doi:10.11959/j.issn.1000-436x.2016128

基于 Arnold 变换的数字图像自适应隐写算法

李琪[1]，廖鑫[1,2,3]，屈国庆[4]，陈国永[1]，杜蛟[5]

（1. 湖南大学信息科学与工程学院，湖南 长沙 410082；2. 中国科学院软件研究所，北京 100190；3. 中国科学院信息工程研究所，北京 100190；
4. 南京大学软件学院，江苏 南京 210093；5. 河南师范大学数学与信息科学学院，河南 新乡 453007）

摘 要：以往的图像自适应隐写算法大多数以顺序满嵌的方式嵌入秘密信息，这类算法秘密信息的隐蔽性不够高，因此提出一种随机非满嵌算法。通过分析出图像的系统参数使图像的满嵌容量刚好大于秘密信息的长度让载体图像达到非满嵌，增强了隐写的灵活性，减少了载体图像的嵌入修改量。再使用 Arnold 变换对数据的嵌入顺序进行置乱，防止攻击者按顺序分析出秘密信息，使秘密信息的隐蔽性变高，进而提高了算法的安全性。实验结果表明本算法提高了隐写的隐蔽性，减少了图像的嵌入失真度，且随机非满嵌操作适用于很多同类算法。

关键词：隐写术；Arnold 变换；系统参数；非满嵌

中图分类号：TP309 **文献标识码**：A

Adaptive steganography algorithm in digital image based on Arnold transform

LI Qi[1], LIAO Xin[1,2,3], QU Guo-qing[4], CHEN Guo-yong[1], DU Jiao[5]

(1. College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China;
2. Institute of Software Chinese Academy of Sciences, Beijing 100190, China;
3. Institute of Information Engineering Chinese Academy of Sciences, Beijing 100190, China;
4. Software Institute, Nanjing University, Nanjing 210093, China;
5. College of Mathematics and Information Science, Henan Normal University, Xinxiang 453007, China)

Abstract: Previous adaptive steganography algorithms were based on ordinal and full-embedding method. However, these algorithms might cause the concealment of secret information not good enough. Therefore, a random and non-fully embedding method was proposed to improve the concealment. The image system parameters could be obtained, so that the image full capacity was exactly greater than the length of information for non-full embedding. Moreover, these parameters made steganography more flexibility by reducing the modifications of image. Then, secret information embedding sequence was scrambled based on Arnold transform for the purpose that the steganalyst cannot detect out information orderly. Therefore, the secret information can be more concealed, which can improve the security of the algorithms. Experimental results show that the algorithm not only improves the concealment of steganography but also reduces stego distortion, and random non-full embedding operating can be applied to many other similar algorithms.

Key words: steganography, Arnold transform, system parameter, non-fully embedding

1 引言

隐写术是信息隐藏的一个重要分支，主要的研究内容是如何把秘密信息隐藏到多媒体数据中实现隐蔽通信[1]。近 10 年来，隐写术在国际上引起了广泛关注[2]。众多隐写方法主要是以数字图像、音频、

收稿日期：2015-08-23；**修回日期**：2016-05-24
通信作者：廖鑫，xinliao@hna.edu.cn
基金项目：国家自然科学基金资助项目(No.61402162，No.U1404601，No.61402154，No.11571094)；教育部博士点新教师基金资助项目(No.20130161120004)；湖南省自然科学基金资助项目(No.14JJ7024)；中国博士后科学基金资助项目(No.2014M560123)；河南省高校科技创新团队支持计划基金资助项目(No.14IRTSTHN023)

Foundation Items: The National Natural Science Foundation of China(No.61402162, No.U1404601, No.61402154, No. 11571094), Doctoral Program of Higher Programs Foundation of Chinese Ministry of Education(No.20130161120004), Hunan Provincial Natural Science Foundation of China (No.14JJ7024), Project Funded by China Postdoctoral Science Foundation (No.2014M560123), Program for Innovative Research Team (Science and Technology) in University of Henan Province(No.14IRTSTHN023)

视频、文本等作为载体，其中，以数字图像为载体的隐写算法研究最为成熟，研究成果最为丰富[3~6]。隐写算法主要关注隐写容量、嵌入失真度、安全性等性能指标[7]。为了提升上述性能指标以便更好地实现隐蔽通信，本文在设计隐写算法时也关注这些指标。

不同的隐写算法对图像造成的影响不同，已有研究者在这方面进行了很多的研究。1996 年，Bender 和 Gruhl 充分利用了人类视觉系统对图像微小改动的不敏感性和图像的最低有效比特位平面的类噪声特性，提出了 LSB 数字图像隐写算法[8]。然而，LSB 隐写算法对每个像素的修改量都是相同的，忽略了图像的局部复杂度和边缘效应。因此，2003 年，Wu 和 Tsai[9]提出了基于像素差值(PVD, pixel value differencing)的数字图像隐写算法。该算法将载体图像划分成许多个互不重叠的像素对，每个像素对包含相邻 2 个像素，2 个像素所被嵌入的秘密信息比特数取决于它们的像素差值，并且用这些差值来负载秘密信息。为了研究出性能更高的隐写算法，2005 年，Wu 等[10]又将原 PVD 算法和经典的 LSB 替换算法相结合，根据不同像素对的像素差值将像素对划分成 2 个区域：对于像素差值较小的像素对直接采用经典的 LSB 替换算法进行隐写；对于像素差值较大的像素对采用原 PVD 算法进行隐写。然而，为了保证秘密信息的准确提取和减少嵌入失真度，在 2008 年，Wang 等[11]提出了一种基于像素差值和模函数的数字图像隐写算法。算法在模函数下利用相邻 2 个像素值之和来负载秘密信息，并且采用一个修改操作来修改像素值。由于以前算法的嵌入修改量大，所以，2011 年，Sun 等[12]提出了基于两像素差值和编码技术的数字图像隐写算法。算法首先利用相邻两像素对的像素差值将像素对划分成 2 个区域，对位于不同区域的像素对采用参数不同的编码技术，修改 2 个像素值使用编码函数值来负载秘密信息。但是基于两像素差值的算法仍然不足以准确判断出载体图像中边缘区域和非边缘区域。这时，Liao 等[13]提出了基于四像素平均差值和编码技术的数字图像隐写算法。该算法描述了一种新颖的平均差值概念，它充分考虑了图像载体的边缘效应并且可以准确地提取出嵌入的秘密信息。

Arnold 变换是数字图像置乱中常用的一种方法。对数字水印或嵌密图像进行 Arnold 变换，实质是让图像的像素位置重新排列，得到一张相对原图像比较混乱的图像，以此来增加图像的保密性。但混乱的图像很容易引起攻击者的怀疑进而截取嵌密图像，攻击者按顺序就可以提取出正确的秘密信息，这样会导致秘密信息的隐蔽性不够高。基于以上两点，本文在图像信息隐藏过程中对嵌密顺序进行 Arnold 变换，使攻击者顺序提取出一串被打乱的秘密信息而得不到正确的秘密信息。对嵌密顺序的置乱间接提高了算法的安全性，原因在于本文使用 Arnold 变换是针对嵌密顺序而不是整张图片置乱。这样就会防止嵌密图像变成混乱的图像，进而不会引起攻击者去还原嵌密图像。若攻击者截取了嵌密载体，但嵌密图像看上去和原始载体一样，就导致攻击者不会使用 Arnold 变换置乱嵌密图像，攻击者会顺序提取出错误的秘密信息，进而提高了算法的安全性。

本文提出基于 Arnold 变换的数字图像自适应隐写算法，解决了前人在研究同类算法中只能对载体图像进行顺序满嵌的问题，提高了算法的安全性。本文分析秘密信息和满嵌容量的大小关系来调整参数改变图像的满嵌容量，使调整后的参数能够满足隐写者的需求，刚好达到非满嵌，减小了图像的嵌入修改量，进而增强了隐写的灵活性。然后，用 Arnold 变换对数据的嵌入顺序进行置乱，解决了同类隐写算法只能对载体图像进行顺序嵌入的问题，提高了载体图像中秘密信息的隐蔽性。由于 Arnold 变换属于本文算法的一部分，置乱嵌密顺序可以提高秘密信息的隐蔽性，其实间接的也提高了算法的安全性。算法在提取秘密信息时要进行一定次数 Arnold 变换，再进行无需原始载体的盲提取操作。然而在现实情况下，假如攻击者不知道图像进行了 Arnold 变换和非满嵌操作，却直接对图像进行顺序提取秘密信息，那么就得不到正确的秘密信息。调整载体图像的参数和 Arnold 变换置乱嵌入顺序这 2 种操作适合很多同类的图像隐写算法，并且这些操作可以提高隐写的隐蔽性和减少图像的嵌入失真度，也提高了算法的安全性。

2　Arnold 变换

Arnold 变换，俗称猫脸变换(cat mapping)，是由数学家 Arnold 在遍历理论的研究中提出来的一种变换。将 Arnold 变换[14]应用在数字图像上，就是通过像素坐标的改变而改变图像灰度值的布局。把数字图像看作一个矩阵，则经 Arnold 变换

后的图像会变得“混乱不堪”。本文中采用 Arnold 变换的目的是生成伪随机载体嵌入的位置，打乱嵌入顺序，使外部观察者在不知道 Arnold 变换的情况下，无法逆向分析出正确的秘密信息，提高了隐写的隐蔽性。Arnold 变换的定义为

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} n_1 & n_2 \\ n_3 & n_4 \end{pmatrix}^k \begin{pmatrix} x \\ y \end{pmatrix} (\mathrm{mod}\ n)$$
$$\begin{pmatrix} n_1 & n_2 \\ n_3 & n_4 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \tag{1}$$

其中，$\mathrm{mod}\, n$ 表示模运算，$x, y \in (1, 2, 3, \mathrm{L}\ , n-1)$ 是原始图像矩阵像素点的位置 x', y' 是经过 Arnold 变换后像素点的位置，k 是变换的次数。Arnold 变换具有周期性[15]，对不同的矩阵阶数 n，Arnold 变换有不同的周期。

3 基于 Arnold 变换的数字图像自适应隐写算法描述

本节分别介绍了嵌入秘密信息的过程和提取秘密信息的过程。首先把图像分成许多互相不重叠的 2×2 的四像素块，然后再使用 Arnold 变换置乱图像的嵌入顺序，最后根据门限阈值划分像素块的等级，由不同的等级像素块中像素值的最大变化值（即非满嵌最佳参数）决定了嵌入秘密信息的最大范围，进而自适应地修改像素块像素值的大小，从而达到提高隐写隐蔽性和减少图像嵌入失真度的目的。

3.1 嵌入秘密信息

Step1 把秘密信息的长度 t，划分像素块等级的门限阈值 $D=15$，非满嵌最佳参数 T^*（请见 Step4）以及控制 Arnold 变换的参数 n_0, n_1, n_2, n_3, k 全部以二进制秘密信息的形式，使用 LSB 隐写算法嵌入到载体图像矩阵中的前 2 行。嵌入顺序是从第 1 行的第 1 个像素点依次从左向右、从上往下逐个嵌入嵌满前面 2 行，长度不足就补零（如图 1 所示）。

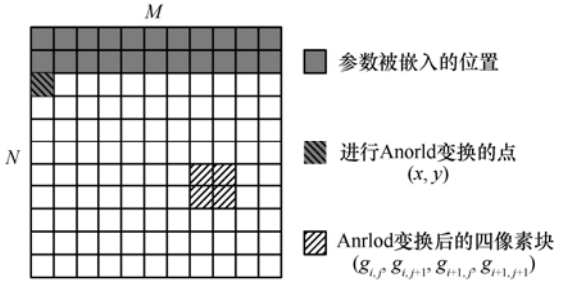


图 1 Arnold 变换

Step2 对载体图像中坐标为 $(x=1, y=3)$ 的点进行 k 次 Arnold 变换得到 (x', y')，然后根据 $i=2x'+1$，$j=2y'-1$ 求出需要嵌密的四像素块 $(g_{i,j}, g_{i,j+1}, g_{i+1,j}, g_{i+1,j+1})$（如图 1 所示）。后面的像素点依次从左向右、从上往下，逐个进行 k 次 Arnold 变换求出其对应的四像素块位置以便逐个进行嵌密，Arnold 变换计算公式如下

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} n_1 & n_2 \\ n_3 & n_4 \end{pmatrix}^k \begin{pmatrix} x \\ y \end{pmatrix} (\mathrm{mod}\ n)$$
$$1 \leqslant x \leqslant \frac{M}{2}, 1 \leqslant y \leqslant \frac{N}{2} \tag{2}$$

Step3 把整张载体图像划分成很多个互相不重叠的 2×2 的四像素块 $(g_{i,j}, g_{i,j+1}, g_{i+1,j}, g_{i+1,j+1})$。四像素块 $(g_{i,j}, g_{i,j+1}, g_{i+1,j}, g_{i+1,j+1})$ 对应的像素值为 (y_0, y_1, y_2, y_3)，找出像素值 (y_0, y_1, y_2, y_3) 中的最小值 $y_{\min}$，然后计算出这 4 个像素值的平均差值 d，计算公式如下

$$d = \frac{1}{3}\sum_{i=0}^{3}(y_i - y_{\min}) \tag{3}$$

根据门限阈值 $D=15$ 和 d 的大小关系来区分该四像素块的等级。若 $d<D$，则该四像素块属于低等级像素块，本文令低等级像素块 4 个像素值在嵌密过程中的最大变化值为 $lk_i (0 \leqslant i \leqslant 3)$。若 $d \geqslant D$，则该四像素块属于高等级像素块，本文令高等级像素块 4 个像素值在嵌密过程中的最大变化值为 $hk_i (0 \leqslant i \leqslant 3)$。$lk_i$ 和 hk_i 的大小是由 Step4 非满嵌最佳参数 T^* 决定的。

Step4 为了方便后面的计算，本文把像素块中 4 个像素值的最大变化值统一为 δ_i，即 $\delta_i = lk_i$ 或 $hk_i (0 \leqslant i \leqslant 3)$。通过该像素块中的像素值 y_i 和 $\varphi_i (\varphi_i = 2\delta_i + 1)$ 来计算编码函数值 F，计算公式如下

$$F = (y_0 \bmod \varphi_0) + (y_1 \bmod \varphi_1)\varphi_0 + (y_2 \bmod \varphi_2)\varphi_1\varphi_0 + (y_3 \bmod \varphi_3)\varphi_2\varphi_1\varphi_0 \tag{4}$$

从二进制秘密信息流中顺序读取 $n = \lfloor \mathrm{lb}(\varphi_0\varphi_1\varphi_2\varphi_3) \rfloor$ bit 的秘密信息，然后把二进制秘密信息转换成十进制数值 S。计算出十进制数值 S 和编码函数值 F 的差值 T 为

$$T = S - F \tag{5}$$

若 $T=0$，代表秘密信息已经被嵌入到该四像素块中，则该像素块中的 4 个像素值不需要修改，

再通过 Step2 按顺序找出下一个新的四像素块，把新的四像素块进行同样的计算。若 $T \neq 0$，代表秘密信息还没被嵌入到该四像素块中，则需要修改 4 个像素值的大小。

Step5　根据十进制数值 S，像素值 y_i 和 φ_i 计算出像素值 y_i 的修改幅度 R_i，计算公式如下

$$\begin{cases} R_0 = S \bmod \varphi_0 - y_0 \bmod \varphi_0 \\ R_1 = \left\lfloor \dfrac{S}{\varphi_0} \right\rfloor \bmod \varphi_1 - y_1 \bmod \varphi_1 \\ R_2 = \left\lfloor \dfrac{S}{\varphi_0\varphi_1} \right\rfloor \bmod \varphi_2 - y_2 \bmod \varphi_2 \\ R_3 = \left\lfloor \dfrac{S}{\varphi_0\varphi_1\varphi_2} \right\rfloor \bmod \varphi_3 - y_3 \bmod \varphi_3 \end{cases} \tag{6}$$

其中，$0 \leqslant R_i \leqslant \varphi_i - 1, 0 \leqslant i \leqslant 3$。

把像素值 y_i 的修改幅度 R_i 控制在最大变化值 δ_i 以内，计算公式如下

$$R_i' = \begin{cases} R_i - \varphi_i \text{，} R_i > \delta_i \\ R_i + \varphi_i \text{，} R_i < -\delta_i \\ R_i \quad \text{，其他} \end{cases} \tag{7}$$

得到修改后的像素值 $y_i' = y_i + R_i', 0 \leqslant i \leqslant 3$。

Step6　对该四像素块执行再调整操作，保证隐写前后四像素块的平均差值在相同的等级。首先令 $y_i'' = y_i' + r\varphi_i$，$r \in \{0,1,-1\}$，$0 \leqslant i \leqslant 3$，然后找出 y_i'' 中的最小值 $y_{\min}''$，最后计算出像素值的平均差值 d'，计算公式如下

$$d' = \frac{1}{3}\sum_{i=0}^{3}\left(y_i'' - y_{\min}''\right) \tag{8}$$

搜索合适的 $(y_0'', y_1'', y_2'', y_3'')$，使之同时满足下列 3 个条件：

1) d_i' 和 d_i 在隐写前后属于相同等级;

2) $\sum_{i=0}^{3}(y_i'' - y_i)^2$ 的值最小;

3) $0 \leqslant y_i'' \leqslant 255$。

四像素块嵌密后的最终像素值为 $(y_0'', y_1'', y_2'', y_3'')$。

循环执行上述步骤直到所有的二进制秘密信息都被嵌入到载体图像中。但最后一个四像素块在嵌入时，可能会出现剩下的秘密信息长度不足 $n = \left\lfloor \mathrm{lb}\left(\varphi_0\varphi_1\varphi_2\varphi_3\right) \right\rfloor$ bit 的问题，则此时需要补零直到长度达到 n bit。这时所有的二进制秘密信息都被嵌入到了载体图像中，可以结束嵌入操作，算法流程如图 2 所示。

3.2　提取秘密信息

Step1　对载体图像的前 2 行进行 LSB 提取操作，提取出来的秘密信息为参数 $t, D, T^*, n_0, n_1, n_2, n_3, k$ 的二进制比特流。

Step2　对载体图像中坐标为 $(x=1, y=3)$ 的点进行 k 次 Arnold 变换得到 (x', y')，然后根据 $i = 2x' + 1$，$j = 2y' - 1$ 求出需要分析的四像素块。后面的像素点依次从左向右、从上往下，逐个进行 k 次 Arnold 变换求出其对应的四像素块位置以便逐个进行分析，Arnold 变换计算公式由嵌入秘密信息过程的 Step2 可知。

Step3　求出的四像素块为 $(g_{i,j}, g_{i,j+1}, g_{i+1,j}, g_{i+1,j+1})$ 其对应的像素值为 $(y_0'', y_1'', y_2'', y_3'')$，找出像素值 $(y_0'', y_1'', y_2'', y_3'')$ 中的最小值 $y_{\min}''$，然后计算出这 4 个像素的平均差值 d'，计算公式如下

$$d' = \frac{1}{3}\sum_{i=0}^{3}\left(y_i'' - y_{\min}''\right) \tag{9}$$

根据门限阈值 $D=15$ 和 d' 的大小关系来判断该四像素块的等级。若 $d' < D$，则该四像素块属于低等级像素块。若 $d' \geqslant D$，则该四像素块属于高等级像素块。通过像素块的等级本文可以得出像素值的最大变化值 δ_i。

Step4　用该四像素块中的像素值 y_i'' 和 $\varphi_i\left(\varphi_i = 2\delta_i + 1\right)$ 来计算编码函数值 F，计算公式如下

$$F = \left(y_0'' \bmod \varphi_0\right) + \left(y_1'' \bmod \varphi_1\right)\varphi_0 + \left(y_2'' \bmod \varphi_2\right)\varphi_1\varphi_0 + \left(y_3'' \bmod \varphi_3\right)\varphi_2\varphi_1\varphi_0 \tag{10}$$

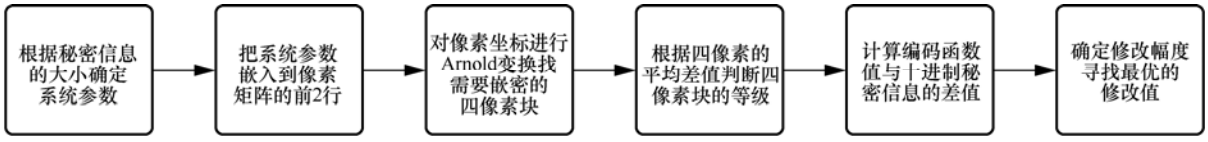


图 2　嵌密算法流程

将十进制编码函数值 F 转换为长度 $n=\left\lfloor \mathrm{lb}\left(\varphi_0\varphi_1\varphi_2\varphi_3\right)\right\rfloor$ 的二进制比特流即为秘密信息。循环执行上述步骤，直到所有的秘密信息提取完成。对于最后一个像素块，本文在提取时要根据 Step1 提取出的二进制秘密信息长度 t，对其进行截取操作。至此，所有秘密信息均准确提取成功，提取算法流程如图 3 所示。

4　非满嵌最佳参数的选择方法

嵌密图像的图像失真度是用峰值信噪比(PSNR, peak signal to noise ratio)来估计。对于一幅 $M\times N$ 矩阵大小的图像，*PSNR* 的值参照下面的定义为

$$PSNR=10\lg\frac{255\times 255MN}{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(p_{i,j}-q_{i,j}\right)^2} \tag{11}$$

其中，$p_{i,j}$ 和 $q_{i,j}$ 分别代表载体图像和嵌密图像的 i 行 j 列的像素值。

嵌密后图像的失真度由 $\sum_{i=1}^{M}\sum_{j=1}^{N}\left(p_{i,j}-q_{i,j}\right)^2$ 决定，所以本文使载体图像的嵌入修改位置越少越好，即让载体图像达到非满嵌，同时也要保证 $\sum_{i=1}^{M}\sum_{j=1}^{N}\left(p_{i,j}-q_{i,j}\right)^2$ 越小越好，即让隐写前后图像所有像素值的最大变化值越小越好。为了找出最佳的像素值最大变化值，本文令本算法中低等级像素块的 4 个像素值的最大变化值 k_0,k_1,k_2,k_3 和高等级像素块的 4 个像素值的最大变化值 k_4,k_5,k_6,k_7，即不同等级像素块的初始参数为 $T_0=(k_0,k_1,k_2,k_3,k_4,k_5,k_6,k_7)$，然后，根据载体图像在初始参数下的满嵌容量 m 和秘密信息长度 t 的大小关系，调整初始参数 T_0，找出最佳参数 T^*。

当 $m>t$ 时，则此时的最佳参数就是 $T^*=T_0$。当 $m\leqslant t$ 时，则本文就要扩大载体图像的满嵌容量即让 T_0 变大，由于 $\sum_{i=1}^{M}\sum_{j=1}^{N}\left(p_{i,j}-q_{i,j}\right)^2$ 决定了 *PSNR*，所以在扩大满嵌容量的过程中不能只让任何一个 $k_i\left(0\leqslant i\leqslant 7\right)$ 变得特别大，本文将 k_i 依次均匀地变大。由于像素值都是整数，因此 k_i 每变化一次的值至少为 1。本文首先让 T_0 中的 k_7 加 1 且后面的 k_i 也逐个进行加 1 操作一直到 k_0，然后再循环返回到 k_7 继续逐个进行加 1，并且每加一次 1 的同时计算 m 和 t 的大小关系，直到 $m>t$ 时，本文就停止加 1。此时的参数由 T_0 变为 T_1，于是本文得到的最佳参数为 $T^*=T_1$。

最后可以得到

$$T^*=\left(lk_0,lk_1,lk_2,lk_3,hk_0,hk_1,hk_2,hk_3\right)$$

5　实验结果分析

5.1　固定参数时载体图像的 *PSNR* 实验结果

本节将给出在固定参数 T 下载体图像的 *PSNR*。实验中以 10 幅大小为 512×512 的经典灰度图像作为载体（如图 4 所示），秘密信息是由伪随机数发生器生成的一串伪随机数字，然后以随机非

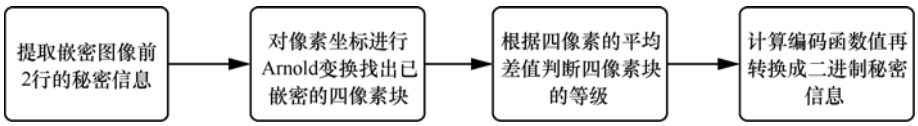


图 3　提取算法流程

(a) Elaine　(b) Lena　(c) Baboon　(d) Peppers　(e) Toys

(f) Girl　(g) Gold　(h) Barb　(i) Zelda　(j) Tiffany

图 4　10 幅载体图片

满嵌的形式嵌入到载体中。用峰值信噪比来估计嵌密图像的图像失真度。*Capacity* 是嵌入容量即秘密信息的大小。*Percent* 表示嵌入容量与满嵌容量的比值即非满嵌比例。通过固定参数值 $T=(k_0,k_1,k_2,\mathrm{L}\ ,k_7)$ 对本文提出的基于 Arnold 变换的数字图像自适应隐写算法进行多组实验，首先分别求出 10 张图片在固定参数 T 下的 10 个满嵌容量及这 10 个满嵌容量的平均值，然后在图像中分别嵌入 $Percent=(10\%,20\%,\mathrm{L}\ ,90\%)$ 的秘密信息即嵌入容量，进而可以求出这 10 张图片在某个 *Percent* 下 10 组不同的 *PSNR* 值和嵌入容量 *Capacity*，最后分别求出 10 个不同 *PSNR* 值的平均值和 10 个不同嵌入容量 *Capacity* 的平均值作为实验结果，如表 1 所示。

表 1　本文算法在不同固定参数 *T* 下的实验结果

(2,2,3,3,4,4,5,5)和 *D*=15			(3,3,4,4,5,5,6,6)和 *D*=15		
Percent	*Capacity*/bit	*PSNR*/dB	*Percent*	*Capacity*/bit	*PSNR*/dB
10%	70 225	52.39	10%	75 043	50.03
20%	139 876	49.41	20%	150 119	47.01
30%	209 764	47.64	30%	225 021	45.25
40%	279 841	46.40	40%	300 053	44.00
50%	350 464	45.45	50%	382 616	42.96
60%	419 904	44.66	60%	450 234	42.25
70%	490 000	44.00	70%	525 328	41.57
80%	559 504	43.42	80%	600 628	41.00
90%	630 437	42.90	90%	675 209	40.48
100%	671 015	42.63	100%	747 637	40.04

根据实验结果可以看出，当固定参数 T 和 D 一定时，如果载体图像嵌入的秘密信息变多即非满嵌比例变大，那么嵌密图像的 *PSNR* 值会变小。当 D 和非满嵌比例一定时，如果固定参数 T 中的 k_i 变小，那么载体图像的满嵌容量会变小，但嵌密图像的 *PSNR* 值变大。所以本文在传输秘密信息的过程中以满足隐写者的需求为前提，选择最佳的参数 T^*，使图像的满嵌容量刚好大于秘密信息的长度让载体图像达到非满嵌，以此来减小嵌密图像的失真度。

5.2　不同图片的最佳参数 T^* 的实验结果

为了进一步得出不同图片的最佳参数 T^*，本节的实验以 Elaine、Lena、Baboon、Peppers、Zelda 这 5 幅大小为 512×512 的经典灰度图像作为载体（图 4 为测试的图像），秘密信息是由伪随机数发生器生成的一串伪随机数字，然后以随机非满嵌的形式嵌入到载体中。本文首先分别求出 5 张图像在初始参数 $T_0=(1,1,1,1,2,2,2,2)$, $D_{lh}=15$ 下的满嵌容量 m，然后根据满嵌容量 m 和秘密信息 t 的大小关系调整初始参数 T_0，找出最佳参数 T^*，而且用峰值信噪比来估计嵌密图像的图像失真度。假如本文要嵌入 410 000 bit 的秘密信息即 $t=410\,000$，对于不同图像的实验结果如表 2~表 6 所示。

表 2　Elaine 图像的实验结果

参数	满嵌容量 *m*/bit	*PSNR*/dB	跟 *t* 的大小关系	是否为最佳参数 *T**
(1,1,1,1,2,2,2,2)	418 303	48.70	大	是

表 3　Lena 图像的实验结果

参数	满嵌容量 *m*/bit	*PSNR*/dB	跟 *t* 的大小关系	是否为最佳参数 *T**
(1,1,1,1,2,2,2,2)	409 891	49.08	小	否
(1,1,1,1,2,2,2,3)	409 891	48.80	小	否
(1,1,1,1,2,2,3,3)	415 959	48.58	大	是

表 4　Baboon 图像的实验结果

参数	满嵌容量 *m*/bit	*PSNR*/dB	跟 *t* 的大小关系	是否为最佳参数 *T**
(1,1,1,1,2,2,2,2)	480 355	47.01	大	是

表 5　Peppers 图像的实验结果

参数	满嵌容量 *m*/bit	*PSNR*/dB	跟 *t* 的大小关系	是否为最佳参数 *T**
(1,1,1,1,2,2,2,2)	406 102	49.25	小	否
(1,1,1,1,2,2,2,3)	406 102	49.06	小	否
(1,1,1,1,2,2,3,3)	410 907	48.88	大	是

表 6　Zelda 图像的实验结果

参数	满嵌容量 *m*/bit	*PSNR*/dB	跟 *t* 的大小关系	是否为最佳参数 *T**
(1,1,1,1,2,2,2,2)	399 823	49.51	小	否
(1,1,1,1,2,2,2,3)	399 823	49.38	小	否
(1,1,1,1,2,2,3,3)	402 535	49.26	小	否
(1,1,1,1,2,3,3,3)	402 535	49.13	小	否
(1,1,1,1,3,3,3,3)	405 247	49.00	小	否
(1,1,1,2,3,3,3,3)	467 816	47.57	大	是

根据实验结果可以看出图像 Elaine 和 Baboon 的最佳参数是 $T^*=(1,1,1,1,2,2,2,2)$，而图像 Lena 和 Peppers 的最佳参数是 $T^*=(1,1,1,1,2,2,3,3)$、图像 Zelda 的最佳参数是 $T^*=(1,1,1,2,3,3,3,3)$。于是本文对于不同的图像，最佳参数 T^* 是不同的。所以本文在传输秘密信息的过程中，在满足隐写者的需求和最小化图像嵌入失真度的前提下找出最佳参数 T^*。

6 结束语

本文通过调整图像参数和Arnold变换这2种操作解决了载体图像在以往同类算法中只能顺序满嵌的问题，提高了算法的安全性，首先根据秘密信息的大小选择最佳的参数，增强了隐写的灵活性使图像达到非满嵌，减少了图像的嵌入失真度，再使用 Arnold 变换对数据的嵌入顺序进行置乱，提高了隐写的隐蔽性。由于 Arnold 变换是算法的一部分，进而也提高了算法的安全性。下一步本文将对图像隐写算法进行更加深入的研究，希望借助这 2 种操作可以适用很多同类算法的特性，设计出更加好的图像自适应隐写算法，使隐写更加隐蔽。

参考文献：

[1] ANDERSON R J, PETITCOLAS F A P. On the limits of steganography[J]. IEEE Journal on Selected Areas in Communications, 1998, 16(4): 474-481.

[2] PETITCOLAS F, ANDERSON R，KUHN M. Information hiding—a survey[J]. Proc IEEE, 1999, 87(7): 1062-1078.

[3] LANGELAAR G C, SETYAWAN L, LAGENDIJK R L. Watermarking digital image and video data: a state-of-the-art overview[J]. IEEE Signal Processing Magazine, 2000, 17(5): 20-46.

[4] LU C S， LIAO H Y. Multipurpose watermarking for image authentication and protection[J]. IEEE Transactions on Image Processing, 2001, 10(10): 1579-1592.

[5] PROVOS N,HONEYMAN P. Detecting steganographic content on the Internet[C]//Network and Distributed System Security Symposium. San Diego, USA, c2002: 1-11.

[6] WANG H, WANG S. Cyber warfare: steganography vs. steganalysis[J].Communications of the ACM, 2004, 47(10): 76-82.

[7] COX I, MATTHEW M, BLOOM J, et al. Digital watermarking and steganography[M/OL]. Morgan Kaufmann, http://www.mkp.com.

[8] UNG K H, High-capacity steganographic method based on pixel-value differencing and LSB replacement methods[J]. The Imaging Science Journal, 2010, 58(4): 213-221.

[9] WU D C, TSAI W H. A steganographic method for images by pixel-value differencing[J]. Pattern Recognition Letters, 2003, 24(9): 1613-1626.

[10] WU H C, WU N L, TSAI C S, et al. Image steganographic scheme based on pixel-value differencing and LSB replacement methods[J]. IEEE Proceedings Vision,Image, and Signal Processing, 2005, 152(5): 611-615.

[11] WANG C M, WU N L, TSAI C S, et al. A high quality steganographic method with pixel-value differencing and modulus function[J]. Journal of Systems and Software, 2008, 81(1): 150-158.

[12] SUN H M, WENG C Y, LEE C F, et al. Anti-forensics with steganographic data embedding in digital images[J]. IEEE Journal on Selected Areas in Communications, 2011, 29(7): 1392-1403.

[13] LIAO X, WEN Q，ZHANG J. A steganographic method for digital images with four-pixel differencing and modified LSB substitution[J]. Journal of Visual Communication and Image Representation, 2011, 22(1): 1-8.

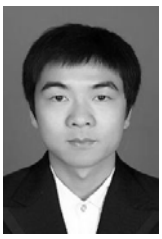
[14] 邹建成, 铁小匀. 数字图像的二维 Arnold 变换及其周期性[J]. 北方工业大学学报, 2000, 12(1): 10-14.
QU J C, TIE X J. Arnold transform two-dimensional digital images and periodicity[J]. Journal of North China University of Technology, 2000, 12(1): 10-14.

[15] DING W, YAN W Q, QI D X. Digital image information hiding technology and its application based on scrambling and amalgamation [J]. Journal of Image and Graphics, 2000, 5(8): 644-649.

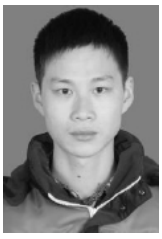
作者简介：

李琪（1989-），男，湖北安陆人，湖南大学硕士生，主要研究方向为信息隐藏。

廖鑫（1985-），男，湖南长沙人，博士，湖南大学讲师、硕士生导师，主要研究方向为多媒体信息安全。



屈国庆（1990-），男，河南信阳人，南京大学硕士生，主要研究方向为信息大数据应用与云计算。



陈国永（1989-），男，河南信阳人，湖南大学硕士生，主要研究方向为信息隐藏。

杜蛟（1978-），男，湖北英山人，博士，河南师范大学讲师，主要研究方向为密码学与应用数学。