基于 Shamir(t,n) 门限方案的数字图象信息分存*

黄煜森[1)] 齐东旭[1.2)]

(1) 澳门科技大学信息科技学院,中国澳门,Email: wioksam <sam321@macau.ctm.net>
2) 北方工业大学 CAD 研究中心,100041,北京石景山)

摘 要 本文基于密码学中的 Shamir(t,n) 门限方案研究数字图象存储与传输中的信息分存方法,主要结果是:对于给定的秘密图象 A,发送者可以从任意选择的 k 幅($k=1,2,3,\cdots$) 同样尺寸图象出发,生成作为伪装的 N 幅图象($N>k$);接收者可以利用这 N 幅图象中 $k+1$ 幅恢复图象 A.本文介绍了利用拉格朗日插值算法给出的分存原理,并提出一类基于射影几何学的分存算法.最后给出了实验图例和视频作品例子说明研究方法的合理性.

关键词 数字图象;信息分存;拉格朗日插值;射影几何;直线束

分类号 TP391.41

1 引言

众所周知,通信安全保密问题的研究十分重要.经典密码学与现代密码学在通信安全保密方面有丰富的理论研究结果,并有成功的应用[1].近年来,有关图形图象的信息安全引起特别的关注,其中数字图象信息隐藏是解决信息安全保密问题的重要内容.

图象信息隐藏(Steganography)是90年代中期以来新兴的研究课题,在国际上连续召开学术会议[2,3].之所以受到重视,是因为数字图象信息隐藏在诸多领域中有非常重要的应用,如机密图象数据的存储、互联网上视频信息的安全传输、货币及证券的防伪等.这一研究在数字产品的版权和著作权的保护,以及基于数字信息的法律取证方面有着非常重要的意义.目前,研究的主要内容有多媒体数字水印技术,图象信息分存、置乱和加密等[3,4,5].

视觉信息占信息总量的大部分,可以说图形图象(诸如地图、照片、电影等)是无处不在的.人们把可视数据存放在计算机里,或者在互联网上传输过程中,有时必须考虑图形图象信息的安全保密.传统密码学和现代密码学,主要针对文本的加密与解密算法的研究.图形图象信息的处理,虽然与文本文件在本质上是一致的,但由于图形图象信息的特殊性,使得对它的加密处理必须有特别的考虑.这个特殊性,首先表现在数据量巨大,简单地从密码学移植过来的算法,往往事倍功半.另一方面,表达图象信息的数据,通常都有相关性,这一特点又是文字信息所不具备的.我们基于这样的认识,开展了数字图象信息的安全保密算法的探索.

分存是图象信息安全处理的重要内容,也是图象信息隐藏的主要方法之一.一般而言,图象分存问题可以描述为:将图象信息分为具有一定可视效果的 n 幅图象,这些图象称为子图象,这些子图象之间没有互相包含关系.如果知

收稿日期:2002-12-03
* 国家自然科学基金(60133020)及国家973(G1998030608)资助项目
* 论文曾在澳门2002年科技研讨会上宣读.
第一作者简介:黄煜森,硕士研究生.主要研究方向:数字图象处理、信息隐藏、数字水印技术.

道图象信息中的 $m(m\leqslant n)$ 幅子图象，则该图象可以得到恢复，如果图象信息少于 $m(m\leqslant n)$ 幅，则图象无法得到恢复.

图象分存的最大特点就是可以做到分存后所得到的子图象仍然是可视的；丢失子图象中的若干幅并不影响图象的恢复，从而增强了图象信息的安全性，减弱了窃取原始图象的可能性[7,8,9].

图象分存不同于图象处理中的 Morphing 方法，Morphing 方法通过两幅图象之间的颜色和位置插值来生成子图象，子图象来源于原始的两幅图象，考虑的是所生成图象的连续视觉效果；而图象分存生成的子图象来源于多幅图象的信息，考虑的是被分存图象的信息安全问题. 就图象的恢复而言，通过 Morphing 方法生成的有限幅子图象，不一定能恢复出 Morphing 前的原始图象；而通过图象分存所生成的子图象和相应的分存算法一定能恢复出分存前的原始图象.

本文研究彩色图象存储与传输中的信息分存方法，主要结果是：对于给定的秘密图象 A，发送者可以从任意选择的 k 幅 $(k=1,2,3\cdots)$ 同样尺寸图象出发，生成作为伪装的 N 幅图象 $(N>k)$；接收者可以利用这 N 幅图象中 $k+1$ 幅恢复图象 A. 为了说明本文的结果，首先给出如下图例，该图例是作者在 PC 机上编程实现的.

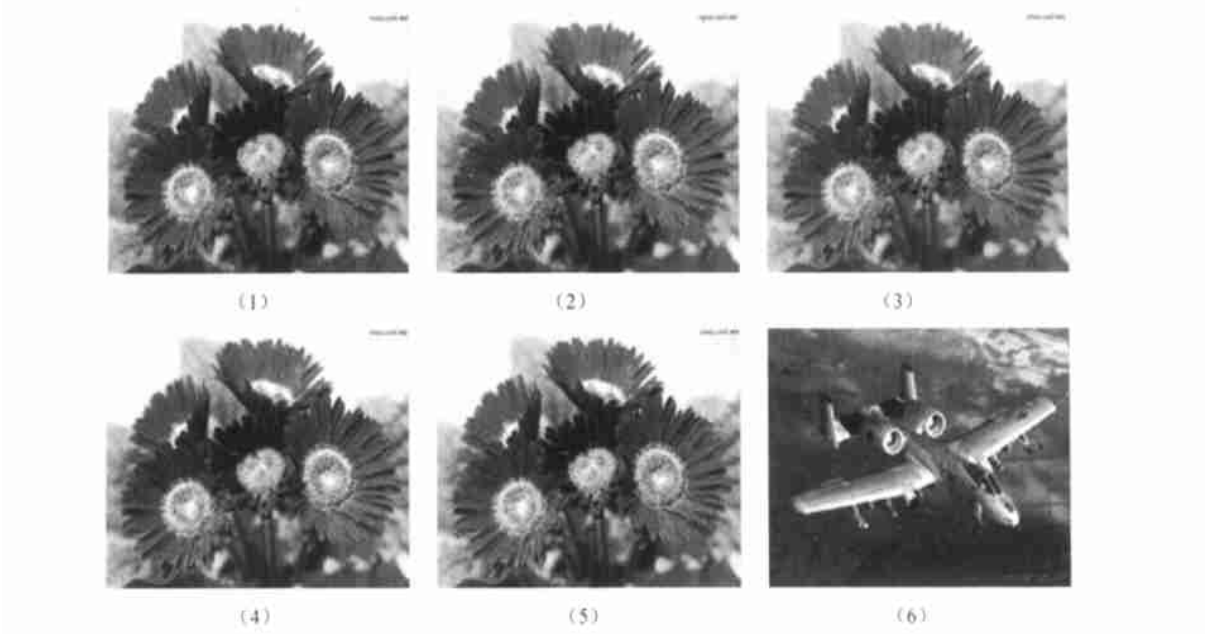

图 1 数字图象信息分存图例

图 1 的前 5 幅是很平常的图象，它们看起来似乎相同. 只要在这 5 个图象中，有任意 2 个，我们就可以通过本文的算法，计算出图(6). 事实上，这 5 个图象内含有某个保密图象(6)的完整信息. 事先为了生成它们，必须用原始图象(6)，但是，一旦生成了 5 个图象之后，缺少其中任何不超过 3 幅都不影响图象(6)的重构. 这里要指出，图 1 的前面 5 幅图象看似相同，事实上是各不相同的，只不过人的视觉能力不足以分辨出它们的极其细微的差别.

2 Shamir 的 (t,n) 一门限方案

Shamir 的 (t,n) 门限方案是将一个密钥分解为 n 部分(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 通常成为方案的门限或阀,或者称为重构秘密所必须的法定人数,参见文献[1]和文献[6]. 经典插值理论中的 Lagrange 多项式表述为:给定 $n+1$ 个节点 $x_0<x_1<x_2<\cdots<x_n$ 的 n 次多项式 $L_n(x)$,满足条件 $L_n(x_j)=y_j, j=0,1,2,\cdots,n$,那么它可以写成

$$L_n(x)=\sum_{k=0}^{n} y_k \frac{\omega_{n+1}(x)}{(x-x_k)\,\omega'_{n+1}(x)}$$

其中

$$\omega_{n+1}(x)=\prod_{k=0}^{n}(x-x_k)$$

$$\omega'_{n+1}(x_k)=\prod_{i=0,i\neq k}^{n}(x_k-x_i)$$

$$k=0,1,2,\cdots,n$$

Shamir 基于 Lagrange 多项式的密钥分存方法指出,任意选取 $a_1,a_2,\cdots,a_n\in GF(q)$,构造多项式 $f(x)=a_0+a_1a+a_2x^2+\cdots+a_nx^n$,其中 a_0 是密钥. 令 a 是 $GF(q)$ 域的本原元素,作 $k_i=f(x_i)$, $i=0,1,\cdots,n$,称 k_i 为子密钥,交给合作者 A_i 保管. 如果 $n+1$ 个合作者分别提供了各自的子密钥以及各自的序号,那么,利用 Lagrange 插值多项式可以从 $f(0)=a_0$ 使密钥得以恢复. 而合作者不超过 n 个,则不足以确定多项式 $f(x)$,因而不能得到 $f(0)=a_0$. 这一原理性的做法,为数字图象的信息分存提供了启发[1].

应用高次拉格朗日多项式插值曲线做数字图象信息分存,数据量和计算量将增大. 此外,多项式次数的增高,会使计算过程产生数值不稳定的病态现象. 基于拉格朗日插值的方法适合于传统的密码学中的信息分存,但对于图象信息分存而言,其结果难令人满意. 由于以上原因,我们探讨动直线生成的有理隐式曲线对图象信息进行分存的途径.

3　直线束与一类有理函数曲线

本节讨论基于动直线与一类有理函数的数字图象信息分存方案.

在射影几何学中,直线常表示为 $aX+bY+cW=0$ 形式,其中 a, b 和 c 不全为零,(X,Y,W) 是笛卡儿坐标系中点的齐次坐标,有

$$(x,y)=\left(\frac{X}{W},\frac{Y}{W}\right)$$

记 P 为三元数组(X,Y,W), L 为三元数组(a,b,c). 则直线 L 表示为:

$$\{(X,Y,W)\mid L\cdot P=(a,b,c)\cdot(X,Y,W)=aX+bY+cW=0\}$$

由此看来,当且仅当 $P\cdot L=0$,点 P 位于直线 $L=(a,b,c)$ 上.

如果齐次坐标为变量 t 的函数,记 $P[t]=(X[t],Y[t],Z[t])$,它表示有理曲线

$$x=\frac{X[t]}{W[t]},\ y=\frac{Y[t]}{W[t]}$$

假定函数是下列形式:

$$X[t]=\sum X_i\phi[t]$$

$$Y[t]=\sum Y_i\phi[t]$$

$$Z[t]=\sum Z_i\phi[t]$$

其中 $\{\phi(t)\}$ 为给定的调配函数,上述方程定义了曲线 $P[t]=\sum P_i\phi[t]$. 给定点的序列 $P_i=(X_i,Y_i,W_i)$ 定义了一族曲线 $L[t]=(a[t],b[t],c[t])$,参见文献[10].

记直线族为 $a[t]x+b[t]y+c[t]=0$,考虑由 4 条直线 L_{00}, L_{01}, L_{10} 和 L_{11} 定义的曲线:

$$L_0[t]=L_{00}(1-t)+L_{01}t,$$

$$L_1[t]=L_{10}(1-t)+L_{11}t$$

这是圆锥曲线,并可以表示成有理 Bernstain-Bezier 曲线 $P[t]$的形式:

$$P[t]=L_0[t]\times L_1[t]$$

并且容易验证 $P[t]$为二次有理 Bezier 曲线,其控制顶点为:

$$P_0=L_{00}\times L_{10}$$

$$P_1=\frac{1}{2}(L_{00}\times L_{11}+L_{01}\times L_{10})$$

$$P_2=L_{01}\times L_{11}$$

同拉格朗日插值方法类似,在简单图象分存中,可以选择两个固定点,让秘密图象和公开图象的参数在一定的范围内变化,参见文献[5].

为了实现图象的多幅分存,我们将动直线生成的曲线推广到高次情形. 假设直线 L_{00}, L_{01}, L_{02} 和 L_{10}, L_{11} 所组成的动直线分别为:

$$L_0[t]=L_{00}(1-t)^2+2L_{01}(1-t)t+L_{02}t^2,$$

$$L_1[t]=L_{10}(1-t)+L_{11}t$$

则 $P[t]=L_0[t]\times L_1[t]$为三次有理 Bezier 曲线，$t\in[0,1]$所对应的点位于曲线上. 用这样的方法可以构造任意次的有理 Bezier 曲线. 不难看出，借助射影几何学方法，利用直线束的性质，可以产生具有再生性的有理函数插值操作，然后，模拟于上述拉格朗日插值的方法，形成数字图象信息分存可行方案.

综上所述，本文研究的基本根据在于多项式插值或有理函数插值的存在唯一性定理. 利用这样的定理，使得节点及其上的数据作出重新选择时，可以再生原来的多项式或有理函数. 由此看来，只要具有再生性的插值操作，都有可能用来做数字图象信息分存.

4 数字图象信息分存实验图例

本文的实验分两部分.

(1) 静态图例：我们选择了各种不同类型的图象. 这里给出本文引言里的例子的进一步说明：图 2A 所示的图象为秘密图象；$B1$、$B2$ 等等表示多张分存图. 对于这样的具有较高灰度级或彩色丰富的图象，利用分存图中任意两张，可以重构得出精确程度如 A 所示的结果.

(2) 动态图象：选定一段视频作品图 3A(飞机飞行表演) 作为不公开的秘密影像数据，下面的图标中 A 表示该段视频作品的第 1 帧；$B1$、$B2$ 表示另一段视频作品(花样滑冰表演) 作为公开的伪装影像数据，实际上它可以由编码者相当自由的选择，与原来的不公开的秘密影像数据无关. 从 $B1$ 与 $B2$ 重构的影像数据，在视觉上与 A 相近(实验中可以进行动态演示).

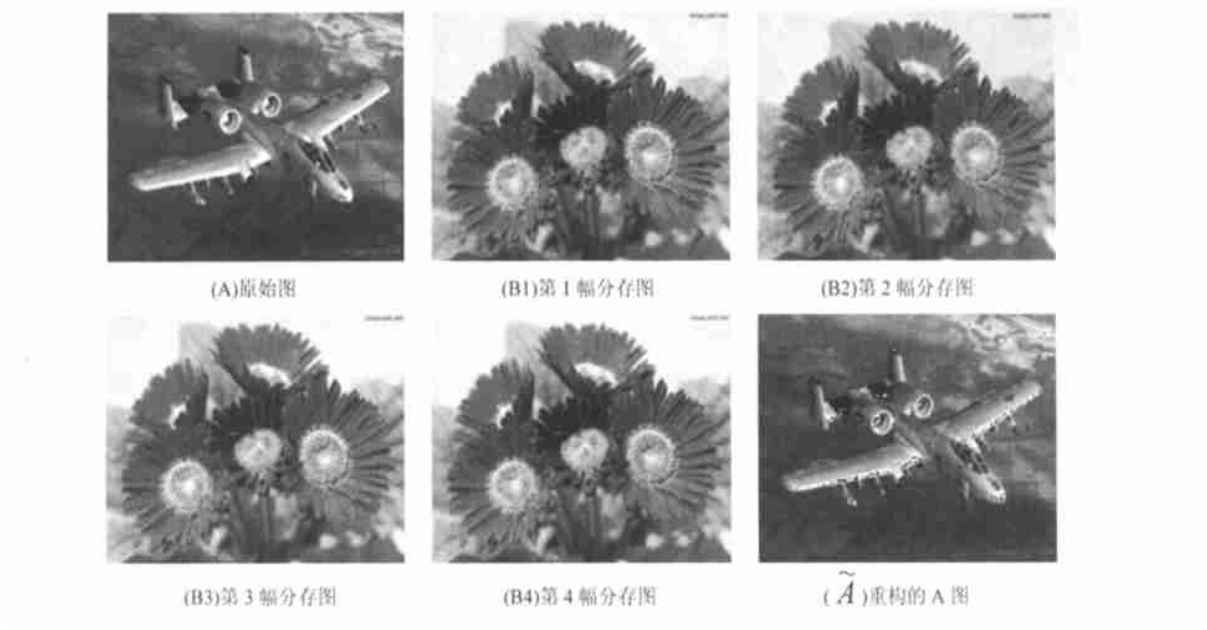

图 2 静态图例

图 3 动态图例

参 考 文 献

1 卢开澄.计算机密码学——计算机网络中的数据保密与安全(第二版). 北京:清华大学出版社, 1998

2 Anderson R, Ed. Information hiding: first international workshop. Cambridge, UK. Lecture Notes in Computer Science, Vol. 1174. Springer-Verlag, Berlin Heidelberg New York, 1996

3 David Aucsmith. editor. Information Hiding: Second International Workshop, volume 1525 of Lecture Notes in Computer Science, Portland, Oregon, U.S.A. Springer-Verlag, Berlin, Germany, 1998

4 丁玮, 齐东旭. 数字图象变换及信息隐藏与伪装技术. 计算机学报, 1998, 21(9): 838～843

5 Yan Weiqi, Ding Wei, Qi Dongxu. Image Sharing Based on Interpolation. In: Proc. of The 6th International Conference on Computer Aided Design & Computer Graphics. Shanghai: Wen hui Publishers, Dec. 1－3, 1999. Vol.2: 867～871

6 Shamir A. How to Share A Secret. Communications of ACM. 1979, 22(11): 612～613

7 Moni Naor, Adi Shamir. Visual Cryptography, In: Advances in Cryptology-urocrypt'94, A. De Santis, Ed., Lecture Notes in Computer Sciences, Springer-Verlag, 1995, 950: 1～12

8 苏中民, 林行良. 图象秘密的任意分存.计算机学报, 1996, 19(4): 293～299

9 Arto Salomaa. Public-Key Cryptography. Berlin Heidelberg: Springer-Verlag, 1990

10 Sederberg T W, Saito T, Dongxu Qi, Klimaszewski K S. Curve Implication Using Moving Lines. Computer Aided Geometric Design, 1994, 11: 687～706

Digital Images Information Sharing Based on the Principle of Shamir's (t,n) Private Key

Huang Yuson[1)]　Qi Dongxu[1,2)]

(1) Faculty of Information Technology, Macau University of Science and Technology, Macau

2) CAD Research Center, North China Univ. of Tech., 100041, Beijing, China)

Abstract　Based on the Principle of Shamir's (t,n) private key of cryptography, the method of digital images information sharing for storing and transmission is investigated in the paper. The main results are: for the original image A, the sender can choose arbitrarily any k quantity of the same size image ($k=1,2,3,\cdots$) to generate N quantity of images($N>k$); by using $k+1$ quantity of these N images, the receiver can restore the original image. The principle using Lagrange interpolation algorithm and a scheme for information sharing based on the projective geometry are also introduced. In order to explain the reasoning, some examples of images and works of video are illustrated.

Key Words　digital image; information sharing; Lagrange interpolation; projective geometry; pencil of line