

基于三维亚仿射变换的数字图像置乱技术

邹玮刚^{1*}, 陈沛云², 黄江燕¹

(1. 江西理工大学 理学院, 江西 赣州 341000 2. 江西理工大学 建筑与测绘工程学院, 江西 赣州 341000)

(* 通信作者电子邮箱 weigangzou@yahoo.com.cn)

摘要:为了提高数字图像信息隐藏的安全性和灵活性,利用亚仿射变换的原理设计了一种新的基于三维亚仿射变换的图像加密算法。该算法通过分析三维亚仿射变换的约束条件,根据变量之间的联系和随机性,给出了一种三维亚仿射变换的快速构造方法。在色彩空间中对每个像素点的三个色彩分量选择不同的方式进行变换,达到图像置乱的效果;对其周期性进行了研究,并提出了奇异点与伪周期的概念。经实验验证,该算法置乱效果良好,具有密钥空间较大、加密灵活、扩散性和扰乱性比较理想、安全性较高的优点。

关键词:信息安全; 数字图像置乱; 三维亚仿射变换; 周期性; 奇异点

中图分类号:TP391 **文献标志码:**A

Digital image scrambling technology based on three dimensional sub-affine transformation

ZOU Wei-gang^{1*}, CHEN Pei-yun², HUANG Jiang-yan¹

(1. School of Science, Jiangxi University of Science and Technology, Ganzhou Jiangxi 341000, China;

2. School of Architectural and Surveying and Mapping Engineering, Jiangxi University of Science and Technology, Ganzhou Jiangxi 341000, China)

Abstract: In order to improve the security and flexibility of digital image information hiding, adopting the theory of sub-affine transformation, a new image encryption algorithm based on three dimensional sub-affine transformation was designed. By analyzing the constraints of three dimensional sub-affine transformation, according to the relation between variables and randomness of variables, a rapid construction method of three dimensional sub-affine transformation was given. Three color components of each pixel in the color space chose different ways to transform for achieving image scrambling, and its periodicity was discussed, for proposing the concept of singularity point and fake period. The experimental analysis shows that the algorithm has good effect of scrambling, larger key space, flexible encryption, and high security. And its diffusion and disturbance are ideal.

Key words: information security; digital image scrambling; three dimensional sub-affine transformation; periodicity; singularity point

0 引言

随着网络技术的飞速发展,如何有效地保证网络上信息传输的安全性问题成为人们研究的热点。由于图像所含信息量大,表现直观,因此数字图像置乱技术是图像信息安全与隐藏的基础性工作^[1],既可以看成图像加密的一种途径,又可用作图像分存技术、水印技术、隐藏技术的预处理和后处理。

为了解决图像信息量大、编码困难的难题,从数学角度不断寻找新的算法。文献[2]从矩阵理论与方法角度介绍了几种数字图像变换:Arnold变换、FASS曲线、Gray代码、Conway“游戏”、IFS模型以及Tangram算法;文献[3]提出了排列变换;文献[4]讨论了三维Arnold变换在数字图像置乱中的应用及其安全性分析;文献[5]提出一种基于基元分形走向的 n 阶三维Hilbert曲线生成算法在图像置乱中的应用;文献[6]提出了一种三维多级置乱的加密方法,以加密过程的混沌序列或密钥序列作为置乱参数,按一定的置乱规则,对不同大小的立方块信息进行多级置乱;文献[7]利用了图像像素可以插入到相邻像素之间以及拉伸折叠的思想设计了一种基于三维坐标的图像加密算法。以上应用于数字图像置乱的变换方法有一个共同特点,就是变换方法的模型较为固定,有一定的

规律可循,这样降低了攻击者进行图像信息解密的难度。

为了提高图像置乱后的保密性以及提高信息隐藏的抗攻击能力,使合法的使用者可以有更多的自由控制的密钥以供选择,文献[8]在仿射变换的基础上,提出了亚仿射变换;文献[9]给出了一种基于改进亚仿射变换的图像信息隐藏算法,但是没有给出亚仿射变换的相应构造方法;文献[10]给出了一种二维亚仿射变换的快速构造法。本文在文献[3,8,10]的基础上,给出了一种三维亚仿射变换的快速构造法,进一步讨论了它的性质和周期性,并提出伪周期和奇异点的概念。由于三维亚仿射变换形式的构造灵活性和复杂性,使得图像信息安全得以提高。同时用实验验证了周期性及其在数字图像置乱中的应用。

1 数字图像的三维亚仿射变换

1.1 三维亚仿射变换的定义

为了便于理解图像的三维亚仿射变换的定义,先介绍三维几何变换的定义。

定义1 三维仿射变换。其一般形式为:

$$\begin{cases} x' = ax + by + cz + k \\ y' = dx + ey + fz + m \\ z' = gx + hy + iz + n \end{cases}$$

收稿日期:2012-02-24;修回日期:2012-06-18。 基金项目:江西省自然科学基金资助项目(2009GQ0047)。

作者简介:邹玮刚(1976-),男,江西进贤人,讲师,硕士研究生,主要研究方向:数字图像处理、粗糙集; 陈沛云(1978-),女,湖南祁阳人,讲师,硕士研究生,主要研究方向:遥感图像处理; 黄江燕(1980-),女,江西定南人,讲师,硕士研究生,主要研究方向:粗糙集。

其中:

$$\Delta = \begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} \neq 0$$

且 $a, b, c, d, e, f, g, h, i, k, m, n$ 为实数。将其写成矩阵形式为:

$$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} k \\ m \\ n \end{bmatrix}$$

要求变换是离散点域 $\{(x, y, z) | 1 \leq x, y, z \leq N \text{ 且均为整数}\}$ 到其自身的一一映射。

定义2 三维亚仿射变换。若变换

$$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} k \\ m \\ n \end{bmatrix} \quad (1)$$

其中: $a, b, c, d, e, f, g, h, i, k, m, n$ 均为整数; $1 \leq x, y, z \leq N$, 且满足变换是离散点域 $\{(x, y, z) | 1 \leq x, y, z \leq N \text{ 且均为整数}\}$ 到其自身的一一映射, 则称该映射为三维亚仿射变换。在色彩空间中 N 称为数字图像的阶数。

1.2 三维亚仿射变换的快速构造法

由文献[5], 根据三维亚仿射变换的定义, 有如下定理。

定理1 由式(1) 给出的变换是三维亚仿射变换的必要条件是:

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = \pm 1.$$

证明 因为变换前后的图像面积不变, 即图像所在区域的几何面积不变, 根据三维亚仿射变换的定义, 有

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = \pm 1$$

定理1 给出的是必要条件, 而非充分条件, 即存在

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = \pm 1$$

并不能推出式(1) 给出的变换是亚仿射变换。

例1 对于给定的

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = \begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & -1 \\ 0 & -1 & 1 \end{bmatrix}$$

$$\text{有 } \begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = -1$$

对于其中的 $a = 1, b = 1, c = -1$, 即 $x' = ax + by + cz + k$ 。下面分情况讨论: ①当 $x + y < z$ 时, $k = N + 1$; ②当 $z \leq x + y < N$ 时, $k = 1$; ③当 $z < N < x + y < 2N$ 时, 无论怎么调整 k 的取值, 均有 $x' < 0$ 或 $x' > N$, 不满足三维亚仿射变换的定义。

因此, 由定义2, 定理1 以及例1 有如下推论。

推论1 若式(1) 为三维亚仿射变换, 则 $a, b, c, d, e, f, g, h, i, k, m, n \in \{-1, 0, 1\}$ 。

推论2 若式(1) 为三维亚仿射变换, 则在矩阵

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$

中, 同一行的元素不能同时为零, 也不能全部非零, 且非零元素不相等。

推论3 至少有一行只有一个非零元素。

由推论1 ~ 3 给出一种三维亚仿射变换的快速构造算法:

第1步 先构造矩阵

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$

$$\text{使 } \begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = \pm 1$$

且满足推论1 ~ 3 的条件;

第2步 以 a, b, c 为例, 求 k :

1) 若 $a + b + c = -1$, 则 $k = N + 1$ 。

2) 若 $a + b + c = 1$, 则 $k = 0$ 。

3) 若 $a + b + c = 0$, 当1在-1之前出现, 不妨令 $a = 1, b = -1$, 则当 $x < y$ 时, $k = N + 1$; 当 $x \geq y$ 时, $k = 1$ 。

4) 若 $a + b + c = 0$, 当-1在1之前出现, 不妨令 $a = -1, b = 1$, 则当 $x \leq y$ 时, $k = 1$; 当 $x > y$ 时, $k = N + 1$ 。

在其余情况下, 按3) 与4) 的规律同理构造。

第3步 根据第2步, 同理构造 m, n 的数值。

第4步 根据第2步与第3步的结果, 对 x, y, z 之间的大小关系给出正确的组合。

例2 由上述算法, 可以很快构造两个三维亚仿射变换如下:

$$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = \begin{cases} \begin{bmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} 1 \\ N+1 \\ N+1 \end{bmatrix}, & x \geq y \text{ 且 } y > z \\ \begin{bmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ N+1 \end{bmatrix}, & x \geq y \text{ 且 } y \leq z \\ \begin{bmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} N+1 \\ N+1 \\ N+1 \end{bmatrix}, & x < y \text{ 且 } y > z \\ \begin{bmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} N+1 \\ 1 \\ N+1 \end{bmatrix}, & x < y \text{ 且 } y \leq z \end{cases} \quad (2)$$

$$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = \begin{cases} \begin{bmatrix} -1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ N+1 \end{bmatrix}, & x \leq y \text{ 且 } y \geq z \\ \begin{bmatrix} -1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} 1 \\ N+1 \\ N+1 \end{bmatrix}, & x \leq y \text{ 且 } y > z \\ \begin{bmatrix} -1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} N+1 \\ N+1 \\ N+1 \end{bmatrix}, & x > y \text{ 且 } y \geq z \\ \begin{bmatrix} -1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} N+1 \\ 1 \\ N+1 \end{bmatrix}, & x > y \text{ 且 } Y < z \end{cases} \quad (3)$$

1.3 三维亚仿射变换的性质

设 F 为三维亚仿射变换的非空集合, “*” 为 F 上的一般

矩阵乘积运算,“+”为 F 上的一般矩阵加法运算。

为了讨论三维亚仿射变换的性质,先将式(1)改为如下形式:

$$\begin{bmatrix} x' \\ y' \\ z' \\ 1 \end{bmatrix} = \begin{bmatrix} a & b & c & k \\ d & e & f & m \\ g & h & i & n \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \\ 1 \end{bmatrix} = \begin{bmatrix} A & B \\ 0 & 1 \end{bmatrix} \begin{bmatrix} y \\ z \\ 1 \end{bmatrix}$$

其中:

$$A = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$

$$B = \begin{bmatrix} k \\ m \\ n \end{bmatrix}$$

并且 A 和 B 满足定义2的条件。因此三维亚仿射变换的性质均可由其变换矩阵

$$T = \begin{bmatrix} A & B \\ 0 & 1 \end{bmatrix}$$

来等价反映,并且 T 的性质主要可由 A 来主导。

由文献[8]的启发,给出三维亚仿射变换的性质如下。

性质1 三维亚仿射变换的积不是三维亚仿射变换。

证明 设有两个三维亚仿射变换矩阵

$$T_1 = \begin{bmatrix} A_1 & B_1 \\ 0 & 1 \end{bmatrix}$$

$$T_2 = \begin{bmatrix} A_2 & B_2 \\ 0 & 1 \end{bmatrix}$$

$$\text{则 } T_1 \times T_2 = \begin{bmatrix} A_1 & B_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} A_2 & B_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} A_1 A_2 & A_1 B_2 + B_1 \\ 0 & 1 \end{bmatrix}$$

虽然 $|A_1 A_2| = |A_1| \times |A_2| = \pm 1$,但是 $T_1 \times T_2$ 不一定是三维亚仿射变换。 $T_1 \times T_2$ 的性质完全可由 $A_1 A_2$ 决定。现举反例如下:

取式(2)~(3)的变换矩阵,得

$$A_1 = \begin{bmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}$$

$$A_2 = \begin{bmatrix} -1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & -1 & 0 \end{bmatrix}$$

$$\text{有 } A_1 \times A_2 = \begin{bmatrix} -1 & -1 & 2 \\ 1 & -1 & -1 \\ 0 & -1 & 1 \end{bmatrix}$$

虽然 $|A_1 A_2| = 1$,但是很显然 $A_1 \times A_2$ 不符合快速构造算法的原理,在 $A_1 \times A_2$ 的第一行就会出现例1中的现象,不符合三维亚仿射变换的定义,因此三维亚仿射变换的积不是三维亚仿射变换。

性质2 三维亚仿射变换的和不是三维亚仿射变换。

此性质显然,证明略。

性质3 三维亚仿射变换的逆一定存在,但逆变换不是三维亚仿射变换。

证明 由

$$T = \begin{bmatrix} A & B \\ 0 & 1 \end{bmatrix}$$

$$\text{有 } T^{-1} = \begin{bmatrix} A^{-1} & -A^{-1}B \\ 0 & 1 \end{bmatrix}$$

因此 T^{-1} 由 A^{-1} 决定。显然

$$|A^{-1}| = \frac{|I_E|}{|A|} = \pm 1$$

其中 I_E 为 3×3 的单位矩阵。

但是 A^{-1} 也不一定为三维亚仿射变换。现举反例如下:

由式(3)可得:

$$A_2 = \begin{bmatrix} -1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & -1 & 0 \end{bmatrix}$$

$$\text{有 } A_2^{-1} = \begin{bmatrix} -1 & -1 & -1 \\ 0 & 0 & -1 \\ 0 & -1 & -1 \end{bmatrix}$$

显然 A_2^{-1} 不能实现三维亚仿射变换。因此三维亚仿射变换的逆一定存在,但逆变换不是三维亚仿射变换。

性质4 三维亚仿射变换的复合变换仍然是三维亚仿射变换。

由于复合变换函数之间变元的传递性,使得三维亚仿射变换的复合变换仍然是三维亚仿射变换。

定理2 代数系统 $\langle F, + \rangle$ 不构成变换群。

由性质2, F 关于加法运算不封闭,因此代数系统 $\langle F, + \rangle$ 不构成变换群。

定理3 代数系统 $\langle F, * \rangle$ 不构成变换群。

由性质3,并不是 F 中的每个元素的逆元素均在 F 中,即存在某个元素在 F 中不存在逆元素,由群的定义,可知代数系统 $\langle F, * \rangle$ 不构成变换群。

2 应用于图像置乱变换的周期性

定义3 对于给定的 N 阶数字图像,三维亚仿射变换(式(1))的变换周期是指能使任何一个 N 阶的数字矩阵经三维亚仿射变换(式(1))恢复到原始图像的最少次数,记为 T_N 。

由三维亚仿射变换的定义和图像置乱周期的定义,有如下定理。

定理4 三维亚仿射变换用于图像置乱变换存在周期。

以式(3)定义的三维亚仿射变换为例,假定图像为一个 N 阶的数字矩阵,求得其周期 T_N 如表1所示。

表1 不同阶数 N 下三维亚仿射变换的周期 T_N

N	T_N	N	T_N	N	T_N
3	8	15	40	256	384
4	6	16	24	289	612
5	20	18	24	290	420
6	8	20	60	300	600
9	24	30	120		
10	60	36	24		

推论4 对于两幅图像 A 和 B ,如果 A 的阶 N_A 整除 B 的阶 N_B ,则 A 的周期 T_{N_A} 整除 B 的周期 T_{N_B} 。

由于图像数据的冗余性和人类视觉的冗余性,并不要求完全恢复原始图像所有像素点就能破解图像所承载的信息,因此并不需要运行整个周期,也不需求所有点均恢复到原始状态,就可以知道图像信息,达到解密的目的。根据周期实验

的结果与规律,下面给出奇异点和伪周期的概念。

定义4 在图像置乱中,在给定循环次数上限不能恢复到原始状态的点称为奇异点。

定义5 对于给定的 N 阶数字图像,三维亚仿射变换(式(1))的伪周期是指在奇异点存在的情况下,能使任何一个 N 阶的数字矩阵经三维亚仿射变换(式(1))重现原始图像信息所需要的像素点恢复到原始状态时所需的次数,记为 WT_N 。

推论5 对于给定的 N 阶数字图像,三维亚仿射变换(式(1))的伪周期小于等于周期。

以式(3)定义的三维亚仿射变换为例,假定图像为一个 N 阶的数字矩阵,求得其伪周期 WT_N 如表2所示,并对奇异点进行举例,本实验循环次数上限为10000。

表2 不同阶数 N 下三维亚仿射变换的伪周期 WT_N

N	WT_N	奇异点举例	N	WT_N	奇异点举例
40	60	(38,39,1)	100	300	(77,88,2)
49	112	(32,29,7)	110	60	(29,79,49)
60	120	(38,49,1)	160	240	(123,111,8)
64	96	(38,49,2)	200	300	(111,123,8)
81	216	(80,6,55)	225	600	(111,123,11)

3 三维亚仿射变换在图像置乱中的应用

由于数字图像本身特点的限制,在色彩空间中,本实验以24位真彩色图像为研究对象。图像中每个像素点的三个色彩分量 r, g, b 的取值范围为 $0 \sim 255$,因此在本实验中 $N = 256$ 。

一幅24位真彩色数字图像可用矩阵 $A = \{m(i, j)_{N \times N}\}$ 表示,其中 $m(i, j)$ 表示图像在第 i 行第 j 列处像素的RGB分量。将三维亚仿射变换应用到数字图像上,在色彩空间中,将点 (x, y) 处像素的RGB颜色分量 r, g, b 进行相应变换,得到点 (x, y) 处像素的另一组RGB颜色分量 r', g', b' ,然后将 $(r', g', b')^T$ 作为下一次相应变换的输入,从而经过一定的迭代置乱变换后,能得到较好的置乱效果,原始图像的信息得到较好的隐藏,这一迭代过程可重复地进行,且具有周期性。

在色彩空间中,用式(3)给出的三维亚仿射变换,对Lena图像(256×256 像素, $N = 256$)进行置乱的效果如图1所示。

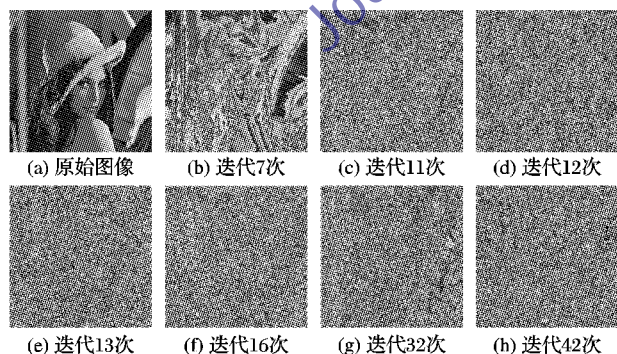


图1 三维亚仿射变换的图像置乱效果

4 三维亚仿射变换置乱效果分析

如何评估图像置乱后的效果,如何能够给出原始图和置乱图一个有效的度量是目前受到关注的一个焦点问题。目前评价图像置乱效果的方法主要分为主观评价法和客观评价法。主观评价法是由人的视觉感知对置乱图像进行评价,具有简单、直观等优点,然而会有很多主观因素影响评价结果的真实性。因此,对图像置乱程度的客观评价研究对于指导信息隐

藏时寻找更好的置乱变换,以及了解他人隐藏信息进行解密等方面具有重要的理论价值和实际意义。

文献[11]提出采用置乱程度来量化置乱效果的思想,并基于置乱前后像素点位置移动的平均距离来定义置乱程度,但效果很不理想;文献[12]从图像纹理特征角度出发利用差分熵定义图像置乱程度,但缺乏置乱图像在位置信息上的充分考虑;文献[13]提出基于均方信噪比来定义图像置乱度,但未考虑图像像素之间的空间邻域关系,导致不能客观真实地评价图像置乱程度;文献[14]基于邻域像素差异程度来定义置乱度,得到了一些较满意的数据。这些评价方法都是针对几何变换置乱算法且各有其特点,至今没有一种十分理想的图像置乱程度评价方法。本文从密钥空间、直方图统计分析和相邻像素的相关性来分析图像置乱的效果。

4.1 密钥空间分析

为了提高图像置乱后的保密性以及提高信息隐藏的抗攻击能力,使合法的使用者可以有更多的自由控制的密钥以供选择,三维亚仿射变换的定义公式(式(1))有12个密钥参数。但是在实例公式(式(3))中,由于在三维空间中 x, y, z 三个参数之间的组合情况的灵活性和复杂性,使得三维亚仿射变换的破解更加困难,在密钥空间中三维亚仿射变换优于一般的三维几何变换,可以更加有效地抵抗穷举攻击。

4.2 直方图统计分析

原图像直方图如图2(a),置乱16次后得到的加密图像的直方图如图2(b)。由图可知,与明文图像的直方图分布不均相比,密文图像直方图分布较为均匀,很好地掩盖了原始图像的分布规律,增加了破译难度,因此密文图像统计特性良好,有着很好的扰乱性。

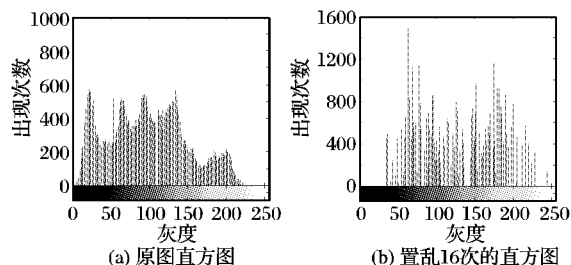


图2 加密前后统计直方图

4.3 相邻像素的相关性分析

相邻像素的相关性可以反映出图像像素的扩散程度,原始图像中相邻两个像素的相关性通常很大,加密后图像相邻像素的相关性要尽可能小。设 x, y 分别表示相邻两个像素的灰度值,相邻两个像素的相关系数 r_{xy} 的计算公式^[15]如下:

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

其中:

$$\text{conv}(x, y) = \frac{1}{N} \sum_{i=1}^N [x_i - E(x)][y_i - E(y)]$$

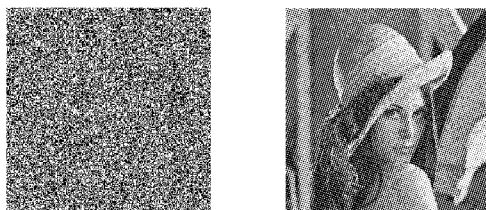
$$D(x) = \frac{1}{N} \sum_{i=1}^N [x_i - E(x)]^2$$

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

分别随机选取原始图像和置乱16次后的加密图像的1000对水平方向、垂直方向和对角方向上的相邻像素进行测试。令 r_{xy}^h, r_{xy}^v 和 r_{xy}^d 分别表示图像水平、垂直、对角三个方向的相关系数。经过计算,原始图像的 $r_{xy}^h = 0.9817, r_{xy}^v = 0.9929,$

(下转第2602页)

强度为5%的高斯白噪声的解密图像。受到噪声污染的密文图像经正确密钥解密后能够恢复原始图像的主要信息,但存在一定的失真,这表明本文算法具有一定的抗噪声能力。



(a) 加密图像加入5%的高斯白噪声 (b) 解密图像

图7 含噪声解密图像

4 结语

结合 FrFT 与混沌置乱技术,本文基于频谱切割提出了一种单通道彩色图像加密算法,并对其密钥空间、均方误差、相关性、抗噪声性能等进行了分析。该算法密文为灰度图像,具有多重密钥,可以抵御穷举攻击。仿真结果表明,加密图像相邻像素之间的相关性小,加密算法具有较强的抗统计分析能力、抗裁剪能力和抗噪声性能。

参考文献:

- [1] JOSHI M, CHANDRASHAKHER K, SINGH K. Color image encryption and decryption using fractional Fourier transform [J]. Optics Communications, 2007, 279(1): 35-42.
- [2] CHEN LIN-FEI, ZHAO DAO-MU. Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms [J]. Optics Express, 2006, 14(19): 8552-8560.
- [3] 杨晓苹,高丽娟,王晓雷,等.基于双相位编码的单通道彩色图像加密[J].物理学报,2009,58(3):1662-1666.
- [4] UNNIKRISHNAN G, JOSEPH J, SINGH K. Optical encryption by double-random phase encoding in the fractional Fourier domain [J]. Optics Letters, 2000, 25(12): 887-889.
- [5] ZHU BANG-HE, LIU SHU-TIAN. Optical image encryption based on the generalized fractional convolution operation [J]. Optics Communications, 2001, 195(5/6): 371-381.
- [6] TAO RAN, MENG XIANG-YI, WANG YUE. Image encryption with multiorders of fractional [J]. IEEE Transactions on Information Forensics and Security, 2010, 5(4): 734-738.
- [7] ZHOU NAN-RUN, DONG TAI-JI, WU JIAN-HUA. Novel image encryption algorithm based on multiple-parameter discrete fractional random transform [J]. Optics Communications, 2010, 283(15): 3037-3042.
- [8] CHEN LIN-FEI, ZHAO DAO-MU, GE FAN. Gray images embedded in a color image and encrypted with FRFT and Region Shift Encoding methods [J]. Optics Communications, 2010, 283(10): 2043-2049.
- [9] 王雅庆,周尚波.基于分数阶 Fourier 变换的数字图像加密算法研究[J].计算机应用研究,2011,28(7):2738-2741.
- [10] 刘正君.分数阶变换及其在图像加密和滤波中的应用[D].哈尔滨:哈尔滨工业大学,2007.
- [11] 龚黎华.基于混沌映射与 FrFT 的单通道彩色图像加密算法[D].南昌:南昌大学,2011.
- [12] LIU ZHENG-JUN, LI QIU-MING, DAI JING-MIN, et al. A new kind of double image encryption by using a cutting spectrum in the 1-D fractional Fourier transform domains [J]. Optics Communications, 2009, 282(8): 1536-1540.
- [13] 黄仿元.基于 Arnold 变换的图像置乱算法及实现[J].贵州大学学报,2008,25(3):277-278.
- [14] 武汉大学学报:理学版,2011,57(5):444-448.
- [5] 万里红,孙燮华,林旭亮.三维 Hilbert 曲线在图像置乱中的应用[J].计算机工程,2011,37(2):227-229.
- [6] 吕政,唐海萍,陈海虹.基于三维置乱的加密算法及效果分析[J].通信技术,2009,42(4):159-162.
- [7] 农盛功,周满元.基于三维空间的图像加密算法[J].计算机系统应用,2010,19(8):87-91.
- [8] 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报,2003,15(2):205-208.
- [9] 卢斌,王冰.基于改进亚仿射变换的图像信息隐藏算法[J].计算机工程,2011,37(11):164-167.
- [10] 邹玮刚,洪春勇.一种亚仿射变换的快速构造法及其性质与应用[C]//第十二届全国图像图形学学术会议论文集.北京:清华大学出版社,2005:117-120.
- [11] 柏森,曹长修.图像置乱程度研究[C]//第3届信息隐藏全国学术研讨会论文集.西安:西安电子科技大学出版社,2001:75-81.
- [12] 商艳红,李南,邹建成. Fibonacci 变换及其在数字图像水印中的应用[J].中山大学学报:自然科学版,2004,43(增刊2):148-151.
- [13] 卢振泰,黎罗罗.一种新的衡量图像置乱程度的方法[J].中山大学学报:自然科学版,2005,44(增刊):126-129.
- [14] 李志伟,陈燕梅,张胜元.基于 SNR 的数字图像置乱程度评价方法[J].厦门大学学报:自然科学版,2006,45(4):484-487.
- [15] 顾国生,刘富春.基于混沌映射的图像 Contourlet 编码加密算法[J].计算机应用,2011,31(3):771-774.

(上接第 2598 页)

$r_{xy}^d = 0.9800$,置乱 16 次后的加密图像的 $r_{xy}^h = 0.0237$, $r_{xy}^v = 0.1259$, $r_{xy}^d = 0.0783$ 。由此可见,明文图像中高度相关的相邻像素,在密文图像中几乎没有相关性。这说明明文图像的统计特性已被扩散到密文中,加密算法具有良好的扩散性。

5 结语

通过对三维亚仿射变换的定义与图像排列变换的规律分析,给出了一种三维亚仿射变换的快速构造法,并用实例对三维亚仿射变换的性质和用于图像置乱的周期性进行了研究,首次给出了伪周期和奇异点的概念。三维亚仿射变换用于图像置乱不仅增加了置乱时的密钥参数选择,同时由于变量之间的组合情况非常灵活,提高了图像置乱后的保密性和信息隐藏的抗攻击能力。因此增加了图像信息的安全性,同时具有很好的置乱效果,能很好地隐藏原始图像的信息,对图像的置乱加密有一定的应用研究价值。

参考文献:

- [1] 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藏中的应用[J].中国科学:E辑,2000,30(5):440-447.
- [2] 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.
- [3] 吴晏升,王介生,刘慎权.图像的排列变换[J].计算机学报,1998,21(6):514-519.
- [4] 刘婷,闵乐泉.基于 Arnold 变换的图像置乱密码的安全性分析