(t,n)门限图像隐藏技术的实施与改进

梅 杨

(暨南大学 信息科学技术学院，广东 广州 610532)

摘 要：在前人研究的基础上，对基于 Shamir 的(t,n)门限的图像隐藏算法提出了新的改进，并且引入了奇偶校验，这样就可以分辨被损坏的图像，从而使隐藏算法具有更强的鲁棒性。

关键词：隐藏；门限；奇偶校验

中图分类号：N **文献标识码**：A **文章编号**：1674-7720(2011)04-0035-02

Practice and improvement of image hiding based on (t, n) threshold

Yang Mei

(College of Information Science and Technology, Jinan University, Guangzhou 610532, China)

Abstract: Based on the previous studies, this paper has proposed new improvements on image hiding algorithm according to Shamir's (t, n) threshold. In addtion, with the introduction of odd-even checking, which can identify the damaged images, the hiding algorithm therafore becomes more robust.

Key words: hiding; threshold; odd-even checking

信息隐藏是指在设计和确定模块时，使得一个模块内包含的特定信息(过程或数据)，对于不需要这些信息的其他模块来说是透明的。图像隐藏则是信息隐藏的一种。在现实的世界中，人类获取外界信息主要靠眼睛，而这就可以将这些信息看成是一幅幅的图像。对于一些非常重要的信息，不论是在保存还是传输过程中，保证其安全性则显得尤为重要。传统的做法就算运用密码学中的各种算法对图像数据进行加密[1-3]，虽然能保证图像数据一定的安全性，但是其效率一般较低，且对目标图像进行加密，也就暴露了重要数据之所在，更容易引起一些不安因素。相比之下，图像隐藏方法就会好很多。而本文将要讨论的图像隐藏方法基于(t,n)门限，将要隐藏的目标图像通过一定的算法将其信息隐藏到 n 幅子图中，只要得到这些子图中的 t 幅就可以恢复出原图，而所获得的子图数只要少于 t 幅就无法恢复出原图。在图像的隐藏方法中运用(t,n)门限方案是图像安全领域的创新，是近些年才开始兴起的。在此之前，有一些学者做了相应的研究[4-5]。本文给出一个全面的隐藏方案以及具体实施过程，并将最终与前面研究者的方法进行一些对比，最后给出相应的结论。

1 BLAKLEY[6] SHAMIR[7]的(t,n)门限方案

SHAMIR 的(t,n)门限方案是将一个密钥分解为 n 个部分的子密钥，然后再将这些子密钥分别交给 n 个人保管，该分解算法对于确定的整数 $t(0<t\leqslant n)$ 满足如下两个条件：

(1)原始密钥可以由任意 $r(t\leqslant r\leqslant n)$ 个人的合作获得；

(2)任意 $r(0<r<t)$ 个人都无法获得原始密钥的任何信息。

这里，t 通常称为方案的门限或阈，或者称为重构密钥所必须的法定人数.

SHAMIR 方案基于如下众所周知的事实：取 t 个不同值 $x_0,x_1,\cdots,x_{t-1}$ 的集并在二维平面上取 t 个点：$(x_0,y_0),(x_1,y_1),\cdots,(x_{t-1},y_{t-1})$，则有唯一的 $t-1$ 次多项式通过这 t 个点，即有：

$$y_i=f(x_i)$$

显然，由$(x_0,y_0),(x_1,y_1),\cdots,(x_{t-1},y_{t-1})$可以列出如下的方程组，从而确定唯一的 $a_0,a_1,\cdots,a_{t-1}$。

$$\begin{cases} y_0=\sum_{i=0}^{n-1} a_i x_0^i \\ \vdots \\ y_{n-1}=\sum_{i=0}^{n-1} a_i x_{n-1}^i \end{cases} \quad (1)$$

这样，只要有了 n 组对应的(x,y)值，就可以完全解

出这个方程组。

2 拉格朗日插值方法

设有如下方程:

$$f(x)=[a_1x_1+a_2x_2+\cdots+a_{t-1}x_{t-1}+K]\bmod p \tag{2}$$

其中，$a_1,a_2,\cdots,a_{t-1}$ 都是小于 p 的随机数，K 为常数，p 为一大素数。

设 G 为满足方程的一组点集$[(x_1,f(x_1)),(x_2,f(x_2)),\cdots,(x_n,f(x_n))]$,$T$ 为含有 t 个点$(x_1,f(x_1)),(x_2,f(x_2)),\cdots,(x_t,f(x_t))$的 G 的子集。T 中所有的点都可以分别通过拉格朗日方程来计算 K。

$$K=f(0)=\sum_{x_i\in T}(L_i\times f(x_i)) \tag{3}$$

这里 $L_i=\prod_{x_i,x_j\in T,x_i\neq x_j}-x_j/(x_i-x_j)$

对于一个 $t-1$ 次的拉格朗日插值多项式而言，至少需要 G 中的 t 个点才能够恢复和重建 K。

3 具体算法以及详细实施过程

3.1 图像的隐藏

首先选取一幅欲隐藏的 8 位 256 色的灰度图像，称之为目标图像，然后选取若干幅(这里假设为 n 幅)普通图像，称之为影子图像。把目标图像信息通过一定的方式保存到这些影子图像中，从而达到隐藏的目的。这些影子图像都是 24 位的彩图，且图像大小、长宽都不小于目标图像。

对于目标图像中的每一个像素的像素值 $M(x,y)$(x、y 分别代表该像素点位于目标图像中的位置)，根据以下方程:

$$f(u)=[a_1u_1+a_2u_2+\cdots+a_{t-1}u_{t-1}+M(x,y)]\bmod p \tag{4}$$

其中，$a_1,\cdots,a_{n-1}$ 都是小于 p 的随机数，p 可取 253。

对于目标图像中的每一个像素都作此变化，只是不同的影子图像对应的一个数字 u_i 不同。这样，把经过计算后的值 $f(u_i)$ 变成 8 位二进制的值填入到每幅影子图像对应像素的每种颜色分量的最后 3 位中。由于改变的是 R、G、B 颜色分量的末 3 位，对于整幅图像的改变从肉眼一般是无法辨认出来的，因此起到了很好的欺骗作用。图 1 所示为两幅随机改变 R、G、B 每种颜色分量最后 3 位后所得图像前后的对比。

图 1 随机改变 R、G、B 每种颜色分量末 3 位后图像的对比

经过以上处理后，由于只填充了 8 位，n 幅影子图像的低位还会有一位像素的空余，对于这一位像素，填入一个奇偶校验位，这样就可以检测出那些在传送过程中可能受到破坏的子图。对于这样的子图放弃不用，从而可以防止由于像素受到破坏而对后面解方程组造成干扰。

3.2 目标图像的恢复

在获得 n 幅影子图像中的 t 幅后，首先判断每一个奇偶校验位是否正确，然后可以就每一位像素组成一个方程组:

$$\begin{cases}f(u_1)=[a_1u_1+a_2u_{12}+\cdots+a_{t-1}u_{1(t-1)}+M(x,y)]\bmod p\\ \vdots\\ f(u_t)=[a_1u_{t1}+a_2u_{t2}+\cdots+a_{t-1}u_{t(t-1)}+M(x,y)]\bmod p\end{cases} \tag{5}$$

可以通过拉格朗日插值法求解出该方程组中的 $M(x,y)$，这样，求解完每一个像素相对应的一个方程组后就可以得到原目标图像所有像素的像素值，目标图像就得以恢复。

4 算法的改进

由于隐藏图像时经常会遇到比较大的图像，因此在逐个隐藏目标图像的每个像素时，算法的效率会显得很重要。如果算法的效率低、时间复杂度高，整个隐藏算法所用的时间就会比较长。为此，特提出了以下改进方案:

将每幅图像按行分成 $1\times t$ 个像素的小块，每个块中的像素值作为式(5)的序数 $a_0,a_1,\cdots,a_{t-1}$($M(x,y)$看作 a_0)的值，然后针对所有的图像给出一个对外保密的未知数 u 值序列。这样，每解一次方程组(5)时就可以一次解出 t 个目标图像像素的值，算法的时间复杂度几乎下降为原来的 $1/t$。

在影子图像的 9 个最低位被填充了 8 位后，还剩下一位空余，可以填入奇偶校验位，这样就可以检验出影子图像在传输过程中是否被损坏，从而不会因为损坏后被改变的像素值而计算出错误的目标图像像素值。

本文提出了新的算法思路，从而大幅加快了隐藏算法的速度。在处理器酷睿双核 2.0 GHz 内存 2.0 GB，VC6.0 平台下实验，CHEN Chang Chin[4]以及陈继超[7] 等人的算法完成一幅 1 000×1 000 图像的隐藏需要时间大概为1.4 s，本文的方法平均约只需要 0.5 s，速度的提升非常明显；其次，提出了简单易行的奇偶校验方法，从而对算法的鲁棒性有了很大的提高。因此，本文提出的基于门限方案的图像隐藏方法高效、强壮且具有很强的实践性。

参考文献

[1] BOURBAKITS N, ALEXOPOULOUS C. Picture data encryption using scan patterns[J]. Pattern Recognition ,1992,25(6):567-581.

[2] CHANG C C, HWANG M S, CHEN T S. A new encryption algorithm for image cryptosystems[J]. Journal of Systems and Software,2001,58:83-91.

[3] KUO C J. Novel image encryption techniques and its applications in progressive transmission[J].Journal of Electronic

Imaging,1993,2(4):345-351.
[4] Chen Changchin, CHANG Liniuon. A new (t,n) threshold image hiding scheme for sharing a secret color image[C]. Proceedings of ICCT2003[C].Beijing :Press of BJUPT,2003.
[5] 陈继超,谢柯.基于(t,n)门限的可防欺骗的图像隐藏方案[J].计算机技术与发展,2006,16(9):208-209,212.
[6] BLAKLEY G R. Safeguarding cryptographic keys[C]. Proceedings of the National Computer Conference.US:American Federation of Information Procession Societies,1979:242-268.
[7] SHAMIR A. How to share a secret[J]. Communication of ACM, 1979,22:612-613.

(收稿日期:2011-01-10)

作者简介:
梅杨,男,1985年生,硕士研究生,主要研究方向:图形图像。