

基于混沌和位运算的图像加密算法

刘乐鹏*, 张雪锋

(西安邮电大学 通信与信息工程学院, 西安 710061)

(*通信作者电子邮箱 liulepeng1986@126.com)

摘要: 为了有效改进图像加密效果及其安全性,在对基于混沌系统及位运算的图像加密算法进行研究的基础上,提出一种改进的数字图像加密算法,该算法首先采用 Logistic 映射产生混沌序列构造行、列置乱向量进行像素位置的置乱,再利用分段非线性 Logistic 产生的序列构造灰度置乱放大因子,对图像进行灰度置乱,且对两个过程进行迭代操作。该算法不仅密钥空间增大,灰度直方图更加均匀,而且像素相关性变弱,运算速度较传统算法更快。实验结果表明,改进算法具有良好的加密效果和安全性。

关键词: 混沌映射;图像加密;位置置乱;像素位;分段非线性映射

中图分类号: TP309.7 **文献标志码:** A

Image encryption algorithm based on chaos and bit operations

LIU Lepeng*, ZHANG Xuefeng

(School of Communication and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an Shaanxi 710061, China)

Abstract: In order to effectively improve the image encryption effect and safety, based on studying image encryption algorithm based on chaotic systems and bit operations, an improved algorithm of digital image encryption algorithm was proposed. Firstly, Logistic map was used to generate chaotic sequences, constructing row and column vector to scramble pixel position by the proposed algorithm. Secondly, another piecewise nonlinear Logistic sequence was applied to construct gray scale scrambling amplification factor to scramble the image gray scale, meanwhile the two processes were iteratively done. The mentioned algorithm made not only the key space increase and gray histogram uniform, but also the pixel correlation weaker and the operation speed faster than traditional algorithms. The experimental results show that the improved algorithm has good encryption efficacy and safety.

Key words: chaotic map; image encryption; position scrambling; pixel bit; piecewise nonlinear mapping

0 引言

随着网络 and 多媒体技术的发展和普及,关于图像等多媒体数据的安全问题日益引起人们的关注。由于数字图像具有冗余度高、数据量大、数据相关性强等特点,采用传统的加密方式进行加密将导致加密速度慢、实时性差等缺点。如何结合数字图像的特点设计有效的数字图像加密算法成为信息安全领域的一个研究热点。

混沌系统具有初值敏感性、非周期性、非收敛性、伪随机性等良好的密码学特性,是非线性确定系统由于内在随机性而产生的外在复杂表现,是一种貌似随机的非随机现象。混沌系统的这些特点使其被广泛应用于数据加密技术^[1-5]。当前,基于混沌的数字图像加密方式主要包括基于置乱的加密技术、基于灰度替换的加密技术和基于混合代结构的图像加密技术^[6-9]。其中基于像素位置置乱的加密算法虽然可以达到对图像加密的目的,但其安全性较差,无法满足实际需求。

由于仅通过像素位置置乱加密图像的加密方式存在可恢复周期等安全隐患,研究者进一步提出了将像素位置置乱和灰度替代相结合的加密方式,这种混合迭代结构的加密方式可以有效提高算法的保密性。

本文首先研究分析了基于混沌和位运算的图像加密算法^[10-17],在此基础上,进一步给出了一种改进的基于混沌和位运算的图像加密算法,改进算法结合具有可控放大因子的

像素灰度替代加密,能够取得更好的加密效果和安全性。

1 Logistic 映射及其特性

1.1 Logistic 混沌映射

Logistic 映射是一种典型的一维混沌系统,其公式定义如下:

$$x_{k+1} = \mu x_k (1 - x_k) \quad (1)$$

其中: μ 为分支参数, k 为迭代次数, $0 \leq \mu \leq 4$, $x_k \in (0, 1)$ 。当 $3.569 \leq \dots \leq \mu \leq 4$ 时,Logistic 映射处于混沌状态,此时对给定的不同初始条件 x_0 和 y_0 ,得到的序列 $\{x_k\}_{k=0}^{\infty}$ 和 $\{y_k\}_{k=0}^{\infty}$ 表现出非周期、非收敛、伪随机等混沌性质。

图 1 给出了当 $\mu = 3.5789$, $x_0 = 0.3333$, $y_0 = 0.5656$ 时,应用式(1)进行迭代计算得到序列的分布情况。实验结果表明,应用式(1)迭代计算得到的序列具有良好的非周期性、非收敛性以及初始条件的敏感性。

1.2 混沌的特性

Logistic 混沌具有遍历性、非周期性、长期不可预测性以及非收敛性等良好的混沌性质。应用 Logistic 映射产生序列的概率密度函数、混沌轨迹的平均值、序列的自相关系数和互相关系数有如下特点。

混沌系统产生序列的概率密度函数为:

$$\rho = \begin{cases} \frac{1}{\pi \sqrt{x(1-x)}}, & 0 < x < 1 \\ 0, & \text{其他} \end{cases} \quad (2)$$

收稿日期:2012-10-15;修回日期:2012-11-23。 基金项目:陕西省教育厅专项科研计划(09JK731, 2010JK820)。

作者简介:刘乐鹏(1986-),女,陕西咸阳人,硕士研究生,主要研究方向:通信安全与信息对抗; 张雪锋(1975-),男,陕西西安人,教授,主要研究方向:信息安全、数字图像保密。

混沌序列轨迹点的平均值为:

$$\bar{x} = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{k=0}^{N-1} x_k = \int_0^1 x p(x) dx = 0.5 \quad (3)$$

混沌序列的自相关系数为:

$$T(\tau) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{k=0}^{N-1} (x_k - \bar{x})(x_{k+\tau} - \bar{x}) = \int_0^1 x f^\tau(x) p(x) dx = 0 \quad (4)$$

混沌序列的互相关系数为:

$$C(\tau) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{k=0}^{N-1} (x_k - \bar{x})(y_{k+\tau} - \bar{y}) = 0 \quad (5)$$

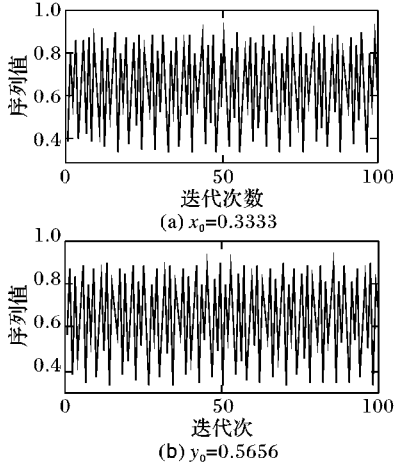


图1 混沌序列分布情况

1.3 基于混沌排序的图像加密

以对大小为 $M \times N$ 的图像进行置乱加密为例,设映射的初始条件为 μ, x_0 , 取正整数 t , 由式(1)生成混沌序列 $\{x_k\}_{k=0}^{\infty}$, 从其中第 $t+1$ 项开始, 取其中 T 项, 对取得的序列 $\{X_{t+1}, X_{t+2}, \dots, X_{t+T}\}$ 进行排序得到序列 $\{\bar{X}_{t+1}, \bar{X}_{t+2}, \dots, \bar{X}_{t+T}\}$, 计算序列 $\{\bar{X}_{t+1}, \bar{X}_{t+2}, \dots, \bar{X}_{t+T}\}$ 在原序列 $\{X_{t+1}, X_{t+2}, \dots, X_{t+T}\}$ 中的位置信息, 得到对应图像行坐标置乱操作的置乱向量 $TM = \{h_1, h_2, \dots, h_T\}$, 实现图像的行置乱。同理可以得到对图像进行列坐标置乱的置乱向量 TN , 实现对图像的列置乱。通过以上两个过程, 实现对图像的置乱加密。图2给出了应用以上方式进行图像置乱加密的实验结果。

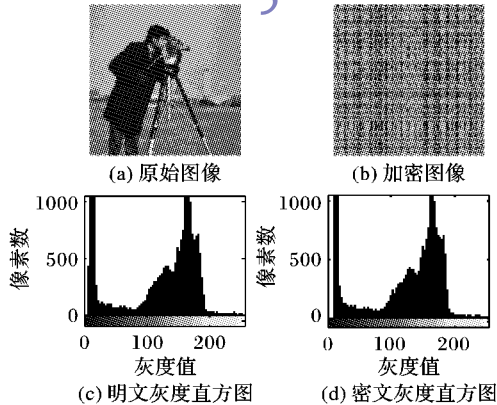


图2 置乱加密结果

图2的实验结果表明, 原始图像和密文图像的灰度直方图没有发生改变, 说明基于位置置乱的图像加密方式不改变图像的灰度统计信息, 这种特点将影响加密结果的安全性, 使得加密结果不能有效抵抗统计分析攻击。为此, 研究者提出了基于混沌和位运算的图像加密算法。

2 图像加密算法及改进算法

2.1 基于混沌和位运算图像加密算法

基于混沌和位运算的图像加密算法, 首先将像素值分解为 bit 位, $p(i, j)$ 表示原始图像的第 i 行, 第 j 列的像素值, $p^t(i, j)$ 表示 (i, j) 位置像素 $p(i, j)$ 分解的第 t 位 ($t = 0, \dots, 7$)。由式(6)将一幅灰度图像转换为由 0 和 1 组成的二值图像。

$$p^t(i, j) = \begin{cases} 1, & (p(i, j)/2^t) \bmod 2 = 1 \\ 0, & \text{其他} \end{cases} \quad (6)$$

式(7)可将二值图像恢复成灰度图像:

$$p(i, j) = \sum_{t=0}^7 2^t \times p^t(i, j) \quad (7)$$

以大小为 $M \times N$ 灰度图像为例, 由式(6)可转化成大小为 $M \times 8N$, 像素值由 0 和 1 组成的二值图像。

加密过程如下:

- 1) 首先读取一幅大小为 $M \times N$ 的灰度图像 A ;
- 2) 由式(6)将图像 A 转换为 $M \times 8N$ 的二值图像, 记为 B ;
- 3) 由式(1)产生混沌序列, 按照 1.3 节的方法, 构造行、列置乱向量, 置乱图像 B , 得图像 C ;
- 4) 用式(7)对图像 C 进行变换, 得大小为 $M \times N$ 的密文图像 D ;
- 5) 加密过程结束。

图3给出了应用以上方式进行图像置乱加密的实验结果。

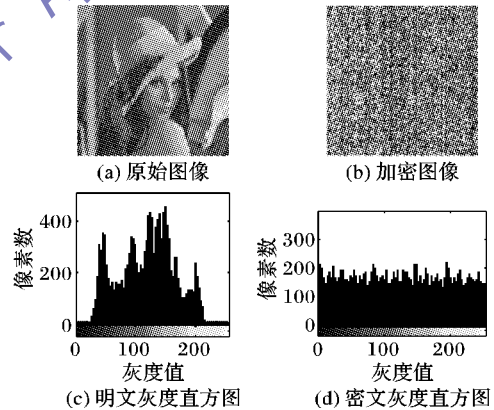


图3 置乱加密结果

图3实验结果表明, 基于混沌和位运算图像加密算法所得密文图像的灰度直方图均匀性较差, 加密效果较差, 无法保证图像的安全性。因此, 本文对该算法进行改进, 采用像素位置置乱和灰度替代混合迭代结构的加密方法, 取得了良好的加密效果。

2.2 改进算法及其分析

在 2.1 节加密算法的基础上, 结合灰度替代加密, 采用这种混合迭代结构的加密方式, 进行数字图像加密。式(8)用于第 k 轮灰度替代加密, 像素灰度替代操作 (S_k 是第 k 轮迭代后位置像素值) 如下:

$$S_{k+1} = \text{mod}((S_k + T(k) | i - j |), 256) \quad (8)$$

其中: $T(k)$ 是第 k 轮迭代所需放大因子, 可由分段 Logistic 映射产生。

分段 Logistic 映射定义为:

$$G(i+1) = \begin{cases} 4 \times u \times G(i) \times (0.5 - G(i)), & G(i) < 0.5 \\ 1 - 4 \times u \times (G(i) - 0.5) \times (1 - G(i)), & G(i) > 0.5 \end{cases} \quad (9)$$

$$T(k) = \text{Floor}(G(i) \times 10^3) \quad (10)$$

像素灰度替代加密,实现灰度的一次“拉伸折叠”,使得原来相邻的两个像素,即使灰度相同经过迭代,不但位置改变,灰度值也会发生很大变化。灰度值解密公式:

$$S_k = (S_{k+1} - T(k) |i - j|) \bmod 256 \quad (11)$$

加密过程如下:

- 1) 首先读取一幅大小为 $M \times N$ 的灰度图像 A ;
- 2) 由式(6)将图像 A 转换为 $M \times 8N$ 的二值图像,记为 B ;
- 3) 由式(1)产生混沌序列,按照 1.3 节的方法,构造行列置乱向量,置乱图像 B ,得到图像 C ;
- 4) 用式(7)对图像 C 进行变换,得大小为 $M \times N$ 的图像 D ;
- 5) 用式(8)对图像 D 进行像素灰度替代加密,得到图像 E ;
- 6) 对图像 E 重复 2) ~ 5) k 次输出密文图像(k 作为密钥)。
- 7) 加密过程结束。

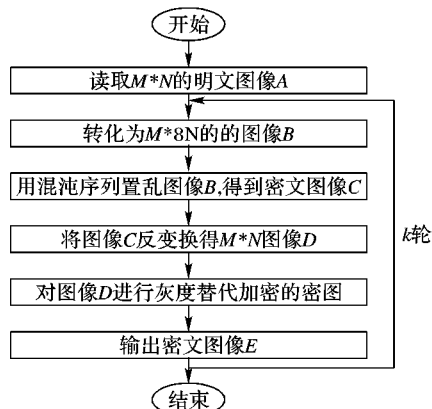


图4 加密流程

解密流程只需对加密过程实施相反的操作便可恢复原始图像。首先对密文图像按照式(8)进行灰度替代解密,然后将解密后的 $M \times N$ 的图像分解成 $M \times 8N$ 的二值图像,采用步骤3) 获取的混沌序列进行相反的操作,最后应用式(7) 得到 $M \times N$ 的图像,并迭代加密的次数,最后恢复出明文图像,具体实施过程见图5。

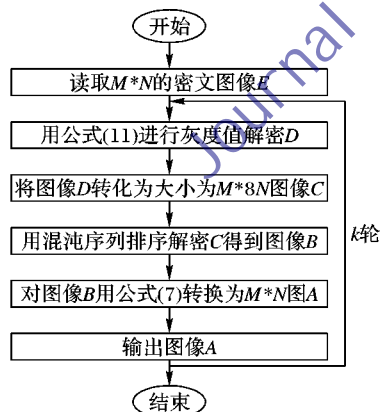


图5 解密流程

图6 给出应用以上加密算法和 2.1 节加密算法的实验对比结果。实验结果表明,与 2.1 节加密算法相比,改进算法的密文图像灰度直方图的均匀性得到很大改善,说明这种像素位置置乱和灰度替代混合迭代结构的加密方式,具有更高的安全性。

3 算法分析

3.1 密钥空间和敏感性分析

密钥空间是指算法所需密钥的总数。与 2.1 节加密算法

相比,本文的改进算法所需密钥数除 2.1 节算法所需密钥 x_0 , μ (不包括 m, n) 外,还包含获取灰度置乱放大因子所需密钥 μ_1 , 以及迭代次数 k , 因此密钥空间明显增大。图7 是大小为 256×256 的 Rice 图,位置置乱初始密钥 $\mu = 3.92$, $x_0 = 0.364$ ($m = 13, n = 27$),灰度置乱放大因子的初始密钥 $\mu_1 = 4$,其中图7(d) 是密钥 μ 变为 3.920000000001 的解密图像。图8 是大小为 500×500 的 original 图,位置置乱初始密钥 $\mu = 3.96$, $x_0 = 0.2008$ ($m = 20, n = 51$),灰度置乱放大因子的初始密钥 $\mu_1 = 4$,其中图8(d) 是获取灰度置乱放大因子所需密钥 μ_1 变化为 4.000000000001 的解密图像。图9 是大小为 512×512 的 Vase 图,采用与图7 相同的密钥初始条件,图9(d) 是仅将 x_0 变为 0.36400000000001 的解密图像。

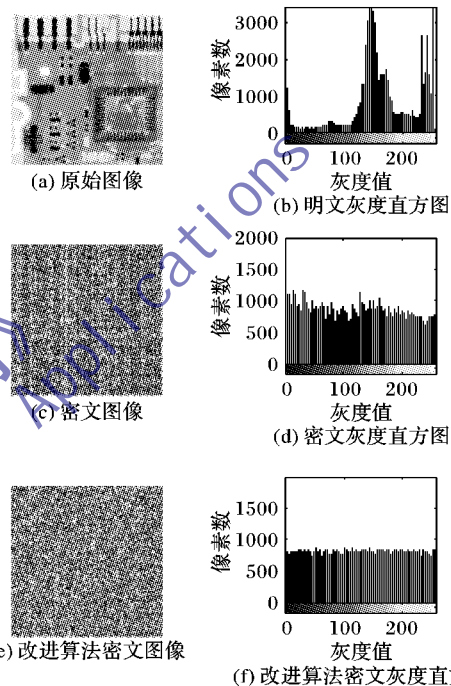


图6 对比加密结果

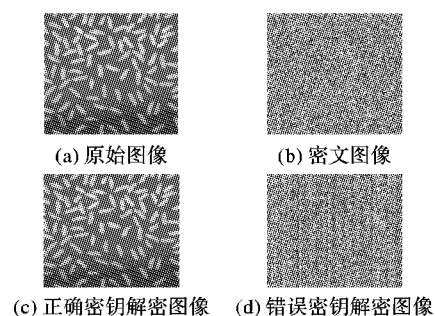


图7 密钥 μ 变化敏感性测试

图7~9 的实验结果表明,改进算法在密钥发生微小变化时,将影响图像成功解密,即改进算法对初始密钥具有较强的敏感特性。

3.2 速度

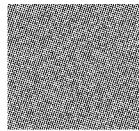
运算速度是衡量图像加密算法性能的一个重要方面,尤其是在实际的网络应用中。该部分使用不同大小为二维图像,分别对本文的改进算法与传统的置乱扩散加密算法及熟知的 DES (Data Encryption Standard) 算法进行比较,实验结果如表1。从表1 中可以看出,本文所给的改进算明显优于传统的置乱扩散以及经典的 DES 算法。因此该算法更适用于实时安全网络传输。同时加密速度相对于传输时间相对缩短。

表1 3种加密方法效率比较

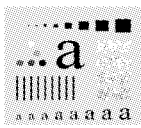
图像大小	灰度级	加密时间/s		
		本文算法	传统置乱扩散算法	DES 算法
200 × 200	256	20	25	32
256 × 256	256	24	30	43
512 × 512	256	70	92	168



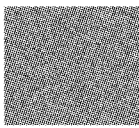
(a) 原始图像



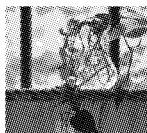
(b) 密文图像



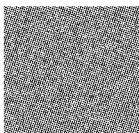
(c) 正确密钥解密图像



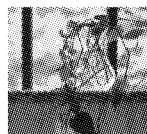
(d) 错误密钥解密图像

图8 密钥 μ_1 变化敏感性测试

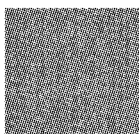
(a) 原始图像



(b) 密文图像



(c) 正确密钥解密图像



(d) 错误密钥解密图像

图9 密钥 x_0 变化敏感性测试

3.3 灰度差异度

图像相邻两个像素的灰度差异计算如下:

$$GN = \left(\sum [G(x, y) - G(x', y')]^2 \right) / 4 \quad (12)$$

其中: (x', y') 可能为 $(x-1, y)$, $(x+1, y)$, $(x, y-1)$, $(x, y+1)$ 其中之一; $G(x, y)$ 是位置 (x, y) 的灰度值。整幅图像平均相邻像素差异计算如下:

$$AN(GN(x, y)) = \frac{\sum_{x=2}^{M-1} \sum_{y=2}^{N-1} GN(x, y)}{(M-2)(N-2)} \quad (13)$$

$$GVN = \frac{AN'(GN(x, y)) - AN(GN(x, y))}{AN'(GN(x, y)) + AN(GN(x, y))} \quad (14)$$

其中: AN, AN' 分别为明文图像和密文图像平均相邻灰度差异。

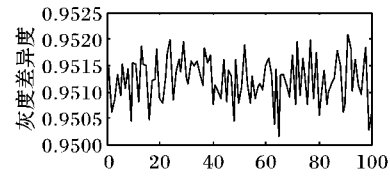
图10的实验结果表明,改进算法较原算法,灰度差异度更接近于1,加密效果更好。

3.4 直方图分析

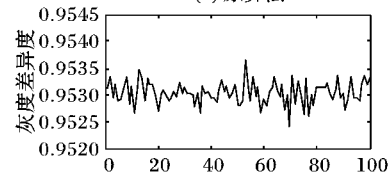
直方图是一幅图像像素有序分布的图表,反映了图像处理之后像素的分布。图11的实验结果表明,改进算法取得更加均匀的灰度分布,这一特点使得很难使用任何统计分析和差分解密密文图像,增强了图像信息的安全性。

3.5 相关性分析

式(15)分别应用于原始图像和密文图像,来检测其相邻两个像素的相关性。以一幅 Lena 图像为例,分别从垂直\水平和对角线方向随机选择1000对相邻的像素进行分析。表2的实验结果表明,改进算法所得密文,相邻像素的相关性分析几乎为0。

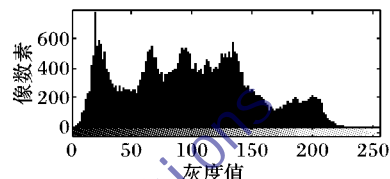


(a) 原算法

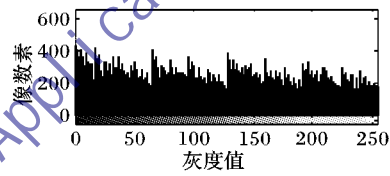


(b) 改进算法

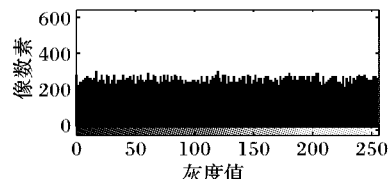
图10 灰度差异度测试



(a) 明文直方图



(b) 原算法直方图



(c) 改进原算法直方图

图11 直方图分析

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)D(y)}};$$

$$\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \quad (15)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2, E(x) = \frac{1}{N} \sum_{i=1}^N x_i$$

表2 相关性对比

方向	原始图像	原始算法	改进算法
水平	0.9355	0.0405	0.0053
竖直	0.9748	0.0934	0.0117
对角	0.9492	0.0823	-0.0504

4 结语

本文提出了一种改进的基于混沌和位运算图像加密算法。该算法在原算法的基础上,结合像素灰度替代加密。实验表明,该算法具有强大密钥空间、良好的灰度直方图、灰度差异度,具有更高的抗攻击能力,且可将该算法扩展到高维混沌映射,也可以应用于三维图像,加密后的密文图像可以直接用于互联网的安全传输。

(下转第1099页)

次匹配所需的时间,结果如表1所示。

由表1可知,二进制串描述符在计算时间与匹配时间上,有巨大的提升。描述符计算效率最高的是ORB,略高于映射法,只需0.018 ms。匹配速度最快的是本文提出的映射法,其速度是SIFT的100倍,这也是本描述符算法最大的优点。

表1 描述符计算时间与描述符匹配时间比较

描述符算法	类型	计算时间/ms	匹配时间/ms
SIFT	128 维浮点型	0.501	0.412
SURF	64 维浮点型	0.161	0.201
ORB	256 比特串	0.018	0.008
映射法	32 比特串	0.034	0.004

4 结语

针对SIFT、SURF等传统描述符算法计算速度慢、匹配时间长的缺点,本文提出了一种基于映射法的二进制串描述符,它在计算速度与匹配速度上有较大的优势,匹配速度达到SIFT算法的100倍。而且此算法生成的局部特征只有32比特,在存储空间与匹配速度上优于同类的ORB描述符,可以在需要大量匹配运算的领域得到有效应用,如大规模图像检索、实时视频识别等。

参考文献:

- [1] 陈方, 蒋云良, 许允喜. 改进的 CenSurE 特征和基于相加图像梯度的快速描述符[J]. 计算机应用, 2011, 31(7): 1818 - 1821.
- [2] RUBLEE E, GARAGE W, PARK M, *et al.* ORB: an efficient alternative to SIFT or SURF [C]// IEEE International Conference on Computer Vision. Barcelona: IEEE, 2011: 2564 - 2571.
- [3] BROWN M, GANG H, WINDER S. Discriminative learning of local image descriptors [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2011, 33(1): 43 - 57.
- [4] AMBAI M, YOSHIDA Y. CARD: Compact and real-time descriptors [C]// IEEE International Conference on Computer Vision. Barcelona: IEEE, 2011: 97 - 104.
- [5] CALONDER M, LEPETIT V, STRECHA C, *et al.* BRIEF: binary robust independent elementary features [J]. ECCV'10: Proceedings of the 11th European Conference on Computer Vision. Berlin: Springer-Verlag, 2010: 778 - 792.
- [6] YU GUOSHEN, MOREL J-M. A fully affine invariant image comparison method [C]// ICASSP09: Proceedings of the 2009 IEEE International Conference on Acoustics, Speech and Signal Processing. Washington, DC: IEEE computer Society: IEEE, 2009: 1597 - 1600.
- [7] BAY H, TUYTELAARS T, van GOOL L. SURF: speeded up robust features [J]. Computer Vision - ECCV 2006. Berlin: Springer-Verlag, 2006: 404 - 417.
- [8] YAN K, SUKTHANKAR R. PCA-SIFT: a more distinctive representation for local image descriptors [C]// Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. Washington, DC: IEEE, 2004, 2: 506 - 513.
- [9] LOWE D G. Distinctive image features from scale-invariant keypoints [J]. International Journal of Computer Vision, 2004, 60(2): 91 - 110.
- [10] ROSTEN E, DRUMMOND T. Machine learning for high-speed corner detection [C]// Computer Vision - ECCV 2006. Berlin: Springer-Verlag, 2006: 430 - 443.
- [11] ROSIN P L. Measuring corner properties [J]. Computer Vision and Image Understanding, 1999, 73(2): 291 - 307.
- [12] Learning local image descriptors data [EB/OL]. [2012 - 11 - 28]. <http://www.cs.ubc.ca/~mbrown/patchdata/patchdata.html>.
- [13] MIKOLAJCZYK K, SCHMID C. A performance evaluation of local descriptors [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2005, 27(10): 1615 - 1630.
- [14] Robotics research group, university of Oxford. Affine covariant features [EB/OL]. [2012 - 11 - 28]. <http://www.robots.ox.ac.uk/~vgg/research/affine/>.

(上接第1073页)

参考文献:

- [1] 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.
- [2] 李晓轩, 王阿川. 一种基于混沌排序的数字图像置乱算法[J]. 黑龙江科技信息, 2009(27): 54 - 54.
- [3] 赵学峰. 基于面包师变换的数字图像置乱[J]. 西北师范大学学报: 自然科学版, 2003, 39(2): 26 - 29.
- [4] 顾勤龙, 姚明. 基于 Logistic 混沌序列的数字图像加密研究[J]. 计算机工程与应用, 2003, 23(3): 114 - 116.
- [5] 郭建胜, 金晨辉. 对基于广义猫映射的一个图像加密系统的已知图像攻击[J]. 通信学报, 2005, 26(2): 131 - 135.
- [6] 曹建秋, 肖华荣. 像素位置与像素值双重置换的混沌加密算法[J]. Computer Engineering and Applications, 2010, 46(28): 192 - 195.
- [7] WANG Y, WONG K W. A chaos-based image encryption algorithm with variable control parameters [J]. Chaos, Solitons & Fractals, 2009, 41(4): 1773 - 1783.
- [8] 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): 136 - 139.
- [9] 张健, 于晓洋, 任洪娥. 基于 Cat 映射和 Lu 混沌映射的图像加密方案[J]. 电子器件, 2007, 30(1): 155 - 157.
- [10] FU CONG, LIN BINBIN, MIAO YUSHENG, *et al.* A novel chaos-based bit-level permutation scheme for digital image encryption[J]. Optics Communications, 2011, 284(23): 5415 - 5423.
- [11] YE G D. Image scrambling encryption algorithm of pixel bit based on chaos map[J]. Pattern Recognition Letters, 2010, 31(5): 347 - 354.
- [12] ZHU Z L, ZHANG W, WONG K W, *et al.* A chaos-based symmetric image encryption scheme using a bit-level permutation[J]. Information Sciences: an International Journal, 2011, 181(6): 1171 - 1186.
- [13] 张雪峰, 范九伦. 基于位运算的数字图像隐藏技术[J]. 信息安全与通信保密, 2007(5): 149 - 150.
- [14] 许艳. 基于位运算的 BMP 图像加密算法研究[J]. 湖南理工学院学报, 2007, 20(4): 41 - 43.
- [15] 袁玲, 康宝生. 基于 Logistic 混沌序列和位换的图像置乱算法[J]. 计算机应用, 2009, 29(10): 2681 - 2683.
- [16] 李涛, 柳健. 基于位平面与混沌系统的图像置乱方法[J]. 西南民族大学学报: 自然科学版, 2009, 34(3): 595 - 599.
- [17] 单佳佳, 朱灿焰. 基于位运算的图像加密技术的研究[J]. 电脑知识与技术, 2007(5): 804 - 805.