基于矩阵变换的彩色图像加密算法

王 旻[1],王方超[2]
(1.海军航空工程学院 研究生5队,山东 烟台 264001;
2.重庆通信学院 图像通信实验室,重庆 400035)

摘 要:研究了矩阵变换的性质,找到一种新的SCAN遍历矩阵,对彩色图像各分量进行像素位置置乱,结合彩色图像结构特点,利用彩色图像每个像素的RGB分量构成三维列向量,并将其作为输入分量,经过矩阵变换,改变其像素值的大小,得到加密矩阵。试验结果表明,加密图像具有类随机性,直方图接近于均匀分布,算法具有很强的密钥敏感性。

关键词: 图像加密;矩阵变换;SCAN语言;位置置乱;像素改变
中图分类号:TG156 文献标识码:A

A color image encryption algorithm based on matrix transformation

WANG Min[1], WANG Fang Chao[2]
(1. Graduate Student Company 5, Naval Aeronautical Engineering Academy, Yantai 264001, China;
2. Image Communication Lab, Chongqing Communication Institute, Chongqing 400035, China)

Abstract: In this paper, some characters about matrix transformation are studied. A new SCAN ergodic matrix is obtained to scramble the RGB segments of the color image. According to the structure of the color image, we proposed a new method to change the value of the pixel through matrix transformation. The input vector of the transformation function is composed by the RGB values of the color image pixels. We took a third-order matrix which was got by a new way to change the input vector and then we got the output vector which was the encoded pixel. The experimental results demonstrate that the suggested encryption algorithm of color image has the advantages of large key space and sensitivity to the secret keys. It is also useful to resist brute-force attacks and statistical attacks.

Key words: image encryption; matrix transformation; SCAN language; pixel scrambling; pixel confusion

随着计算机和网络技术的发展,数字信息技术得到了普遍的发展,与人们的日常生活和工作产生了密不可分的联系。随着数字信息交互的不断扩大,个人信息和公众信息在公共网络上的传输安全问题成了人们关注的焦点。图像作为信息的重要传播载体,其安全性就成为一个十分重要的研究内容。

对于图像信息安全,由于图像数据的信息量大,而且传统的信息安全领域一些加密方法比如DES、IDEA和RSA等的加密速度慢,因此不适用于图像数据的加密[1],需要寻找适合图像加密的专门算法。近年来,随着图像处理技术的发展,人们在此领域已经取得了一系列丰硕的研究成果,常用的图像加密思想主要有三种:对图像像素位置的置乱、对图像像素灰度值的改变以及两者的结合使用。其中,图像像素位置的置乱是一类十分重要的加密方法,用于将图像扰乱,消除像素的相关性,使人们无法通过视觉或计算机系统来发现图像的真正含义。目前提出的图像像素的置乱方法有Arnold变换[2]、Fibonacci-Q变换[3]、亚放射变换[4]、骑士巡游变换[5]、魔方变换[6]、幻方变换[7]、Hilbert曲线[8]、Tangram算法[9]、IFS模型[9]和Gray码[10]以及SCAN语言加密[11]等。其中,以Arnold变换和Fibonacci-Q变换为代表的矩阵变换加密应用十分广泛。虽然Arnold变换和Fibonacci-Q变换用于图像加密易于实现,方法简单,但是由于其变换矩阵固定,因此恢复方式都是周期的,这对于加密图像的安全性来讲存在很大的隐患。此外,普通矩阵变换加密,只是置乱了图像像素的位置,没有改变图像的直方图,很难抵御攻击者的统计分析攻击。

本文结合彩色图像的特点,利用每个像素的R、G、B 3

个分量组成 1 个三维向量,利用 1 个非固定三维变换矩阵对其进行像素值的改变,得到加密图像。在进行矩阵变换之前,先用一种新的 SCAN 遍历矩阵对图像进行一次像素的位置置乱,降低各像素之间的相关性。试验结果显示,通过这种方法得到的加密图像不仅直观上是随机噪声图像,直方图也接近于均匀分布,并且密钥量大,密钥敏感性强。

1 彩色图像加密原理

1.1 矩阵变换原理

基于矩阵变换的图像加密可以用以下公式表示:

$$\boldsymbol{C}=EK(\boldsymbol{P})=\boldsymbol{KP} \mod N \tag{1}$$

同样,解密过程可以表示为:

$$\boldsymbol{P}=DK(\boldsymbol{C})=\boldsymbol{K}^{-1}\boldsymbol{C} \mod N \tag{2}$$

当 $\boldsymbol{C}$ 和 $\boldsymbol{P}$ 分别代表原始图像和加密后图像的二维位置坐标向量时,式(1)和式(2)表示对图像进行位置置乱,N 为大于零的整数时,表示用于正方形图像置乱,即二维等长图像置乱;N 为二维列矢量时可以表示二维非等长图像置乱[12]。

无论是二维等长图像置乱还是二维非等长图像置乱,都是对图像像素的位置进行置乱,式(1)和式(2)中 $\boldsymbol{C}$ 和 $\boldsymbol{P}$ 均为像素的位置坐标向量。如果使 $\boldsymbol{C}$ 和 $\boldsymbol{P}$ 表示彩色图像 3 个分量 RGB 的像素值组成的向量时,式(1)和式(2)可以用来表示对彩色图像进行灰度混乱,即改变图像的灰度值。

对于彩色图像灰度值混乱加密,$\boldsymbol{C}=\vec{y}=(y_1,y_2,y_3)^{\mathrm{T}}$ 和 $\boldsymbol{P}=\vec{x}=(x_1,x_2,x_3)^{\mathrm{T}}$ 都为三维列向量,在式(1)中,$P=\vec{x}=(x_1,x_2,x_3)^{\mathrm{T}}$ 为由原始彩色图像像素的 3 个分量 RGB 的值构成的三维列向量,其中,x_1,x_2,x_3 分别为同一像素在 RGB 分量中的相应取值;$\boldsymbol{C}=\vec{y}=(y_1,y_2,y_3)^{\mathrm{T}}$ 为矩阵变换后,即加密后的像素值。在式(2)中 $\boldsymbol{C}$ 表示加密后图像的像素值构成向量,$\boldsymbol{P}$ 表示解密图像的像素值构成向量。加密矩阵 $\boldsymbol{K}=\boldsymbol{A}_{3\times3}$ 为三阶方阵,此时 N 为非零整数,因此图像加密和解密过程可以写为:

$$\vec{y}=A_{3\times3}\vec{x} \mod N \tag{3}$$

和

$$\vec{x}=A_{3\times3}^{-1}\vec{y} \mod N \tag{4}$$

其中,$\boldsymbol{A}_{3\times3}^{-1}$ 是加密矩阵 $\boldsymbol{A}_{3\times3}$ 的模 N 逆矩阵,因为是对像素值进行混乱,图像的灰度级为 256,所以 $N=256$。式(3)和式(4)能够用于图像像素值混乱,必须满足以下条件:

条件 1 输入向量 $\vec{x}$ 的元素取值于整数域 $\{(x_1,x_2,x_3):0\leqslant x_1,x_2,x_3\leqslant255\}$;

条件 2 变换是整数域 $\{(x_1,x_2,x_3):0\leqslant x_1,x_2,x_3\leqslant255\}$ 到其自身的一一映射;

条件 3 变换的模 N 逆变换存在,且也是整数域 $\{(x_1,x_2,x_3):0\leqslant x_1,x_2,x_3\leqslant255\}$ 到其自身的一一映射。

定义 1 假设存在矩阵 $\boldsymbol{B}$,使得 $\boldsymbol{AB}=\boldsymbol{I} \mod N$,其中,$\boldsymbol{I}$ 为单位矩阵。则称 $\boldsymbol{B}$ 为矩阵 $\boldsymbol{A}$ 的模 N 可逆矩阵。

因为 $\vec{x}$ 各分量为像素值,条件 1 满足;当变换矩阵 $\boldsymbol{A}_{3\times3}$ 定义在整数域 $\mathbf{Z}$ 即 $\{\boldsymbol{A}(i,j)\in\mathbf{Z}:1\leqslant i\leqslant3;1\leqslant j\leqslant3\}$ 并且满足 $(|\boldsymbol{A}|,N)=1$ 时,变换是整数域到整数域的一一映射,并且其模 N 逆存在[13],条件 2 和条件 3 也满足。

为了保证 $(|\boldsymbol{A}|,N)=1$ 成立,由参考文献[14]可以得到变换矩阵 $\boldsymbol{A}$ 的构建公式:$\boldsymbol{A}=\boldsymbol{LDUW}$。其中 $\boldsymbol{L}$、$\boldsymbol{U}$ 和 $\boldsymbol{D}$ 分别为定义在整数域 $\mathbf{Z}$ 上的三阶单位下三角矩阵、单位上三角矩阵和对角阵,且满足 $\boldsymbol{L}(i,j)\neq0,i>j;\boldsymbol{U}(i,j)\neq0,i<j;|\boldsymbol{D}|$ 为奇数。矩阵 $\boldsymbol{W}$ 是为了避免变换矩阵 $\boldsymbol{A}$ 的第一个元素 $\boldsymbol{A}(1,1)$ 在 $|\boldsymbol{A}|=1$ 时始终为 1 而增加的附加阵,而 $\boldsymbol{A}(1,1)$ 始终为 1 时,算法的安全性显然不能令人满意[14]。

由 $\boldsymbol{A}=\boldsymbol{LDUW}$ 知,本算法的密钥是由构建矩阵的 $\boldsymbol{A}_{3\times3}$ 矩阵 $\boldsymbol{L}_{3\times3}$、$\boldsymbol{D}_{3\times3}$、$\boldsymbol{U}_{3\times3}$ 和 $\boldsymbol{W}_{3\times3}$ 组成,其结构如下:

$$\boldsymbol{L}=\begin{pmatrix}1&0&0\\b_{21}&1&0\\b_{31}&b_{32}&1\end{pmatrix};\boldsymbol{U}=\begin{pmatrix}1&c_{12}&c_{13}\\0&1&c_{23}\\b_{31}&b_{32}&1\end{pmatrix};\boldsymbol{W}=\begin{pmatrix}1&0&0\\w&1&0\\0&0&1\end{pmatrix};$$

$$\boldsymbol{D}=diag(d_1,d_2,d_3)$$

并且,$|\boldsymbol{A}|=|\boldsymbol{D}|=d_1\times d_2\times d_3$,其中,$b_{21}$、$b_{31}$、$b_{32}$、$c_{12}$、$c_{13}$、$c_{23}$、$w$、$d_1$、$d_2$、$d_3$ 为非零整数,不取 0 作为密钥是为了排除弱密钥的一些情况出现。具体的分析参考文献[14]。

1.2 SCAN 语言置乱

从式(3)可以看到,当图像的某片区域像素值都相等时,如背景单一的图像,由变换的一一映射性质可以知道,变换后这些区域的像素值还会相等,虽然不再是原始图像的像素值,但明显存在安全隐患。这对图像加密来讲显然是一个缺陷。为了克服这个问题,在进行灰度置乱之前对图像进行一次位置置乱。

本文进行位置置乱使用一种新的 SCAN 遍历矩阵。SCAN 是一种扫描次序,即将矩阵中的每个元素访问一次且仅一次。

首先按照下面定义 2 产生两种 SCAN 遍历矩阵,然后利用 SCAN 矩阵对彩色图像的 R、G、B 分量进行像素位置的置乱[11]。

定义 2 假设给定彩色图像的 R、G、B 3 个分量中相关性最小的分量[15]记为 A,则进行奇异值分解(SVD)$A=U\times S\times V'$,对 U 分量和 V 分量进行由上至下、由左到右的大小排序,排列序号即构成 SCAN 矩阵。

对图像进行像素位置置乱的目的是为了消除像素之间的相关性,因此,利用彩色图像 R、G、B 三个分量当中的相关性最小的分量进行奇异值分解并生成两种 SCAN 遍历矩阵,分别对彩色图像其他 2 个分量进行位置置乱。

置乱后的图像不会再有大面积的相邻像素值相等区域,即图像像素相关性降低。因此,接着利用矩阵变换进行灰度值混乱得到图像各分量灰度值分布十分均匀,

原始图像变为伪随机噪声图像。

2 加密流程

加密过程分为图像位置置乱和像素值混乱2个阶段,其具体步骤如下:

(1) 根据参考文献[15]中提到的计算图像像素相关性的公式,计算彩色图像3个分量R、G、B的各自相关性的大小,分别设为$r1$,$r2$,$r3$;

(2) 将$r1$、$r2$和$r3$中值较小的一个对应的分量作为奇异值分解(SVD)的对象,按照定义2给定的方法得到两种SCAN遍历矩阵,即2个置乱矩阵$\boldsymbol{S}1$和$\boldsymbol{S}2$;

(3) 利用$\boldsymbol{S}1$和$\boldsymbol{S}2$对未进行奇异值分解的另两个分量进行像素值的置乱,得到彩色图像3个预处理分量$R1$、$G1$和$B1$;

(4) 随机选取7个整数值作为矩阵$\boldsymbol{L}$、$\boldsymbol{U}$和$\boldsymbol{W}$的参数,其中$\boldsymbol{L}$和$\boldsymbol{U}$分别有3个参数,$\boldsymbol{W}$有1个参数,根据($|\boldsymbol{A}|$,N=1)(N=256)选取$|\boldsymbol{A}|$的大小,即选$|\boldsymbol{A}|$为某一奇数即可,根据$|\boldsymbol{A}|=|\boldsymbol{D}|=d_1\times d_2\times d_3$,确定对角阵$\boldsymbol{D}$的参数$d_1$、$d_2$、$d_3$,利用公式$\boldsymbol{A}=\boldsymbol{LDUW}$构造出变换矩阵$\boldsymbol{A}$;

(5) 从(3)得到的3个图像分量的左上角分别取出第一个点的像素值组成输入向量$\vec{x}=(R1(1,1),G1(1,1),B1(1,))$,其中{$R1(1,1)$, $G1(1,1)$, $B1(1,1)$}分别表示3个图像分量像素值的大小,利用公式$\vec{y}=\boldsymbol{A}_{3\times3}\vec{x} \bmod 256$对其进行变换得到像素混乱后的输出向量$\vec{y}$;

(6) 按照从右至左、从上往下的顺序依次从3个图像分量中取出像素值组成输入向量,重复(5)的混乱过程,直到所有像素值都被混乱,得到混乱后的3个图像分量$R2$、$G2$和$B2$,即得到加密后的图像。

算法的解密过程是加密的逆过程,用到的公式为$\vec{x}=\boldsymbol{A}_{3\times3}^{-1}\vec{y} \bmod 256$,其中解密矩阵是加密过程矩阵的模$N$逆矩阵。模$N$逆矩阵的求法利用了参考文献[13]提出的算法,$\boldsymbol{A}_N^{-1}=\boldsymbol{A}_{N\times N}^{*}|\boldsymbol{A}|_N^{-1}$,其中$\boldsymbol{A}_N^{*}$是其对应伴随矩阵$\boldsymbol{A}^{*}$的$G_N$规格化,$|\boldsymbol{A}|_N^{-1}$为方阵$\boldsymbol{A}$所对应的行列式$|\boldsymbol{A}|$在模$N$下的乘法逆元,具体的一些概念和算法参见参考文献[13]。

3 实验结果及安全性分析

3.1 实验结果分析

为了验证以上算法的加密效果,在DuoT2450 PC上采用Matlab7.1平台对其进行了仿真实验。

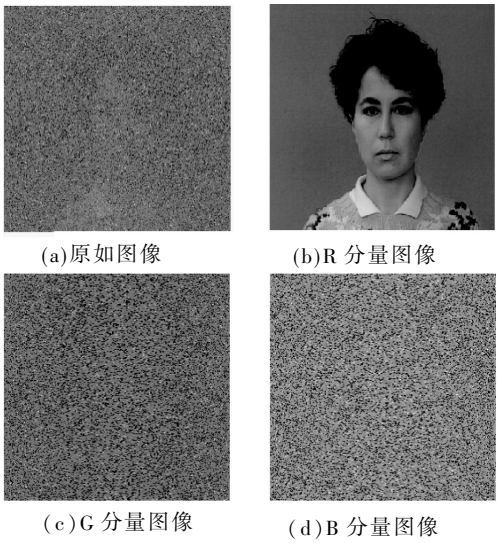
实验中使用了256×256的彩色图像(如图1所示,依次为原始图像及其RGB分量)。第一步,位置置乱,降低各像素点之间的相关性,得到的图像如图2所示(依次为原始图像及其RGB分量)。图3是原始图像位置置乱前后的直方图,从左至右依次为RGB分量。由图2和图3可以看出,只进行位置置乱的视觉效果和直方图均衡性都不能令人满意。图4是经过本文算法加密后的彩色图像及其RGB各分量,类似于随机噪声图像。图5是密钥发生微小变化,即b_{32}的值加1后的解密图像,可以看出,几乎没有得到原始图像的任何信息。图6(a)是图4各分量的直方图,可以看出,矩阵加密后的直方图已经接近于均匀分布,具有很好的抗统计攻击能力。图6(b)是错误解密时对应的其R、G、B分量的直方图,无法得到原始图像直方图的任何信息。图7是输入正确密钥解密得到的图像。

3.2 算法安全性分析

在密钥量方面,本文所用算法具有10个参数,取值也都是非零整数域。相比Arnold变换只有4个参数[2],该算法密钥量方面还是占很大的优势,并且10个参数的取值范围都是非零整数域,因此可以有效地抵御穷举攻击。由图6(a)可以看出,加密后图像各分量的直方图接近于均匀分布,这有利于抗统计攻击。图5是密钥b_{32}的值加1后的错误解密出的图像,图6(b)是其对应的直方图,可以看出,该算法的密钥敏感度比较高,密钥的微

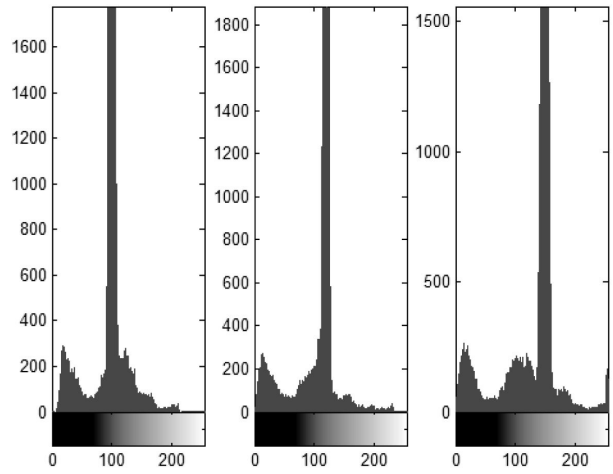
(a)原如彩色图像 (b)R分量图像 (c)G分量图像 (d)B分量图像

图1 原始彩色图像和RGB各分量图像

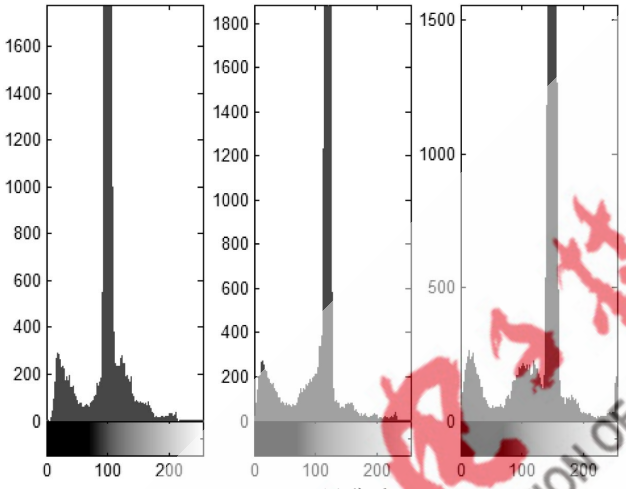


(a)原如图像 (b)R分量图像 (c)G分量图像 (d)B分量图像

图2 位置置乱后图像和其RGB各分量图像

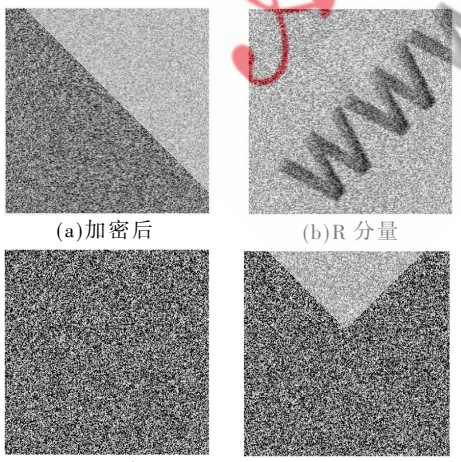


(a)置乱前



(b)置乱后

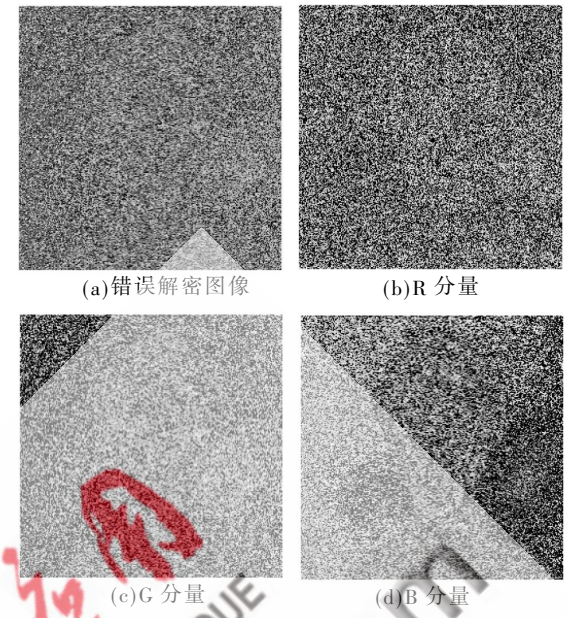
图 3 原始彩色图像各分量直方图和位置置乱后彩色图像各分量直方图



(a)加密后 (b)R 分量

(c)G 分量 (d)B 分量

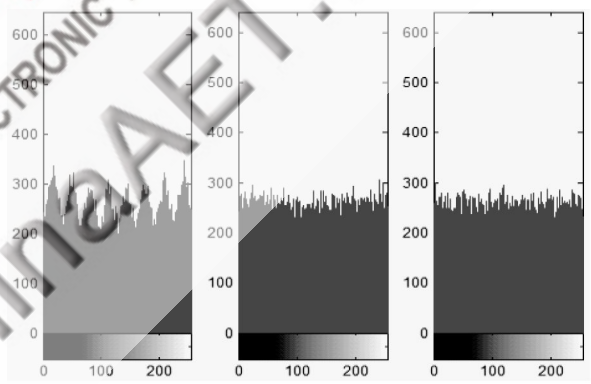
图 4 像素加密后图像和其 RGB 各分量图像



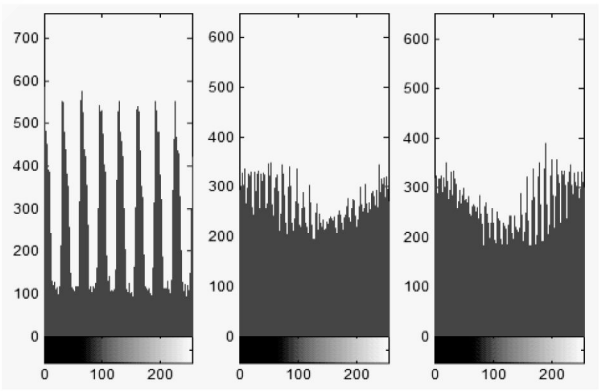
(a)错误解密图像 (b)R 分量

(c)G 分量 (d)B 分量

图 5 错误解密图像和其 RGB 各分量图像



(a)加密后的图像各分量的直方图



(b)错误解密后的图像各分量直方图

图 6 加密后的图像各分量的直方图和错误解密后图像各分量直方图

图 7 正确解密后图像

小变换可以导致解密图像的巨大差异。

本文结合彩色图像具有 RGB 3 个分量的结构特点，提出首先利用 RGB 3 个分量中相关性小的分量进行奇异值分解得到 2 个 SCAN 遍历矩阵，根据遍历矩阵对另外 2 个分量进行像素位置置乱，然后对预处理后的彩色图像进行矩阵变换，对图像的像素值进行改变，得到加密图像。实验结果表明，加密后的图像具有类随机性，直方图分布比较均匀，并且算法对于密钥具有很高的敏感性。

参考文献

[1] KWOK H S，WALLACE K S Tang. A fast image encryption system based on chaotic maps with finite precision representation [J]. Chaos, Solitons & Fractals，2007:1518-1529.

[2] 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):338-341.

[3] ZOU Jian Cheng, QI Dong Xu, WARD R K. A novel watermarking method based on Fibonacci numbers[A]. International Conference on Virtual Reality Continuum and Its Applications [C]. Hongkong, China, 2006:335-338.

[4] 柏森,曹长修.亚仿射变换的性质及其应用[J].计算机辅助设计与图形学学报,2003,15(2):205-208.

[5] 柏森,曹长修.一种新的数字图象置乱隐藏算法[J].计算机工程,2001,27(11):18-19.

[6] SHEN Jian Bing, JIN Xiao Gang, ZHOU Chuan. A color image encryption algorithm based on Magic cube transformation and modular arithmetic operation [A]. 6th Pacific Rim Conference on Multimedia[C]. Jeju Island, Korea,2005:270-280.

[7] 王冬梅.奇数阶幻方变换数字图像的准周期[J].浙江工业大学学报,2005,33(3):292-294.

[8] 林雪辉,蔡利栋.基于 Hilbert 曲线的数字图像置乱方法研究[J].中国体视学与图像分析,2004,9(4):224-227.

[9] 齐东旭.矩阵变换及其在图像信息隐藏中的应用研究[J].北方工业大学学报,1999,11(1):24-28.

[10] 邹建成,李国富.广义 Gray 码及其在数字图像置乱中的应用[J].高校应用数学学报(A 辑),2002,17 (3):363-370.

[11] MANICCAM S S, BOURBAKIS N G .Losslessimagecompression and encryption using SCAN [J]. Pattern Recognition,2001:1229-1245.

[12] 邵利平,覃征,高洪江,等.二维非等长图像置乱变换[J].电子学报,2007,35(7):1290-1294.

[13] 邵利平,覃征,衡星辰,等.基于矩阵变换的图像置乱逆问题求解[J].电子学报,2008,36(7):1355-1363.

[14] WANG Fang Chao, BAI Sen, ZHU Gui Bin, et al. An image encryption algorithm based on affine transformation in N-dimension. IEEE computer society, 2009:579-585.

[15] GAO Tie Gang, CHEN Zeng Qiang. A new image encryption algorithm based on hyper-chaos [J]. Physics Letters A,2008 (372):394-400.

(收稿日期:2009-10-21)

作者简介:

王旻,女,1985 年生,硕士研究生,主要研究方向:信息安全、军事训练安全管理;

王方超,男,1984 年生,硕士研究生,主要研究方向:数字图像处理、信息安全及网络通信。

宏基新款 DisplayPlus 显示器选配飞思卡尔 IC
飞思卡尔将在国际消费电子展(CES)上演示宏基智能显示器

2010 年 1 月 7 日,美国内华达州拉斯维加斯 (2010 国际消费电子展) ——随着互联网连接扩展到传统的计算平台之外,宏基(Acer)公司设计出一款激动人心的新产品。它采用了来自于飞思卡尔半导体的处理、电源管理和模拟技术。

宏基即将推出一款名为 DisplayPlus D241H 的 24 英寸智能显示器,它包含飞思卡尔高性能的、功能丰富的 i.MX515 应用处理器,支持微件应用和多媒体播放。该显示器还集成了飞思卡尔的 MC13892 电源管理 IC 以及 SGTL5000 音频编解码器。

宏基计划于 2010 年第一季度正式推出这款智能显示器。新推出的产品把 CPU 直接集成到显示器内部,与传统的 PC 和显示器配置相比,它节省了宝贵的桌面空间。

"宏基最新的智能显示器是一款创新产品,展示了飞思卡尔面向消费市场提供的产品组合的广度和深度。"

(飞思卡尔半导体供稿)