文章编号 1004-924X(2008)08-1483-07

适用于矩形图像的新二维映射图像加密算法

任洪娥,尚振伟,张 健
(东北林业大学 信息与计算机工程学院,黑龙江 哈尔滨 150040)

摘要:针对目前的图像加密方法大多只局限于对方形图像进行加密的特点,提出了一种同时适用于方形图像和矩形图像的加密算法。将基于图像分割的新二维映射用于图像位置置乱,将含有混沌映射的扩散函数用于图像灰度置乱,从而得到一种位置置乱和灰度置乱相结合的图像加密算法。实验仿真结果表明,该算法能够很好地实现对任意大小的方形和矩形图像进行加密,且具有密钥空间大($10^{15}\sim10^{30}$),密钥敏感性强以及能够抵御统计和已知明文攻击等优点,基本满足图像加密的有效性和安全性要求。

关 键 词:图像加密;矩形图像;置乱;扩散;混沌映射
中图分类号:TP309.7 **文献标识码**:A

Image encryption algorithm based on new two-dimensional map for rectangular image

REN Hong-e, SHANG Zhen-wei, ZHANG Jian

(*College of Information and Computer Engineering, Northeast Forestry University, Harbin* 150040, *China*)

Abstract: A new encryption algorithm was proposed to apply to both square and rectangular image encryptions. A new two-dimensional map based on image segmentation was applied to the location scrambling, and a spread function containing chaos map to the gray scrambling, so that an image encryption algorithm combined with both position and gray scramblings was obtained. The experimental simulation shows that this algorithm can achieve good image encryption for any size of square and rectangular images with a large key space ($10^{15}\sim10^{30}$). Proposed algorithm also has advantages in withstanding statistical and known plaintext attack, which basically satisfies the requirements of validity and safety for image encryption.

Key words: image encryption; rectangular image; scrambling; diffusion; chaotic map

1 引 言

随着计算机网络和多媒体技术的迅速发展,数字图像的安全保障问题日益凸显。因此,图像加密技术近年来成为一个非常重要的研究方向。传统的图像置乱方法如 Arnold 变换,面包师变换,Standard 映射,幻方变换,魔方变换等已不再

收稿日期:2007-12-03;**修订日期**:2008-02-27.
基金项目:国家自然科学基金资助项目(No. 30771679);国家 948 计划资助项目(No. 2005-4-62)

安全。1989 年 Matthews 采用基于变形 Logistic 映射的混沌加密算法，提出了“混沌密钥”的概念，由此混沌加密逐渐成为研究的热点[1]，但是基于混沌理论的图像加密方法大多不能抵抗已知明文攻击[2]。最近黄峰提出了一种基于分割思想的图像加密算法，首先将原始图像各像素点通过某种映射拉伸成为一条直线，然后再折叠成一个新图像，从而实现对图像位置置乱的目的[3]。该加密算法在抗攻击能力上有了较大的提高，但只限于对方形图像进行加密，另外算法中用于灰度置乱的扩散函数也过于简单，在未知密钥的情况下，通过对密图进行简单的像素值逆运算就可以解出原图位置置乱后的图像（第一个像素点除外），从而可以得到原图像的精确直方图。本文针对这些不足提出了一种图像加密算法，利用新的二维映射进行图像位置置乱，同时采用一个更加安全的基于混沌映射的扩散函数，实现图像灰度置乱。该算法不仅适用于加密方形图像而且对矩形图像同样适用，实验结果表明对矩形图像的加密效果更好。

2　新二维映射原理与算法

2.1　新二维映射原理

设图像 A 的大小为 $M\times N$，首先将图像分为左右两个部分，左边的图像块为 M 行，$\lceil N/2\rceil$ 列，右边的图像块则有 M 行，$\lfloor N/2\rfloor$ 列（其中 $\lfloor X\rfloor$ 表示不大于 X 的最大整数，$\lceil X\rceil$ 表示不小于 X 的最小整数）。对于图像块的每相邻两列，可以将一列元素依次插入到另一列的纵向相邻的两像素之间，反复该过程，依次连接各像素点，原始图像块将被拉伸成为一条直线。根据插入的角度不同，共有 4 种插入方法，如图 1 所示：

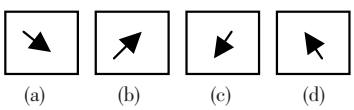


图 1　4 种插入方法

Fig. 1　Four insert methods

举例说明：当图像为 3×5 时，采用插入方法(a)时，如图 2 所示，则依次将像素(3,1)插入像素(3,2)之后，像素(2,1)插入像素(2,2)和(3,2)之间，像素(1,1)插入像素(1,2)和(2,2)之间……重复这个过程，即按照图 2 的方式可将原图像拉伸成为一条直线：(3,1),(3,2),(2,1),(2,2),(1,1),(1,2),(3,3),(3,4),(2,3)……，其它 3 种插入方法和方法(a)类似。

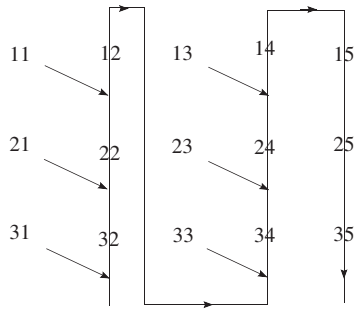


图 2　插入方法(a)

Fig. 2　Insert method (a)

从图 1 所示的 4 种插入方法中任选两种分别对原图像的左右两个图像块进行操作，这样原始图像块将被拉伸成为两条直线，依次将它们连接起来得到一条长为 $M\times N$ 直线，然后，再折叠成一个 $M\times N$ 的新图像，实现图像位置的置乱。

根据左右两个图像块采用的插入方法的不同可以得到 12 种不同的组合方式，如图 3 所示。

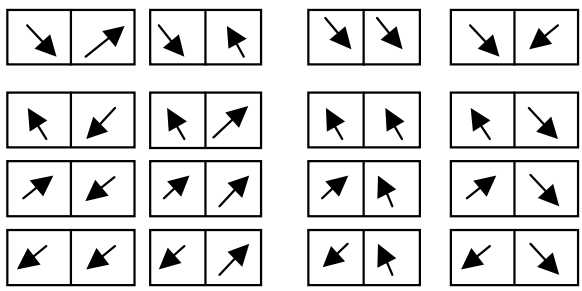


图 3　构造映射示意图

Fig. 3　Sketch map of constitution

在实际的加密中，可以任意抽取其中的若干组合方式用于图像位置置乱。

2.2　新二维映射计算算法

2.2.1　各插入方法的计算算法

由于映射是由 4 个插入方法任意组合形成的，分别给出各插入方法的算法如下：

设图像大小为 $M\times N$，$A(i,j)$ 为图像中的任意一点像素值 $i=1,2\cdots,M$，$j=1,2\cdots,N$，$L(t)$，

$t=1,2,\cdots,M\times N$ 为将 $A(i,j)$ 拉伸后的一维向量。

(1)方法(a)的算法:

如图 2 所示,插入方法为(a)算法:

当 j 是奇数时,

若 $j=N$,

$$L(M\times(j-1)+i)=A(i,j), \tag{1}$$

若 $j<N$,

$$L(M\times(j-1)+2\times(M-i)+1)=A(i,j), \tag{2}$$

当 j 是偶数时,

$$L(M\times(j-2)+2\times(M-i+1))=A(i,j). \tag{3}$$

(2)方法(b)的算法:

当 j 是奇数时,

若 $j=N$,

$$L(M\times(j-1)+i)=A(i,j), \tag{4}$$

若 $j<N$,

$$L(M\times(j-1)+2\times i-1)=A(i,j), \tag{5}$$

当 j 是偶数时,

$$L(M\times(j-2)+2\times i)=A(i,j). \tag{6}$$

(3)方法(c)的算法可以通过下列过程得到:

将原图 A 做一次镜像,如式(7)所示,A' 表示镜像后的图像,

$$A'(i,j)=A(i,N-j+1), \tag{7}$$

其中,$i=1,2,\cdots,M$;$j=1,2,\cdots,N$,然后通过算法(a)中式(1)~(3),可得到算法(c)。

(4)方法(d)的算法可以通过下列过程得到:

将原图 A 如式(7)所述做一次镜像得到 A' 通过算法(b)中(4)~(6)式,可得到方法(d)的算法。

2.2.2　新映射的计算算法

对于图 3 所示的 12 种映射可以随机抽取其中的两种或多种映射组合用于图像加密,本文的加密方法采用映射①↘|↗和映射②↖|↙,所以这里只给出映射①和②的算法。

设图像 A 的大小为 $M\times N$,首先将 A 分为左右两个部分,左边的图像块 B 为 M 行,$\lceil N/2\rceil$ 列,右边的图像块 C 则为 M 行,$\lfloor N/2\rfloor$ 列,设 $D=\lceil N/2\rceil$。

(1)映射①算法:

对 B 实行算法(a)得到长为 $M\times D$ 的直线 L_1,然后对 C 实行算法(c)得到长为 $M\times(N-D)$ 的直线 L_2。则

$$L(1:(M\times D))=L_1, \tag{8}$$

$$L(((M\times D)+1):M\times N)=L_2, \tag{9}$$

得到一条长为 $M\times N$ 的直线 L。

(2)映射②算法:

映射②算法可以通过下列过程得到:

将原图 A 做一次镜像,如式(7)所示得 A',然后对 A' 施行映射①算法,如此得到映射②的算法。

(3)折叠算法:

把直线 L 重新折叠成 $M\times N$ 的图像的算法如式(10)所示:

$$E(i,j)=L((i-1)\times N+j), \tag{10}$$

其中,$i=1,2,\cdots,M$;$j=1,2,\cdots,N$。$E(i,j)$ 是位置置乱后的图像。

3　图像加密、解密算法

3.1　图像加密算法原理

本加密算法采用了位置置乱和灰度置乱相结合的方法,图像的整个加密过程如图 4 所示。

3.1.1　密钥设计

如图 4 所示,算法采用两个密钥 K_1 和 K_2,其中 K_1 用于图像位置置乱,K_2 作为混沌映射的初值,用于灰度置乱,其范围为(0,1)。位置置乱中采用了映射①和映射②,其映射次数可以作为密钥 K_1。如 $K_1=1\ 234$,表示依次用①映射 1 次,用②映射 2 次,然后用①映射 3 次,最后用②映射 4 次。由于图像是有限像素点的集合,像素的排列组合是有限的。因此在有限次迭代之后,加密图像会恢复到原来的状态,即混沌映射都具有庞加莱回复性。Fridrich[4] 指出,当迭代次数较小(如<15)时,加密算法是安全的。本文将密钥

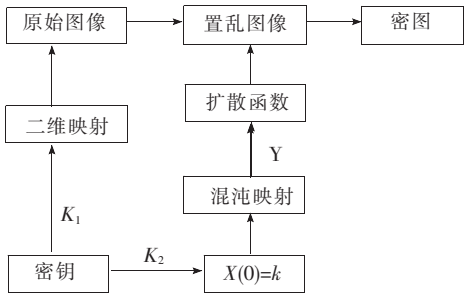


图 4　图像加密算法

Fig. 4　Encryption algorithm of image

K_1 的每一位设计为$>10^{15}$的整数。由于新映射的周期非常大（$<10^{15}$），这种设计是合理的。本文采用的扩散函数如式(11)所示。

$$v'_k = v_k + Y^2 \bmod L, \tag{11}$$

其中，v_k 是指每一个像素的灰度值，v'_k 为扩散后的像素灰度值，Y 为由混沌映射产生的混沌序列，L 为像素灰度级。该类扩散函数结构简单、扩散速度快。

3.1.2 混沌序列 Y 的产生

采用简单的 logistic 映射，其函数式如下：

$$X_{n+1} = f(\mu, X_n) = \mu X_n(1 - X_n). \tag{12}$$

当 $\mu = 4$ 时，系统处于混沌状态[5]，此时系统产生的序列具有随机性，遍历性，对初值的敏感性，其范围为(0,1)。K_2 作为混沌序列的初值 $X(0)$。对产生的混沌实值序列，每个实值取其从百分位开始的 3 个数字组成的十进制数构成序列 Y 即对于 $X(i)=0.b_1b_2b_3b_4b_5\cdots\cdots$序列，$Y$ 由式(13)得到：

$$Y(i) = 100 \times b_1 + 10 \times b_2 + b_3, i = 0,1,2,\cdots. \tag{13}$$

在扩散函数中引入了伪随机序列，克服了在已知扩散函数时通过简单的逆运算就可得到原图像精确直方图的缺陷，使得该加密方法可以抵御已知明文攻击。

3.2 图像加密算法步骤

图像加密算法可分为 3 步进行：

(1)利用密钥 K_1 及映射①或②的算法，将图像 $A(i,j)$拉伸处理为一条直线 $L(t)$，其中 $t=1,2,\cdots,M\times N$。

(2)利用折叠算法如式(10)所示，将直线折叠处理 ，得到置乱图像 $E(i,j)$。

(3)利用密钥 K_2 及 logistic 映射和扩散函数，对置乱图像进行扩散处理得到密图。

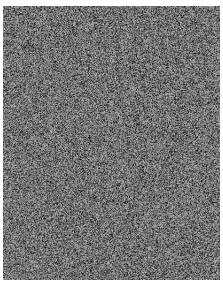
解密算法与加密算法密钥相同，过程相反。

4 仿真结果与分析

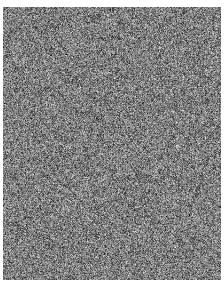
4.1 仿真结果

为了测试该加密方法的性能，利用 MATLAB 对该算法进行了仿真。将 410 pixel×512 pixel 的 cameraman 灰度图像作为实验图像，在密钥 K_1= 12 345 678 和 K_2=0.2 的条件下对该图像进行加密，其结果如图 5(b)、(c)所示。

(a) 原始图像
(a) Original image



(b)位置置乱后密图
(b) Encrypted image after location scrambling



(c)灰度置乱后密图
(c) Encrypted image after gray scrambling

图 5 仿真结果
Fig. 5 Simulation results

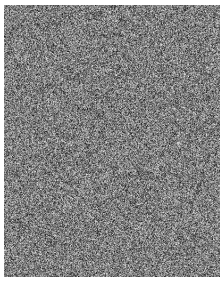
4.2 穷举分析

对于位置置乱，研究表明 ，密钥空间大小只和密钥长度有关。在理想情况下(计算速度允许)，密钥长度能无限增加。因此密钥空间可以无限大。对于灰度置乱，基于 logistic 混沌映射的图像加密算法具有很大的密钥量，以混沌映射 logistic 中的 x_0 作为密钥，加密的密钥空间可以无限大。然而，由于计算机数字精度的限制，实际操作中只能把密钥空间限制在一个小范围内。在此方案中，采用双精度浮点数作为密钥，由于把密钥输入限制在了(0,1)之间，所以密钥空间为 $10^{15}\sim10^{30}$。

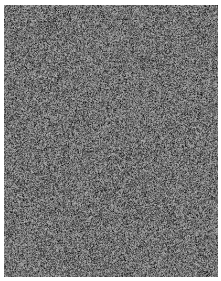
可见，试图用穷举方法来进行攻击显然是不能够实现的。

4.3 密钥敏感性分析

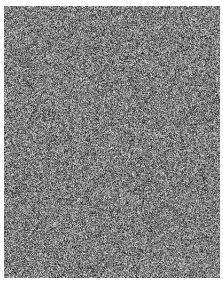
不考虑灰度置乱，仅用 K_1= 12 345 678 对



(a) K_1=12 345 678 密图
(a) Encrypted image K_1=12 345 678



(b) K_1=12 345 677 解密图
(b) Deciphered image K_1=12 345 677

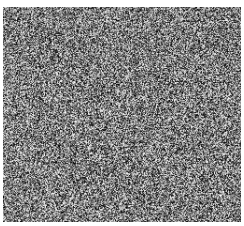


(c) K_1=12 345 679 解密图
(c) Deciphered image K_1=12 345 679

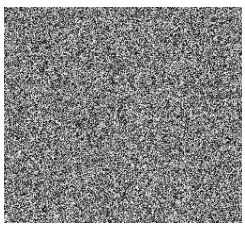
(d) K_1=12 345 678 解密图
(d) Deciphered image (K_1=12 345 678)

图 6　密钥 K_1 敏感性分析

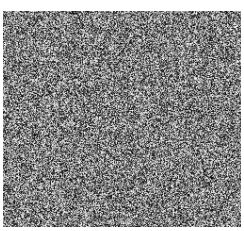
Fig. 6　Sensitivity analysis of secret key K_1



(a) K_1=12 345 678 K_2=0.2 密图
(a) Encrypted image (K_1=12 345 678,K_2=0.2)



(b) K_1=12 345 678 K_2=0.200 2 解密图
(b) Deciphered image (K_1=12 345 678,K_2=0.200 2)



(c) K_1=12 345 678 K_2=0.199 9 解密图
(c) Deciphered image (K_1=12 345 678,K_2=0.199 9)

(d) K_1=12 345 678 K_2=0.2 解密图
(d) Deciphered image (K_1=12 345 678,K_2=0.2)

图 7　密钥 K_2 敏感性分析

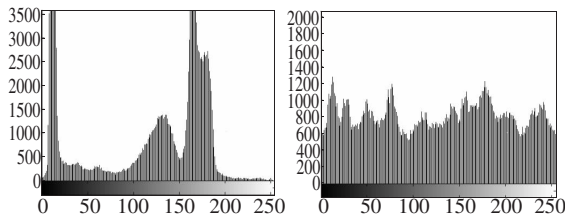
Fig. 7　Sensitivity analysis of secret key K_2

一个 410 pixel×512 pixel 的灰度图像加密的密图如图 6(a)所示，用 K_1=12 345 677 进行解密，结果如图 6(b)所示。用 K_1= 12 345 679 解密，结果如图 6(c)所示。可以看到，即使加密密钥和解密密钥仅有很小的差异(1 位)，也无法解密密图，证明位置置乱加密算法对密钥非常敏感。

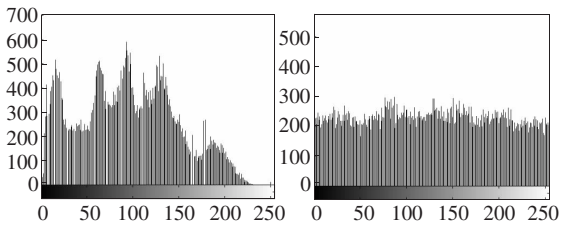
加入灰度置乱后，算法中将混沌映射的初值作为密钥 K_2，而 logistic 映射对混沌态初始值是很敏感的，这也确保了此加密方案对密钥的敏感性。在密钥 K_1 正确无误的情况下，即使是 K_2 微小的变化，都无法准确地恢复出原始图像。这里对灰度图像做了一个实验，用 K_1=12 345 678，K_2=0.2 对一个 256 pixel×230 pixel 的灰度图像进行加密，密图如图 7(a)所示，稍微改变密钥 K_2 的值，则解密后图像完全不可读(如图 7(b)，7(c)所示)。只有在 K_1，K_2 都正确时，才能正确解密出原始图像(如图 7(d)所示)。

4.4　灰度直方图分析

两个实例图像在加密前后的灰度直方图如图 8 所示：



(a) 410×512 原图直方图　(b) 410×512 密图直方图
(a) Grey histogram of 410×512 original image　(b) Grey histogram of 410×512 encrypted image



(c) 256×230 原图直方图　(a) 256×230 密图直方图
(c) Grey histogram of 256×230 original image　(a) Grey histogram of 256×230 encrypted image

图 8　灰度直方图分析

Fig. 8　Grey histogram analysis

对图像加密前后的灰度直方图进行分析，由图 8 可以看出，原始图像的像素点集中分布在某些灰度上，而加密图像的像素值均匀分布在整个

灰度值空间，从而说明该加密方法具有很好的灰度均匀分布特性，可以抵抗一定程度的统计分析攻击。

4.5 相邻像素相关性分析

研究表明图像置乱效果的好坏与相邻像素相关性的大小存在反比关系，相关性越大，置乱效果越差，相关性越小，置乱的效果越好。测试置乱图像的水平(垂直)相邻像素的相关性方法如下：

将图像的像素与其水平(垂直)向的下一个像素组成相邻像素对，然后用下面的公式计算相邻像素的相关性：

$$D(x) = 1/k\sum_{i=1}^{k}[x_i - E(x)]^2, \quad (14)$$

式中，x 是像素的灰度值；k 是像素数；$E(x)$是 x 的数学期望，$D(x)$是 x 的方差。

$$\mathrm{cov}(x,y) = 1/k\sum_{i=1}^{k}[x_1 - E(x)][y_i - E(y)], \quad (15)$$

式中，x 是像素对中前者的灰度值；y 是像素对中后者的灰度值，$\mathrm{cov}(x,y)$ 是 x,y 的协方差。

$$r_{xy} = \mathrm{cov}(x,y)/(\sqrt{D(x)}\ \sqrt{D(y)}), \quad (16)$$

式中，r_{xy}是相关系数[6]。

在以上用到的两个实例图的原图和加密后的图像上分别随机取 1 000 个像素点，利用公式(14)～(16)分别计算其水平、垂直方向相邻像素的相关系数，求得的结果如表 1 所示。从表中可以看出，加密图像比原始图像在各方向的相关系数均小得多，说明算法的置乱程度高。

表 1 相邻像素相关性比较

Tab. 1 Correlation comparison of adjacent pixels

像素关系	垂直相邻像素相关系数	水平相邻像素相关系数
256×230 原始图像	0.991 0	0.985 6
256×230 只经位置置乱后图像	−0.059 4	0.943 7
256×230 最终加密后图像	0.035 8	0.040 4
410×512 原始图像	0.994 7	0.984 5
410×512 只经位置置乱后图像	0.000 3	−0.012 1
410×512 最终加密后图像	−0.029 6	−0.021 0

5 结　　论

本文根据折叠、拉伸的思想，提出了一种新的二维混沌映射，并将其应用于图像的位置置乱，实验结果表明该方法能够取得很好的置乱效果。此外为了抵御已知明文攻击，将含有混沌映射的扩散函数对位置置乱后的图像，并进行灰度值的置乱，仿真结果证明了该算法的有效性和安全性。另外，为了进一步提高抗攻击能力，可以将本算法的扩散函数采用高维混沌映射，以及多种位置置乱插入方法。

参考文献：

[1] 梁士利，张玲，王广，等. 一维加法 CA 的同步系统研究[J]. 光学 精密工程，2006，14 (3)：4952497.
LIANG SH L，ZHANG L，WANG G，*et al*.. Study on synchronization of 1D-k3 additive cellular automata [J]. *Opt. Precision Eng*.，2006，14(3)：495-497. (in Chinese)

[2] 张大奇，康宝生. 基于混沌序列和分组密码的数字图像置乱技术[J]. 计算机应用与软件，2007，24(7)：21-29.
ZHANG D Q，KANG B SH. Digital image scrambling based on chaotic sequence and ZF-02 block cipher scheme [J]. *Computer Applications and Software*，2007，24(7)：21-29. (in Chinese)

[3] 黄峰，冯勇. 利用图像分割思想的二维混沌映射及图像加密算法[J]. 光学 精密工程，2007，15(7)：1096-1102.
HUANG F，FENG Y. Novel 2D chaotic map based on image segmentation and image encryption approach [J]. *Opt. Precision Eng*.，2007，15(7)：1096-1102. (in Chinese)

[4] FRIDRICH J. Symmetric ciphers based on two-dimensional chaotic maps[J]. *Int. J. Bifurc. Chaos*, 1998,8(6):1259-1284.

[5] 樊春霞,姜长生.一种基于混沌映射的图像加密算法[J].光学 精密工程,2004,12(2):179-184.
FAN CH X,JIANG CH SH. Image encryption based on discrete chaotic maps [J]. *Opt. Precision Eng.*,2004,12(2):179-184. (in Chinese)

[6] 孙鑫,易开祥,孙优贤.基于混沌系统的图像加密算法[J].计算机辅助设计与图形学学报,2002,14(2):1-4.
SUN X,YI K X,SUN Y X. New image encryption algorithm based on chaos system [J]. *J. Computer-Aided Design & Computer Graphics*,2002,14(2):1-4. (in Chinese)

作者简介:任洪娥(1962－) 女,教授,博士,硕士生导师,研究方向为图像处理与模式识别、人工智能与智能控制、优化设计与计算机辅助建模等。E-mail:renhonge@163.com

尚振伟(1983－),女,研究生,研究方向为图像处理、信息安全。E-mail:dabaiweiwei@163.com

张　健(1980－),男,博士生,研究方向为图像处理、信息安全、混沌理论。

●下期预告

激光跟踪测量系统角度自动校正装置设计

刘万里[1],王占奎[2],欧阳健飞[3],曲兴华[1]

(1.天津大学 精密测试技术及仪器国家重点实验室,天津 300072;
2.河南科技学院 机电学院,河南 新乡 453003;3.河南理工大学 精密工程研究所,河南 焦作 454003)

研制开发了一种能使激光跟踪测量系统在动态条件下连续测量的角度自动校正装置。它主要由精密圆形导轨和角度方位自动调节机构组成,能使角锥棱镜在动态测量过程中始终指向激光跟踪测量系统,从而实现在动态条件下的连续工作。最后利用研制角度自动校正装置对激光跟踪测量系统进行了角度误差补偿试验,结果表明该装置使激光跟踪测量系统的水平角测量误差由 34.69 μm 减小到 9.71 μm,垂直角测量误差由 35.43 μm 减小到 10.03 μm,从而有效地提高了激光跟踪测量系统的角度测量精度,解决了激光跟踪测量系统在动态测量中因角锥棱镜逆反射器接收角度范围限制而导致无法测量的问题。