

基于 Arnold 变换和图像融合的数字图像隐藏算法

田鹏辉^{1,2}, 隋立春²

(1 长安大学 地质工程与测绘学院, 陕西 西安 710054; 2 西安工业大学 计算机科学与工程学院, 陕西 西安 710032)

摘 要: 针对传统 Arnold 反变换需要先计算出变换周期和恢复图像时间较长的弱点, 提出了快速 Arnold 反变换方法, 该方法利用 6 个方程组求解得到。实验证明该方法可行、效果好, 大大节省了恢复原始图像的时间, 提高了传统 Arnold 算法的效率, 同时具有良好的鲁棒性。

关键词: 数字图像; 图像隐藏; 猫脸变换; 图像融合

中图分类号: TP391

文献标识码: A

文章编号: 1000-7180(2013)04-0010-04

Digital Image Hiding Technology Based on Arnold Transformation and Image Blending

TIAN Peng-hui^{1,2}, SUI Li-chun²

(1 College of Engineering and Geomatics, Chang'an University, Xi'an 710054, China;

2 School of Computer Science & Engineering, Xi'an Technological University, Xi'an 710032, China)

Abstract: Traditional Arnold inverse transformation needs to calculate the cycle of transformation, and it spends on more times in images recovery. In this paper a recovery method of hidden digital image based on fast Arnold inverse transformation is proposed. It needs to solve six equations set. Experimental results show the proposed method has high robustness, improves the efficiency of image restoration than the traditional Arnold inverse transformation.

Key words: digital images; image hiding; Arnold transformation; image blending

1 引言

信息隐藏(Information Hiding)技术,是国际上近年来提出的一种信息安全的新的概念^[1]。而以数字图像为载体的信息隐藏技术,更具有迷惑性,同时产生的隐藏信息更能经受起恶意的攻击。随着互联网的迅速普及和多媒体技术的飞速发展,信息隐藏已经在通信保密、资料的完整性验证、数字作品的版权保护以及商务活动中的票据防伪等领域发挥着重要作用。

与一般的文字信息相比,数字图像本身可以携带更多的信息量,这使得传统的加密方法不适合应用到图像的加密上^[2]。而图像置乱技术是当前重要的数字图像加密技术^[3]。其中 Arnold 变换算法简单

而具有周期性^[4-6],因而在数字图像的置乱加密方面得到了广泛应用,然而其加密过程由于不断的进行矩阵的迭代运算,因此非常耗费运算时间,因而在实时的数字图像置乱加密领域很少应用。

本文基于 Arnold 变换思想给出一种改进的 Arnold 反变换代替传统的 Arnold 置乱算法,从而有效提高了隐藏图像恢复的效率。实验表明该方法具有较好的图像置乱效果和鲁棒性。

2 数字图像置乱和图像融合技术

数字图像置乱是一种重要的图像加密技术。当前常见的主要有 Arnold 变换、幻方变换、IFS 模型、分型 Hilbert 曲线、Tangram 算法、Gray 码变换等方法。而 Arnold 变换由于算法简单且具有周期性,

因此在数字图像信息隐藏方面得到了很好的应用^[7].

2.1 Arnold 变换

Arnold 变换是俄国数学家 V. J. Arnold 在遍历理论中提出的一种变换,俗称猫脸变换. 根据不同相位空间,可分为 2 维、3 维以及 N 维的 Arnold 变换. 一幅 $N \times N$ 的数字图像的 2 维 Arnold 变换定义为:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{N} \quad (1)$$

其中 $x, y \in \{0, 1, 2, \dots, N-1\}$ 表示变换前像素的位置, x', y' 表示变换之后的像素位置, mod 为模运算.

利用式(1),依次对数字图像中每个像素做变换后,就可以产生置乱后的图像,对置乱图像再进行重复迭代变换就能得到理想的置乱效果. 同时,Arnold 变换具有周期性,即当重复变换到一定次数后,将重新得到原来的图像.

表 1 为不同阶数 N 与数字图像的 Arnold 变换周期 C_N 的关系,可以看出 Arnold 变换的周期与数字图像的大小有关系,但并非线性关系.

表 1 不同阶数 N 下的 Arnold 变换周期

N	2	5	10	50	100	128	256	512
C_N	3	10	30	150	150	96	192	384

使用 Arnold 变换,对于一幅 256×256 的灰度数字图像进行置乱后的效果如图 1 所示.



图 1 多次 Arnold 变换效果图

数字图像可以看作一个 2 维矩阵,经过 Arnold 变换之后图像的像素位置会重新排列,这样图像会显得杂乱无章,从而实现了图像的置乱加密效果. 因此,传统的 Arnold 反变换都采用与 Arnold 正变

换(假定已经正变换 t 次, $t \in [1, N]$)同样的算法,通过再迭代变换一定的周期即 $C_N - t$ 次,就能还原图像,而这种方法却极其耗费运算时间,在大量的图像恢复场合是不适合使用的.

2.2 数字图像融合技术

从构成数字图像的像素角度考虑,可以在两幅同等大小的图像之间进行线性插值,来实现对其中某一幅图像的快速隐藏,这就是基于融合的图像隐藏的基本原理^[8].

假设待隐藏图像为 H ,载体图像为 C ,融合的结果图像为 R ,则根据插值原理有如下公式:

$$R(i, j) = \alpha(H(i, j) - C(i, j)) + C(i, j) \quad (2)$$

$0 < \alpha < 1$

式中 $H(i, j)$ 和 $C(i, j)$ 分别为待隐藏图像和载体图像上对应像素 (i, j) 处的灰度值, $R(i, j)$ 为两个像素之间插值的结果.

当融合因子 α 从 0 变到 1 时,则相应的结果图像从载体图像变化到待隐藏图像. 图 2 是采用式(2)的方法进行融合的结果,分别进行了 4 次不同融合因子的插值运算.

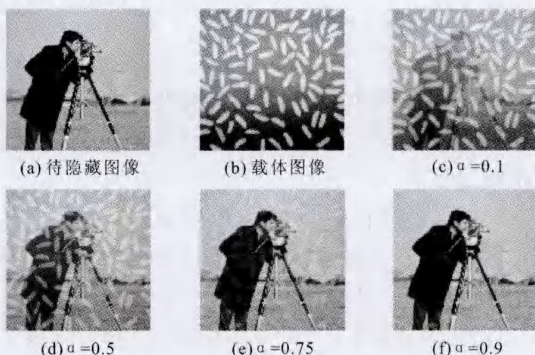


图 2 基于不同融合因子的图像隐藏

实验表明,当 α 越接近于 0,待隐藏图像的隐藏效果越差;反之,当 α 越接近于 1,隐藏效果就越好,然而此时,图像恢复也就越困难.

3 数字图像隐藏与恢复方法

合数字图像融合技术和 Arnold 变换理论,下面给出基于图像融合技术和快速 Arnold 反变换的数字图像隐藏及恢复方法.

3.1 快速 Arnold 反变换

为了克服 Arnold 变换在数字图像置乱后重新进行恢复时的不足,对于一幅 $N \times N$ 的 2 维数字图像,上述 Arnold 变换公式(1)可以写成如下等价形式:

$$\begin{bmatrix} x'-1 \\ y'-1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x-1 \\ y-1 \end{bmatrix} \pmod{N} \quad (3)$$

即

$$\begin{cases} x'-1 = x+y-2 \pmod{N} \\ y'-1 = x+2y-3 \pmod{N} \end{cases} \quad (4)$$

因此表明存在 m, n (m, n 为整数) 使得

$$\begin{cases} (x+y-2-x'+1)/N = m \\ (x+2y-3-y'+1)/N = n \end{cases}$$

即

$$\begin{cases} x+y = Nm + x' + 1 \\ x+2y = Nn + y' + 2 \end{cases} \quad (5)$$

而在图像处理的实际情况下, 又隐含着约束条件:

$$1 \leq x, y, x', y' \leq N \quad (6)$$

因此, 由式(5)可以得到

$$\begin{cases} 2 \leq x+y \leq 2N \\ 3 \leq x+2y \leq 3N \end{cases} \quad (7)$$

由式(4)、(6)可以得到

$$\begin{cases} 0 \leq x+y-x'-1 \leq 2N-2 \\ 0 \leq x+2y-y'-2 \leq 3N-3 \end{cases}$$

$$\text{即} \begin{cases} 0 \leq Nm \leq 2N-2 \\ 0 \leq Nn \leq 3N-3 \end{cases} \quad (8)$$

因此 m 只能取 0, 1; 而 n 只能取 0, 1, 2. 于是可以得到 $C_2^1 \times C_3^1 = 6$ 个方程组. 以下根据实际情况分析求解过程.

(1) $x' \leq y'$, 则 $y' - x' \geq 0$, 所以 $m = n$, 即

$y = y' - x' + 1$. 若 $x' < y$, 则 $x = N + x' - y + 1$; 否则 $x = x' - y + 1$.

(2) $x' > y'$, 则 $y' - x' < 0$, 所以 $n = m + 1$, 即

$y = N + y' - x' + 1$. 若 $x' < y$, 则 $x = x' - y + N + 1$; 否则, $x = x' - y + 1$.

该方法克服了利用周期性进行 Arnold 置乱恢复需要预先求变换周期以及恢复时间长的弱点, 能够快速有效地恢复出原始图像.

3.2 图像隐藏算法

隐藏算法步骤如下:

步骤 1: 输入待隐藏图像 H 、载体图像 C , 根据表 1 的不同阶数 N 下的 Arnold 变换周期范围, 选取待隐藏图像进行 Arnold 变换的置乱次数 k (例如 $k=10$).

步骤 2: 将待隐藏图像 H 按照第 2.1 节的 Arnold 变换算法, 进行置乱处理, 得到置乱图像 H_1 .

步骤 3: 根据 2.2 节提出的图像融合技术, 选取适当的乘法因子 α , 将图像 H_1 的每一个像素 $H_1(i,$

$j)$ 隐藏在载体图像对应像素 $C(i, j)$ 中, 隐藏后的该位置像素变为:

$$R(i, j) = \alpha(H_1(i, j) - C(i, j)) + C(i, j) \quad (9)$$

步骤 4: 重复步骤 3 直到图像 H_1 的所有像素 $H_1(i, j)$ 都隐藏在载体图像 C 的对应像素 $C(i, j)$ 中.

3.3 图像恢复算法

恢复算法其实是隐藏算法的逆过程, 步骤如下:

步骤 1: 根据公式(8), 求出恢复隐藏图像的算式, 即:

$$H_1(i, j) = \frac{1}{\alpha} R(i, j) - C(i, j) + C(i, j) \quad (10)$$

步骤 2: 按照公式(10)对结果图像 R 和载体图像 C 的每一像素逐一进行计算, 得到置乱后的隐藏图像 H_1 .

步骤 3: 利用 3.1 节给出的快速 Arnold 反变换对图像 H_1 的像素 $H_1(i, j)$ 进行恢复(反置乱).

步骤 4: 重复步骤 3, 直到 H_1 的所有像素都进行了快速 Arnold 反变换, 至此得到恢复的隐藏图像.

4 实验仿真结果

实验中待隐藏图像和载体图像大小相同, 均为 256×256 像素, 通过上述算法进行数字图像的隐藏及恢复. 利用 MATLAB 进行仿真实验, 实验结果如图 3 所示.

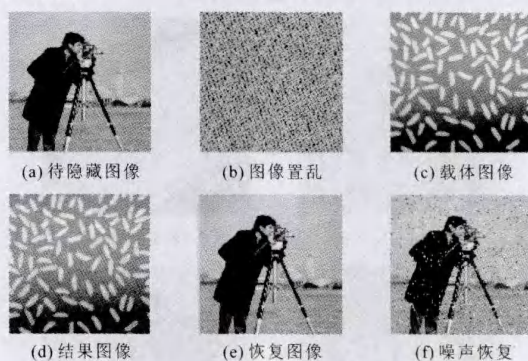


图 3 数字图像隐藏与恢复的实验结果

图 3(a) 为待隐藏图像, 图 3(b) 为待隐藏图像经过 10 次 Arnold 变换置乱后的图像, 图 3(c) 为载体图像, 图 3(d) 为融合因子 $\alpha=0.1$ 的隐藏图像效果, 图 3(e) 为利用快速 Arnold 反变换恢复的待隐藏图像, 图 3(f) 为隐藏结果图像加入椒盐噪声后的恢复图像.

通过在奔腾 3.0GHz 的 CPU 上的实验对比, 改进的快速 Arnold 反变换比传统 Arnold 变换在时间

上缩短了 45%,该方法明显提高了图像隐藏的安全性和恢复图像时的效率。

5 结束语

本文提出了基于快速 Arnold 反变换的隐藏数字图像恢复方法。该方法利用改进的 Arnold 反变换,在保证了对加密待隐藏信息的同时,大大节省了恢复原始图像的时间,提高了 Arnold 算法的效率。实践表明,该方法具有良好的鲁棒性。同时,由于 Arnold 变换具有周期性,使得密钥空间比较小,即图像经过若干次 Arnold 变换后,又变回原来的图像,这是下一步要深入研究的问题。

参考文献:

- [1] Petiteolas F A P, Andesron R J, Kuhn M G. Information hiding — a survey[J]. Proceedings of the IEEE, 1999, 87(7):1062—1077.
- [2] Chen Guanrong, Mao Yaobin, CHUI Charles K. A symmetric image encryption scheme based on 3D chaotic cat maps [J] Chaos, Solutions and Fractals, 2004, 21(3):749—761.
- [3] Qi D X, Zou J C, Jan X Y. A new scramble transformation and its application to image hiding[J]. Science in China: Series E, 2000, 30(5):440—447.
- [4] Sun W. The periodicity of Arnold transformation[J]. Journal of North China University of Technology, 1999, 11(1):29—32.
- [5] Zou J C, Tie X Y. Arnold transformation of digital image with two dimesions amd its periodicity[J]. Journal of North China University of Technology, 2000, 12(1):10—14.
- [6] 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:自然科学版, 2008, 25(3):276—279.
- [7] Chin S S, Hsiang C H, Feng H W, et al. Genetic watermarking based on transform — domain techniques [J]. The Journal of the Pattern Recognition Society, 2004, 37(3):555—565.
- [8] 张雪锋, 范九伦. 基于图像融合的数字图像隐藏技术[J]. 微电子学与计算机, 2007, 24(2):188—190.

作者简介:



田鹏辉 (1975—), 博士研究生, 副教授. 研究方向为数字图像处理、空间目标识别与跟踪。

隋立春 (1963—), 教授. 研究方向为影像分析、InSAR 及激光雷达数据处理等。