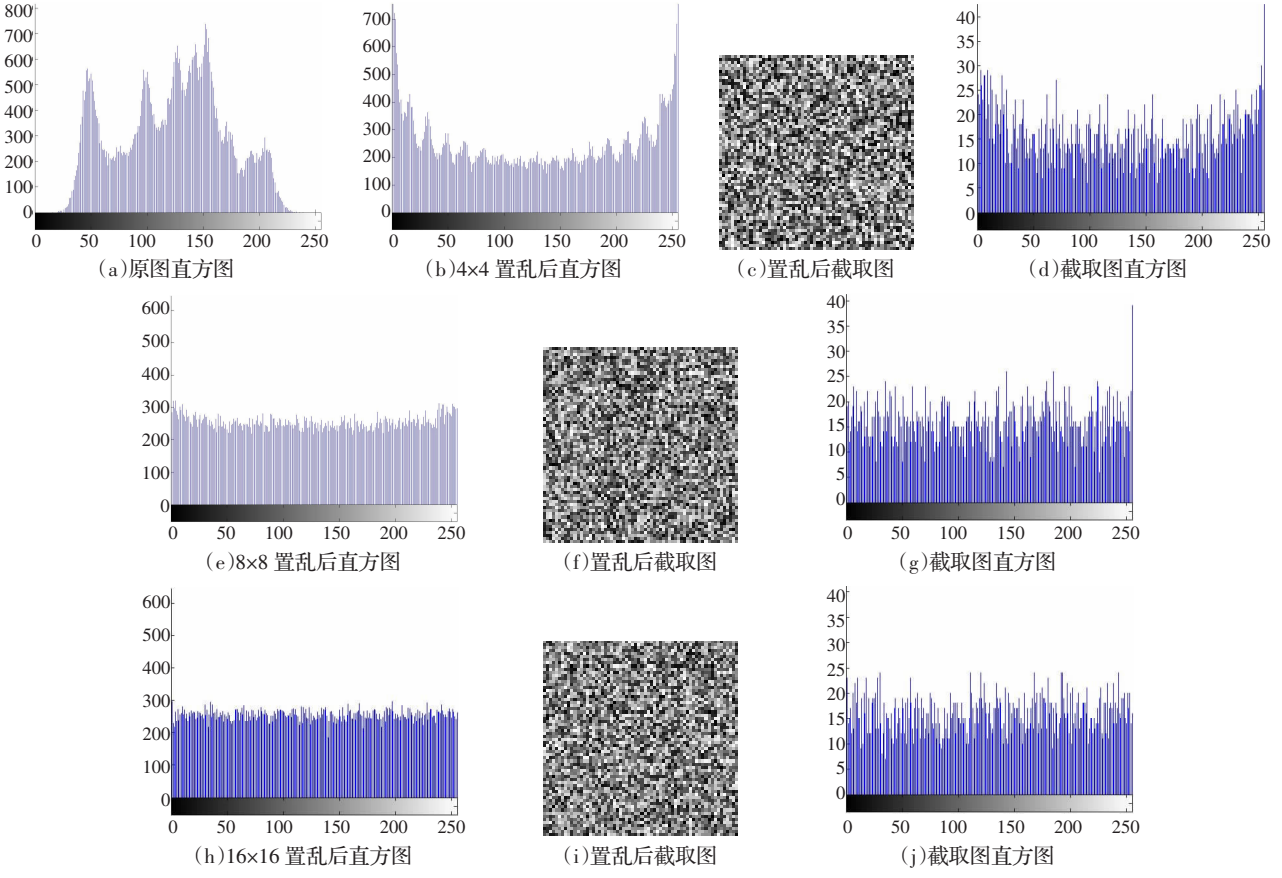
(a)原始图像　(b)N=2,T=1　(c)N=4,T=1

(d)N=8,T=1　(e)N=16,T=1　(f)恢复图像

图 2　采用数论变换的色彩置乱效果图

为了比较图 2(c)、图 2(d)和图 2(e)的置乱效果,需要通过对置乱后的图像数据进行分析。可以通过直方图的比较来分析置乱的效果。对于一幅类似白噪声的图像,其直方图充满整个区域,而且分布比较均匀。同时,任意截取其中的某个小区域,其直方图的分布具有自相似性。图 3 就是对置乱前后图像的直方图的一个比较。其中,图 3(a)为图 2 (a)的直方图,图 3(b)为图 2(c)的直方图,图 3(c)是从图 2(c)中任意截取一块小区域,图 3(d)是图 3(c)的直方图。对图 2(d)和图 2(e)可以类似地生成对应的直方图,如图 3(e)至图 3(j)所示。

为了定量分析置乱效果,引入直方图相似度的定义。设两图像灰度直方图分别为 $h_1(k)$,$h_2(k)$,k=0,1,…,G−1,则定义直方图的相似度为[13]:



(a)原图直方图　(b)4×4 置乱后直方图　(c)置乱后截取图　(d)截取图直方图

(e)8×8 置乱后直方图　(f)置乱后截取图　(g)截取图直方图

(h)16×16 置乱后直方图　(i)置乱后截取图　(j)截取图直方图

图 3　图像直方图的比较

$$\alpha=1-\frac{\sum_{k=0}^{G-1}|h_1(k)-h_2(k)|}{\sum_{k=0}^{G-1}|h_1(k)+h_2(k)|} \quad (3)$$

用式(3)分别计算不同分块大小下置乱后的图像与白噪声图像、置乱后截取的小图像与白噪声图像以及截取部分与整幅置乱图像的直方图相似度,如表 1 所示。

表 1 不同分块下的直方图相似度

分块大小	置乱图像与白噪声	截取部分与白噪声	截取部分与整幅图像
2×2	0.469 6	0.517 3	0.644 0
4×4	0.845 3	0.866 0	0.853 6
8×8	0.965 1	0.900 9	0.889 2
16×16	0.972 8	0.903 8	0.909 4

从表中可以看出,分块越大则经过置乱后对原始图像相关性的破坏越大,从而置乱图像越类似于白噪声,直方图的分布越均匀,置乱效果越好。其中分块大小为 8×8 与 16×16 时各相似度非常接近,若考虑计算时间,分块大小 8×8 较为合理;同时,实验结果说明置乱后的图像改变了原始图像的统计特性,提高了保密信息的迷惑性,通过随机选取单位根和增加迭代次数可进一步增强隐藏图像的安全性。

4 结论

利用矩阵变换的方法进行图像置乱是一类简单有效的方法,其中,基于位置空间的矩阵变换研究较多,但存在不能改变图像统计特性的缺陷,同时变换矩阵形式固定,保密性不高。提出了一种新的色彩空间上的置乱方法,与其他方法相比,具有以下优点:(1)置乱效果好;通过灰度值的置乱改变了图像的灰度级分布,使其与原图像在视觉效果及统计特性上都发生了变化。(2)置乱速度快;采用快速数论变换,乘法仅需移位运算既可实现。(3)逆过程求解简单;在进行置乱的过程中都定义了相应的变换矩阵,因此接收方在恢复的过程中只需要求出相应的逆矩阵就可以得到结果。(4)变换矩阵形式不固定;通过选择合适的参数,二维数论变换矩阵可变且有不同的组合,和其他方法结合,可以设计出加密算法和密钥有效分开,加密算法完全公开,符合现代密码体制要求的图像加密算法,这也是今后研究的方向。

参考文献:

[1] Zhong Ning,Kuang Jing-ming,He Zun-wen.A GA-based optimal image watermarking technique[C]//Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing,2007,1(26):291-294.

[2] Zhang M R,Shao G C,Yi K C.T-matrix and its applications in image processing[J].IEE Electronics Letters,2004,40(25):1583-1584.

[3] 闫伟齐,邹建成,齐东旭.一种基于 DES 的数字图像置乱新方法[J].北方工业大学学报,2002,14(1):1-7.

[4] 陈燕梅,张胜元.基于 AES 的数字图像置乱方法[J].中国图象图形学报,2006,11(8):1077-1080.

[5] 齐东旭,邹建成,韩效宥.一类新的置乱变换及其在图像信息隐蔽中的应用[J].中国科学:E 辑,2000,30(5):440-447.

[6] 丁玮,齐东旭.数字图像变换及信息隐藏与伪装技术[J].计算机学报,1998,21(9):839-843.

[7] 丁玮,闫伟齐,齐东旭.基于 Arnold 变换的数字图像置乱技术[J].计算机辅助设计与图形学学报,2001,13(4):339-341.

[8] 柏森,曹长修,曹龙汉.基于骑士巡游变换的图像细节隐藏技术[J].中国图象图形学报,2001,6(11):1096-1100.

[9] 朱桂斌,曹长修,胡中豫,等.基于仿射变换的数字图像置乱加密算法[J].计算机辅助设计与图形学学报,2003,15(6):711-715.

[10] 李昌刚,韩正之,张浩然.图像加密技术综述[J].计算机研究与发展,2002,39(10):1317-1324.

[11] 王泽辉.二维随机矩阵置乱变换的周期及在图像信息隐藏中的应用[J].计算机学报,2006,29(12):2219-2224.

[12] 孙琦,征德勋,沈仲琦.快速数论变换[M].北京:科学出版社,1980:60-80.

[13] 眭新光,罗慧.基于 S 盒的数字图像置乱技术[J].中国图象图形学报,2004,9(10):1223-1226.

(上接 177 页)

[14] Zhang L,Samaras D.Face recognition under variable lighting using harmonic image exemplars[C]//Proc IEEE Conf Computer Vision and Pattern Recognition,2003,1:19-25.

[15] Zhao J,Su Y,Wang D,et al.Illumination ratio image:Synthesizing and recognition with varying illuminations[J].Pattern Recognition Letter,2003,24:2703-2710.

[16] Lee K C,Ho J,Kriegman D J.Acquiring linear subspaces for face recognition under variable lighting[J].IEEE Trans Pattern Anal Mach Intell,2005,27(5):684-698.

[17] 李弼程,罗建书.小波分析及其应用[M].北京:电子工业出版社,2003.

[18] Wang Wei,Song Jia-tao,Yang Zhong-xiu,et al.Wavelet-based illumination compensation for face recognition using eigenface method[C]//Proceedings of the 6th World Congress on Intelligent Control and Automation,Dalian,China June 21-23,2006.

[19] Martínez A M,Benavente R.The AR face database,Technical Report,no.24[R].CVC,1998-06.

[20] Phillips P J,Wechsler H,Huang J,et al.The FERET database and evaluation procedure for face recognition algorithms[J].Image and Vision Computing,1998,16(5):295-306.

(上接 180 页)

[2] 赵晖,梁光明.一种基于差分算子和区域增长的细胞自动识别方法[J].计算机与现代化,2005,4(10):23-27.

[3] 潘晨,闫相国,郑崇勋.基于 MEAN-SHIFT 和 SVM 的血细胞图像分割[J].仪器仪表学报,2004,8(24):467-472.

[4] 潘晨,闫相国,郑崇勋,等.利用单类支持向量机分割血细胞图像[J].西安交通大学学报,2005,2(39):150-153.

[5] 孙杰,王传永,袁跃辉,等.染色血液白细胞目标图像快速提取方法的研究[J].南开大学学报,2006,12(39):59-63.

[6] 饶洁.基于区域特征及边缘信息的彩色血液显微图像分割[D].成都:四川大学,2006.

[7] Comaniciu D,Meer P. Meanshift:A robust approach toward feature space analysis[J].IEEE Trans on Pattern Analysis and Machine Intelligence,2002,24(5):603-619.

[8] 王兆仲,赵宇,周付根,等.血细胞图像的自适应分割[J].中国体视学与图像分析,2002,3(7):49-52.

[9] Ruberto C D,Dempster A,Khan S,et al.Analysis of infected blood cell images using morphological operators[J].Image and Vision Computing,2002,20(2):133-146.