一种基于二维混沌映射的三角形图像信息隐藏方案

冯志杰，王红梅
（青岛滨海学院 教务处，山东 青岛 266555）

摘　要：针对空域图像信息隐藏技术容易出现高失真、频域图像信息隐藏技术藏量偏小的问题，提出一种基于二维混沌映射的三角形隐藏方案。首先，利用二维 Baker 映射对秘密图像的像素位置进行置乱，使其能量在频谱上分布趋向均匀，其优点是用统计方法不易检测出隐藏信号，更有利于信息的隐藏；然后，通过探索秘密图像块和覆盖图像块的关系进行块匹配，构建一个直角三角形，找出其差异，生成密钥，并将秘密图像信息嵌入到覆盖图像中。实验结果表明：该方案实现了双重加密，增加了破解难度，具有较大的密钥空间，伪装图像的逼真度高，可以加密任意尺寸的图像，能够快速实现。

关键词：信息隐藏；混沌；Baker 映射；三角形算法

中图分类号：TP391.41　　**文献标志码**：A　　**文章编号**：1672-3767(2014)05-0063-07

Triangular Algorithm of Image Data Hiding Based on Two-dimensional Chaotic Map

Feng Zhijie, Wang Hongmei
(Dean's Office, Qingdao Binhai University, Qingdao, Shandong 266555, China)

Abstract: To solve the problem of high distortion of image information hiding in the space domain and the small capacity in frequency domain, a scheme of triangular-ciphers was proposed based on two-dimensional chaotic maps with analysis on theory and technology of information hiding. Firstly, the image information algorithm in the secret image's pixel position was scrambled by two-dimensional Baker map to make the spectrum energy evenly distributed. This promotes information hiding in preventing hidden information being detected by statistical method. Then the scrambled image was hidden by triangular algorithm. The experimental results show that this scheme realizes double encryption, increasing difficulty of decipher, with larger key space and higher stego-image's fidelity. Images of any size can be enciphered more efficiently.

Key words: data-hiding; chaos; Baker map; triangular algorithm

图像文件相对文本具有信息量大、相邻像素间具有相关性等特点。DES(data encryption standard，数据加密标准)算法、AES(advanced encryption standard，高级加密标准)算法等已被广泛应用到图像加密领域，但这些算法加密度低、安全性不能保证，需要同时解决压缩和加密等问题。混沌映射为多媒体信息加密和隐藏提供了一种快速有效而且简单经济的新途径。Shannon 指出：好的加密系统应具有对密钥的敏感性，以及能够将明文充分地置乱并改变其统计特性[1]，而混沌恰恰具有对初值和参数敏感的特性以及混沌映射的拓扑传递性。

近年来，人们提出了许多新的图像加密方案，如余建德等[2]提出按像素的灰度值作图像区域非均匀剖分的思想，将像素的灰度值作为拟合数据，用最小二乘法作数据拟合，得到数字图像的自适应非均匀剖分算法。崔世宇[3]提出基于维诺图(Voronoi diagram, VD)的图像信息隐藏算法，将灰度载体图像的像素对映射到灰度值空间坐标系内，构建维诺图，利用优化算法对像素对所代表意义进行赋值，通过互有联系的像素对相互

收稿日期：2014-03-20
基金项目：山东省高等学校科技计划项目(J09LG67)
作者简介：冯志杰(1969—)，男，山东青州人，副教授，主要从事模式识别和图像处理方面的研究. E-mail: bhfzj@163.com

覆盖或保持原有像素对的形式，将秘密信息无感知地嵌入到图像中。黄峰等[4]研究了基于构造三角形的可逆二维映射图像加密算法，将原图像像素构造成等腰三角形，从而达到置乱像素位置的目的，能够加密任意形状的图像。Fridrich[5]分别采用 Baker 映射和 Cat 映射构造了二维可逆图像加密方案。张小华等[6]将混沌序列进行量化，再用量化序列进行置乱，量化过程是一个信息损失的过程，这使得解密者无法推测混沌系统的初值。乌旭等[7]提出一种复合混沌系统的思想，产生出 4 个混沌序列，经异或运算得到新的复合序列，使得解密者无法由破译的加密模板来推测混沌系统。

本研究将混沌映射跟三角形算法有效结合，提出了一种基于二维混沌映射的三角形隐藏方案。该方案采用双重加密，增加了破解难度，伪装图像的逼真度高，可以加密任意尺寸的图像，且具有较大的密钥空间，能够快速实现。

1 方案描述

本文中，需要加密的图像称为秘密图像(secret image)，用 S 表示；载体图像称为覆盖图像(cover image)，用 C 表示。首先，利用二维 Baker 映射对秘密图像的像素位置进行置乱，使其能量在频谱上分布趋向均匀，这样用统计方法不易检测出隐藏信号，更有利于信息的隐藏。再通过探索秘密图像块和覆盖图像块的关系进行块匹配，利用三角形加密算法进一步加密。加密流程如图 1 所示。

解密过程是加密过程的逆过程，如图 2 所示。

2 算法设计

2.1 利用二维 Baker 映射对秘密图像进行置乱

2.1.1 二维 Baker 映射

定义连续二维 Baker 映射：

$$B(x,y)=\begin{cases}(x/\alpha,\alpha y), & 0\leqslant x<\alpha\\((x-\alpha)/\beta,(\alpha+\beta y)), & \alpha\leqslant x\leqslant 1\end{cases},$$

取 $\alpha+\beta=1$ 为保面积映射。

该映射先在水平方向上对数据进行分割，然后对数据进行压缩和拉伸，再将结果按一定顺序排列在相同面积内。该映射可以应用于任意尺寸的图像，因而采用更具有一般性的矩形为例来说明，整个过程如图 3 所示。

1)将 $M\times N$ 的矩形沿着 X 轴方向切分成任意竖条；

2)将每个竖条沿着 X 轴扩展，沿着 Y 轴压缩(保持变换前后面积不变)；

3)将 2)中得到的长条堆叠成新的矩形。

2.1.2 混沌加密算法

1)将尺寸为 $M\times N$ 个像素的秘密图像(图 4(a))沿着水平方向分为 k 个矩形块，矩形的宽度为 m_i，且 $m_1+m_2+\cdots+m_k=M$，则每个矩形就有 $N\times m_i$ 个像素(图 4(b))；

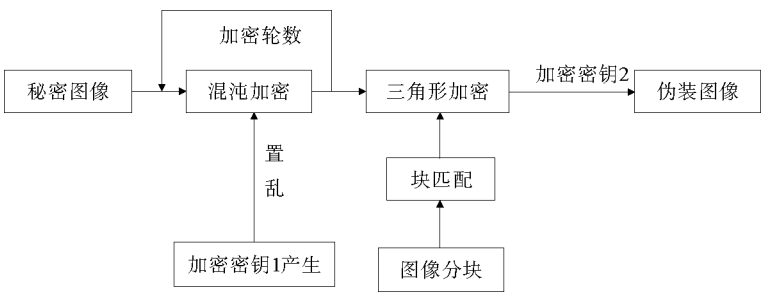


图 1 加密流程图

Fig. 1 The flowchart of the encryption

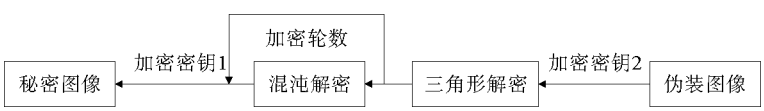


图 2 解密流程图

Fig. 2 The flowchart of the decryption

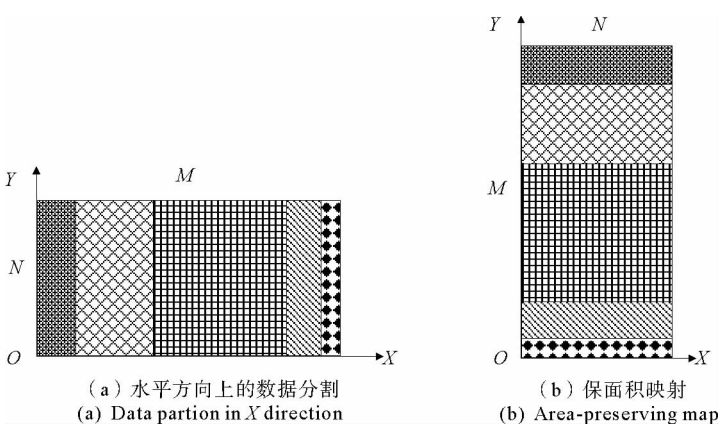


图 3 二维 Baker 映射对秘密图像的置乱示意图

Fig. 3 Scrambling the secret-image by two-dimensional Baker map

2)把每个矩形块分成 m_i 个子块(图 4(c)),每个子块正好有 $(N\times m_i)/m_i=N$ 个像素。如果 N 能被 m_i 整除,则分成的子块为矩形块,否则,分成的子块不会正好呈矩形;

3)将每个子块中的像素按从下到上,从左到右的顺序重新排列成一行(图 4(d));

4)将子块对应的像素行按从上到下,从右到左的顺序排成新的矩形(图 4(e))。

图 4 混沌加密算法

Fig. 4 Chaotic encryption algorithm

2.2 三角形算法

2.2.1 加密算法

通过一个直角三角形建立覆盖图像块和秘密图像块的关系,找出其差异,生成密钥,并将带有秘密图像信息的密钥嵌入到覆盖图像中,形成伪装图像。

1)图像块匹配。用覆盖图像块 $\boldsymbol{C}_i$,秘密图像块 $\boldsymbol{S}_i$ 分别作为三角形的斜边和一条直角边,而另一条直角边则表示其差异 $\boldsymbol{D}_i$。

将 $\boldsymbol{S}_i=[s_{kj}]_{n\times n}$ 和 $\boldsymbol{S}_i=[s_{kj}]_{n\times n}$ 中的元素依次配对,则块差异 $\boldsymbol{D}_i=[d_{kj}]_{n\times n}$,其中 $d_{kj}=\sqrt{\mathrm{sign}(s_{kj}-c_{kj})(s_{kj}^2-c_{kj}^2)}$($d_{kj}$,$s_{kj}$,$c_{kj}$ 分别表示 $\boldsymbol{D}_i$,$\boldsymbol{S}_i$,$\boldsymbol{C}_i$ 中的元素,$k,j=1,2,\cdots,n$)。

2)生成密钥 $\boldsymbol{D}'_i=\dfrac{\boldsymbol{D}_i-\hat{\boldsymbol{D}}_i}{\hat{\sigma}_i}$。其中 $\hat{\boldsymbol{D}}_i=\hat{d}_i\boldsymbol{A}$,$\boldsymbol{A}=\begin{pmatrix}1&1&\cdots&1\\1&1&\cdots&1\\\vdots&\vdots&\cdots&\vdots\\1&1&\cdots&1\end{pmatrix}_{n\times n}$,$\hat{d}_i$ 为 $\boldsymbol{D}_i$ 的估计值,$\hat{d}_i=\dfrac{1}{n^2}\sum_{k=1}^{n}\sum_{j=1}^{n}d_{kj}$,$\hat{\sigma}_i=\sqrt{\dfrac{1}{n^2-1}\sum_{k=1}^{n}\sum_{j=1}^{n}(d_{kj}-\hat{d}_i)^2}$ 为 $\boldsymbol{D}_i$ 的标准差。

3)嵌入密钥 $\boldsymbol{D}'_i$ 到覆盖图像块中,生成伪装图像 $\boldsymbol{C}_{\boldsymbol{S}_i}=[\boldsymbol{C}_i+\boldsymbol{D}'_i]$,这里的算符 $[\cdot]$ 表示对其中的元素取整,得到伪装图像块,并组合生成伪装图像 $\boldsymbol{C}_{\boldsymbol{S}}$。

2.2.2 解密算法

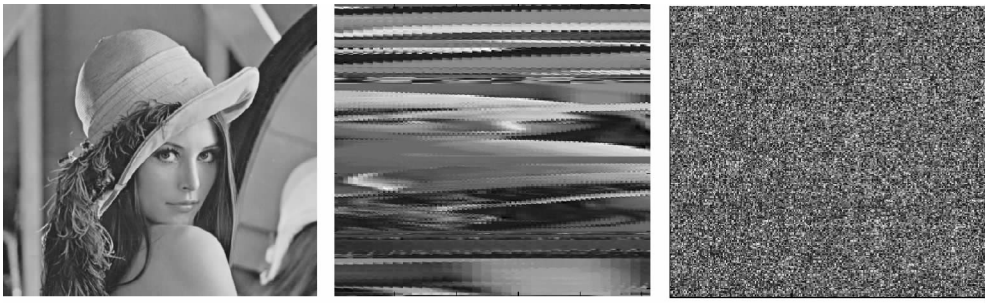
解密算法是加密过程的逆过程,只要提取覆盖图像信息 $\boldsymbol{C}_i$ 和密钥 $\boldsymbol{D}'_i$,以及 $\hat{\sigma}_i$ 和 $\hat{\boldsymbol{D}}_i$ 就可以由 $s_{kj}=\sqrt{c_{kj}^2+\mathrm{sign}(s_{kj}-c_{kj})(d'_{kj}\hat{\sigma}_i+\hat{d}_i)^2}$($d'_{kj}$ 为 $\boldsymbol{D}'_i$ 的元素)获取所有的秘密图像块 $\boldsymbol{S}_i$,再恢复秘密图像 $\boldsymbol{S}$。

3 实验

为了测试所提出的图像信息隐藏方案的可行性与效果,完成了大量的实验。下面将以 256×256(像素)的 Airplane 作为覆盖图像,以 256×256 像素的 Lena 作为秘密图像的实验为例来说明。

3.1 混沌加密

以 256×256 像素的 Lena 作为秘密图像(图 5(a)),利用二维混沌映射对其像素值进行置乱,随机生成加密密钥 1:(1,32,16,4,4,64,64,4,2,32,32,1)。混沌 1 次的图像如图 5(b)所示,混沌 10 次的图像如图 5(c)所示。



(a) 原图(256×256像素)
(a) Secret image

(b) 混沌1次的Lena
(b) Image after applying the Baker map one time

(c) 混沌10次的Lena
(c) Image after applying the Baker map ten times

图 5　秘密图像、混沌 1 次的图像和混沌 10 次的图像

Fig. 5　Secret-image, images after applying the Baker map one and ten times

3.2　三角形加密

以 256×256 像素的 Airplane 作为覆盖图像 $\boldsymbol{C}$，以混沌 10 次的 256×256 像素的 Lena 作为秘密图像 $\boldsymbol{S}$。首先将它们分成 8×8 的块，其中某一个 8×8 块的像素值分别为

$$\boldsymbol{C}_i=\begin{pmatrix}126&124&124&126&128&130&130&126\\126&128&124&128&131&131&129&128\\126&126&126&128&129&131&129&129\\127&125&124&127&130&131&129&130\\126&126&124&128&132&130&129&130\\125&126&124&127&132&130&130&129\\126&126&124&127&130&131&129&130\\126&127&127&127&130&132&131&130\end{pmatrix};\boldsymbol{S}_i=\begin{pmatrix}133&133&154&107&105&126&28&124\\48&94&132&81&102&128&34&101\\159&85&19&102&133&147&95&121\\85&137&132&122&102&191&70&158\\60&33&147&25&91&46&119&63\\139&95&67&94&174&127&50&28\\180&83&133&103&144&119&119&69\\127&190&71&95&133&102&70&105\end{pmatrix}。$$

将秘密图像与覆盖图像相对应的块依次配对，块差异 $\boldsymbol{D}_i$ 为

$$\boldsymbol{D}_i=\begin{pmatrix}42.58&48.09&91.32&66.54&73.21&32.00&126.95&22.36\\116.50&86.88&45.26&99.11&82.20&27.88&124.44&78.63\\96.98&93.01&124.56&77.33&32.37&66.69&87.27&44.72\\94.36&56.07&45.26&35.29&80.60&139.00&108.36&89.80\\110.80&121.60&78.95&125.53&95.62&121.59&49.80&113.71\\60.80&82.77&104.34&85.40&113.37&27.77&120.00&125.92\\128.55&94.80&48.09&74.30&61.94&54.77&49.80&110.18\\15.91&141.32&105.30&84.29&28.09&83.79&110.73&76.65\end{pmatrix}。$$

再求出 $\boldsymbol{D}_i$ 的估计值 $\hat{d}\approx 81.907$，以及其标准差 $\hat{\sigma}_i\approx 88.897$，从而求出 $\boldsymbol{D}'_i$，即加密密钥 2：

$$\boldsymbol{D}'_i=\begin{pmatrix}-0.442&-0.380&0.106&-0.173&-0.098&-0.561&0.507&-0.670\\0.389&0.056&-0.412&0.194&0.003&-0.608&0.478&-0.037\\0.170&0.125&0.480&-0.051&-0.557&-0.171&0.060&-0.418\\0.140&-0.291&-0.412&-0.524&-0.015&0.642&0.298&0.089\\0.325&0.447&-0.033&0.491&0.154&0.446&-0.361&0.358\\-0.237&0.010&0.252&0.039&0.354&-0.609&0.429&0.459\\0.525&0.145&-0.380&-0.086&-0.225&-0.305&-0.361&0.318\\-0.742&0.668&0.263&0.027&-0.605&0.021&0.324&-0.059\end{pmatrix}。$$

将带有秘密图像块信息的 $\boldsymbol{D}'_i$ 嵌入到覆盖图像中，从而得到伪装图像。

3.3 图像还原

图像的解密过程基本上是隐藏过程的逆过程，将先前嵌入的信息提取出来获得秘密图像块，由所有的秘密图像块还原成完整的秘密图像，即混沌 10 次的秘密图像，然后施行混沌映射的逆运算，从而恢复原始的秘密图像。

3.4 实验结果

实验以 PSNR(peak signal to noise ratio，峰值信噪比)和实际嵌入秘密信息的伪装图的视觉效果评价秘密图像的隐藏效果。用 256×256 像素的 Boat 作为覆盖图像，用混沌 10 次的 256×256 像素的 Lena 作为秘密图像，实验结果分别如图 6～11 所示。

图 6 覆盖图像 Boat(256×256 像素)

Fig. 6 Cover image boat (256×256 pixels)

图 7 原秘密图像 Lena (256×256 像素)

Fig. 7 The original secret image Lena (256×256 pixels)

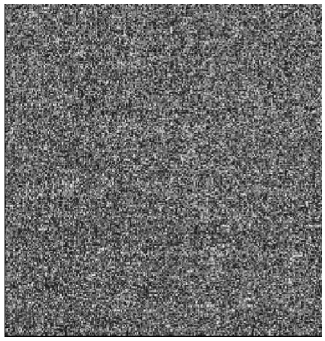


图 8 混沌 10 次的秘密图像 Lena(256×256 像素)

Fig. 8 The secret image after applying the Baker map ten times (256×256 pixels)

图 9 伪装图像 Boat(256×256 像素)

Fig. 9 Stego-image (256×256 pixels)

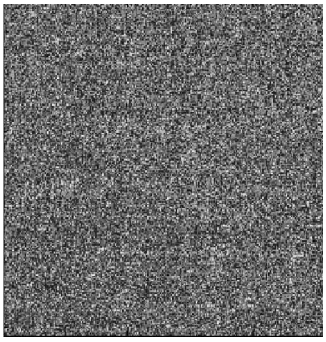


图 10 混沌秘密图像(由伪装图像提取出来的图像，256×256 像素)

Fig. 10 The secret image extracted from stego-image(256×256 pixels)

图 11 复原的秘密图像 Lena(256×256 像素)

Fig. 11 The secret image after restored(256×256 pixels)

实验中，分别将 256×256，512×256 和 512×512 像素的 Boat 作为覆盖图像，将 256×256 像素的 Lena 作为原始的秘密图像，得到的 PSNR 值如表 1。

由实验结果可知，随着覆盖图像的尺寸的增加，PSNR 值明显增大，伪装图像的质量明显增强。另外，大量实验结果表明，从视觉上看伪装图像和覆盖图像几乎一样，从而进一步增强了该方案信息隐藏的隐蔽性。

为了便于与其他隐藏方案的实验结果对比，本实验的测试图集选取国际上普遍应用的灰度图像，例如将两个 512×

表 1 PSNR 值

Tab. 1 The PSNR value

覆盖图像 (Boat)	秘密图像 (混沌 10 次的 Lena)	PSNR
256×256	256×256	48.20
512×256	256×256	50.89
512×512	256×256	53.90

512 像素的 Lena 和 Baboon 作为覆盖图像(图 12),将 3 个 512×256 像素的 Airplane,Scene 和 Tiff 作为原始的秘密图像(图 13),3 个混沌 10 次之后的图像(图 14)密码均为(2,32,32,16,32,4,4,64,128,64,4,2,16,32,16,32,16,16)。

分别利用文献[8-11]的方案和崔世宇[3]的维诺图(VD)方法,得到峰值信噪比实验结果如表 2 所示。与对照方法相比较,基于二维混沌图像的三角形隐藏方案在视觉质量上有明显优势。以用 512×512 像素的 Lena 作为覆盖图像为例:与文献[11]的方案(BD)相比,Airplane 作为秘密图像时,峰值信噪比提高了 12.45 dB,提高幅度达 30.22%;平均来看,峰值信噪比提高了 11.06 dB,提高幅度达 27.42%。与文献[3]相比,Airplane 作为秘密图像时峰值信噪比提高了 9.77 dB,提高幅度达 22.27%;平均来看,峰值信噪比提高了 7.89 dB,提高幅度达 18.12%。

(a) Lena (b) Baboon

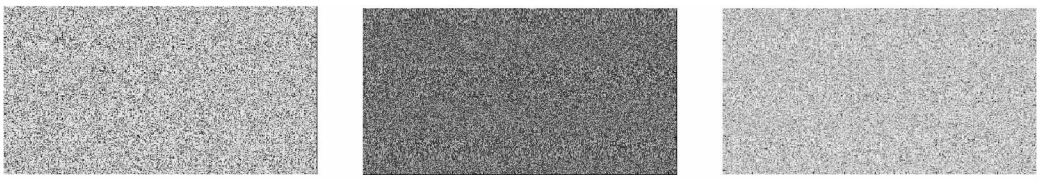
图 12 覆盖图像(512×512 像素)

Fig. 12 Cover-image (512×512 pixels)

(a) Airplane (b) Scene (c) Tiff

图 13 秘密图像(512×256 像素)

Fig. 13 Secret image (512×256 pixels)



(a) Airplane (b) Scene (c) Tiff

图 14 混沌 10 次的秘密图像(512×256 像素)

Fig. 14 The secret image after applying the Baker map ten times (512×256 pixels)

表 2 峰值信噪比实验结果对照表

Tab. 2 The experinental results of different moethod dB

cover image (512×512 像素)	secret image (512×256 像素)	LSB[8]	OLSB[9]	OPAP[10]	BD[11]	VD[3]	本文方法
Lena	Airplane	31.94	32.71	34.83	41.20	43.88	53.65
	Scene	32.06	32.55	34.79	40.35	43.62	51.10
	Tiff	31.28	32.90	34.84	41.46	43.75	50.94
Baboon	Airplane	32.02	32.79	34.79	39.62	43.21	50.83
	Scene	32.15	32.50	34.80	39.35	43.32	50.91
	Tiff	31.33	32.95	34.79	40.00	43.25	50.91

4 结束语

提出的基于二维混沌图像的三角形隐藏方案极大地提高了伪装图像的质量，提高了信息的隐蔽性，从而提高了安全性。在隐藏操作前对秘密数据进行置乱，用三角形算法实现图像信息隐藏和提取，进一步提高隐藏的安全性。方法综合了混沌加密和三角形加密算法的优点：具有更大的密钥空间且结构稳定；对图像的置乱速度快；加密密钥 D'_i 较小，嵌入时的信息较少；伪装图像与秘密图像相似度高，隐藏难于被察觉；双重加密不易破解。

参考文献：

[1]Shannon C E. Communication theory of secrecy systems[J]. Bell System Technical Journal,1949,28(4):656-715.

[2]余建德，宋瑞霞，齐东旭. 基于数字图像三角形剖分的信息伪装算法[J]. 计算机研究与发展，2009，46(9)：1432-1437.
Yu Jiande,Song Ruixia,Qi Dongxu. A scheme for steganography based on triangular partition of digital images[J]. Journal of Computer Research and Development,2009,46(9):1432-1437.

[3]崔世宇. 基于维诺图的图像信息隐藏法研究[D]. 大连：大连理工大学，2011：28-33.

[4]黄峰，冯勇，李娟. 一种基于构造三角形的可逆二维映射图像加密算法[J]. 光电子·激光，2009，20(3)：378-381.
Huang Feng,Feng Yong,Li Juan. An image encryption approach based on an invertible two-dimensional map by construction triangle[J]. Journal of Optoelectronics · Laser,2009,20(3):378-381.

[5]Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps[J]. International Journal of Bifurcation and Chaos,1998,8(6):1259-1284.

[6]张小华，刘芳，焦李成. 一种基于混沌序列的图像加密技术[J]. 中国图象图形学报，2003，8(4)：374-378.
Zhang Xiaohua,Liu Fang,Jiao Licheng. An image encryption arithmetic base on chaotic sequences[J]. Journal of Image and Graphics,2003,8(4):374-378.

[7]乌旭，陈尔东，胡家升. 一种基于混沌的图像加密改进方法[J]. 大连理工大学学报，2004，44(5)：754-757.
Wu Xu,Chen Erdong,Hu Jiasheng. An improved chaotic image encryption method[J]. Journal of Dalian University of Technology,2004,44(5):754-757.

[8]Wang R Z,Lin C F,Lin J C. Image hiding by optimal LSB substitution and genetic algorithm[J]. Pattern Recognition,2001,34(3):671-683.

[9]Chan C K,Cheng L M. Hiding data in images by simple LSB substitution[J]. Pattern Recognition,2004,37(3):469-474.

[10]Li S L,Leung K C,Cheng L M,et al. A novel image-hiding scheme based on block difference[J]. Pattern Recognition,2006,39(6):1168-1176.

[11]Wang H M,Qu L M,Wang F R. A triangular algorithm of image-hiding[C]//8th World Congress on Intelligent Control and Automation. Jinan,July 7-9,2010:1012-1016.

（责任编辑：吕文红）