ISSN1000-9825 Journal of Software 软件学报 2000,11(9):1176~1180

一种基于动直线的多幅图像分存方法*

闫伟齐[1] 丁玮[1] 齐东旭[1,2]

[1](中国科学院计算技术研究所CAD开放研究实验室 北京 100080)

[2](北方工业大学CAD研究中心 北京 100041)

E-mail: Yanweiqi@263.net/RickDing@126.com/Qidongxu@unet.net.cn

摘要 Shamir给出了一种基于拉格朗日插值的密码学分存方案,该文将其思想引入到图像信息安全处理当中,提出了用动直线进行多幅图像分存的方法,并阐述了这一算法的数学基础.此外,在进行图像分存时考虑了更多的原始图像,采用高次有理曲线进行图像分存计算,并分析比较了基于拉格朗日插值的分存算法和基于动直线的分存算法在多幅图像分存上的异同,指出了基于拉格朗日插值的图像分存算法在实际应用中存在的问题.最后,给出了采用动直线进行图像分存的实验结果.

关键词 信息隐藏,动直线,密码分存,图像分存,(t,n)-门限方案.

中图法分类号 TP309

图像分存是图像信息安全处理的重要内容,也是图像信息隐藏的主要方法.图像信息隐藏(steganography)是90年代中期以来新兴的研究课题,在国际上仅召开过3次学术会议[1,2].信息隐藏在诸多领域有着非常重要的作用,如国际互连网上信息的安全传输、货币及证券的防伪等,近年来,则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.当前的研究热点涉及数字产品版权保护、多媒体隐蔽通信、阈下通道、隐藏信息检测、低概率截取通信等领域.该课题同传统意义下的计算机密码学不同,密码学考虑的对象通常是二进制流,主要研究文本信息.对图像信息而言,其特点在于图像信息的可视性和相关性以及巨大的数据量.图像信息安全处理以数字图像处理、计算机图形学以及计算机密码学的知识为基础,研究图像信息传输、保存和复制以及鉴定中的安全问题,所研究的主要内容有多媒体数字水印技术,图像信息的隐藏、分存、置乱和加密等.目前,对图像信息安全的研究在国内开始活跃起来,文献[3,4]对图像信息的安全处理作了概括的介绍和讨论,文献[5]从密码学中密钥分存的角度出发,着重讨论了基于插值的图像分存方法,介绍了低次拉格朗日插值和低次动直线生成的有理曲线对图像的分存.本文在文献[5]的基础上,对图像信息的分存问题进行了进一步的讨论,特别是对多幅图像的分存问题进行了研究.

一般而言,图像分存问题可以描述为:将图像信息分为具有一定可视效果的n幅图像,这些图像称为子图像,这些子图像之间没有互相包含关系.如果知道图像信息中的$m(m\leqslant n)$幅子图像,则该图像可以得到恢复,如果图像信息少于$m(m\leqslant n)$幅,则图像无法得到恢复.

图像分存的最大特点就是可以做到分存后所得到的子图像仍然是可视的,丢失子图像中的若干幅并不影响图像的恢复,从而增强了图像信息的安全性,减弱了窃取原始图像的可能性.此外,即使丢失了若干幅子图像,依然可以恢复原图像.

图像分存不同于图像处理中的Morphing方法.Morphing方法通过两幅图像之间的颜色和位置插值来生成子图像,子图像来源于原始的两幅图像,考虑的是所生成图像的连续视觉效果;而图像分存生成的子图像来源于

---

* 本文研究得到国家自然科学基金(No.19671003)和国家973高科技项目基金(No.G1998030608)资助.作者闫伟齐,1968年生,博士生,主要研究领域为计算机图形学.丁玮,1971年生,博士生,主要研究领域为数字图像处理与压缩,计算机图形学.齐东旭,1940年生,教授,博士生导师,主要研究领域为计算机图形学,数值计算、分析,计算机辅助几何设计.

本文通讯联系人:闫伟齐,北京 100080,中国科学院计算技术研究所CAD开放研究实验室

本文2000-02-28收到原稿,2000-04-19收到修改稿

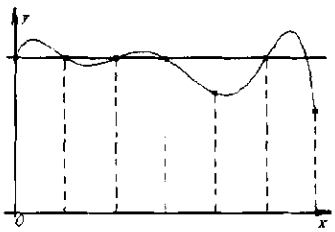

Fig. 1 Image sharing based on Lagrange interpolation
图 1 拉格朗日图像分存原理

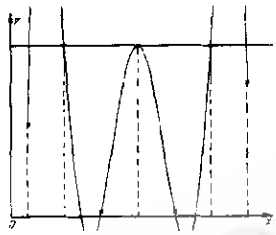

Fig. 2 Runge phenomena effects of image sharing based on Lagrange interpolation
图 2 拉格朗日分存算法的龙格现象

2 基于动直线的多幅图像分存算法

2.1 基于动直线图像分存的一般原理

在投影几何中,直线的方程可以表示成 $aX+bY+cW=0$,其中 a,b 和 c 不全为 0,(X,Y,W)是笛卡尔坐标系中点的齐次坐标,$(x,y)=(X/W,Y/W)$,设 P 记作三元数组(X,Y,W),L 记作三元数组(a,b,c). 则直线 L 为

$$\{(X,Y,W)\,|\,L\cdot P=(a,b,c)\cdot(X,Y,W)=aX+bY+cW=0\}. \tag{4}$$

可以认为,当且仅当 $P\cdot L=0$ 时,点 P 位于直线 $L=(a,b,c)$上.

如果齐次坐标为附加变量的函数,记 $P[t]=(X[t],Y[t],Z[t])$. 它等价于有理曲线 $x=X[t]/W[t]$,$y=Y[t]/W[t]$,如果函数是以下形式:

$$X[t]=\Sigma X_i\varphi_i[t],\quad Y[t]=\Sigma Y_i\varphi_i[t],\quad Z[t]=\Sigma Z_i\varphi_i[t],$$

其中$\{\varphi_i(t)\}$为给定的混合函数. 上述方程定义了曲线 $p[t]=\Sigma P_i\varphi_i[t]$. 齐次点序列 $P_i=(X_i,Y_i,W_i)$定义了一组曲线 $L[t]=(a[t],b[t],c[t])$. 参见文献[11~13].

记直线组 $a[t]x+b[t]y+c[t]=0$,为了获得两组直线的交集,我们考虑下述 4 条直线 L_{00},L_{01},L_{10},和 L_{11},它们可以定义为

$$L_0[t]=L_{00}(1-t)+L_{01}t,\ L_1[t]=L_{10}(1-t)+L_{11}t, \tag{5}$$

$t=0,\Delta t,2\Delta t,\ldots,1$ 所对应的点位于曲线上. 该曲线为圆锥曲线,可以表示成有理 Bernstain-Bézier 曲线 $p[t]$的形式:$P[t]=L_0[t]\times L_1[t]$,$p[t]$为二次有理 Bézier 曲线,其顶点为

$$P_0=L_{00}\times L_{10},\ P_1=\frac{1}{2}(L_{00}\times L_{11}+L_{01}\times L_{10}),\ P_2=L_{01}\times L_{11}. \tag{6}$$

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

2.2 多幅图像分存原理

为了实现图像的多幅分存,我们将动直线生成的曲线推广到高次情形进行讨论. 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

$$L_0[t]=L_{00}(1-t)^2+2L_{01}(1-t)t+L_{02}t^2,\quad L_1[t]=L_{10}(1-t)+L_{11}t,$$

则 $P[t]=L_0[t]\times L_1[t]$为三次有理 Bézier 曲线,$t\in[0,1]$所对应的点位于曲线上,如图 3 所示.

更一般地,由 $L_{00},L_{01},L_{02},\ldots,L_{0m}$和 $L_{10},L_{11},L_{12},\ldots,L_{1n}$所组成的动直线分别为

$$L_0[t]=\sum_{i=0}^{m}L_{0i}B_i^m(t)$$

$$L_1[t]=\sum_{i=0}^{n}L_{0i}B_i^n(t).$$

则 $P[t]=L_0[t]\times L_1[t]$为 $n+m$ 次的有理 Bézier 曲线,$t\in[0,1]$所对应的点位于曲线上.

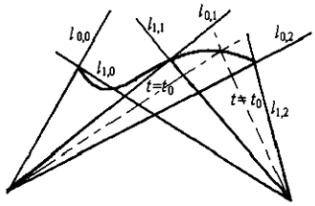

Fig. 3 Principle of high degree implicit curves generated by moving lines

图 3 动直线生成高次隐式曲线的原理

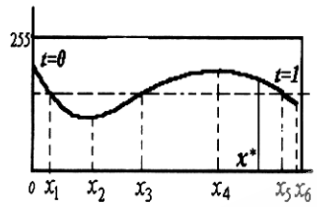

Fig. 4 Principle and condition of image sharing of many frames based on moving lines

图 4 基于动直线的多幅图像分存原理及条件

在多幅图像分存中,为了使分存过程稳定、可靠,一般在每一个具体的分存点附近设置两个固定点,让秘密图像和公开图像的参数在一定范围内变化. 如图 4 所示,x_1,x_3,x_5 为预先设置的固定点,它们可以保证曲线不会超出预定范围之外. 实验结果参见图 5.

(a) Original image 1

(a) 原始图像 1

(b) Original image 2

(b) 原始图像 2

(c) Original image 3

(c) 原始图像 3

(d) Sharad image, PSNR=22.47

(d) 生成的分存图像,PSNR=22.47

(e) Reconstucted image, PSNR=34.33

(e) 恢复后的图像,PSNR=34.33

Fig. 5 Results of image sharing of many frames based on moving lines

图 5 基于动直线的多幅图像分存结果

3 进一步的工作

本文讨论了基于拉格朗日插值和基于动直线的多幅图像分存算法. 图像分存问题的实质是寻求能够通过曲线上的一组不同点恢复原曲线所确定的密钥问题. 这是因为 Shamir 的(t,n)-门限方案最终归结为方程组(2)的求解问题,而解决这一问题的最好方法是通过拉格朗日插值方法. 拉格朗日插值可以通过曲线上的一组不同点恢复原曲线所确定的密钥,这也正是拉格朗日插值不同于其他插值的优点. 与拉格朗日插值类似,动直线生成的有理隐式曲线也满足这一性质,这正是采用动直线方法进行图像分存的原因.

基于拉格朗日插值的多幅图像分存由于其自身的缺陷,很难得到广泛的应用. 基于动直线的图像分存方法采用隐式有理曲线对图像进行分存,稳定可靠,有着较好的应用前景. 在今后的研究中,我们应当进一步考虑动直线的推广形式——动曲线和动曲面来进行图像的分存. 当前,对于一般图像分存仍然面临很多问题,尤其是如何更好地进行图像伪装、如何有效地控制分存数据膨胀等都是有待于进行深入讨论的问题. 一般认为,解决图像信息的分存问题,一方面要研究数学基础理论,注意与相关科学相结合,另一方面是要结合具体问题给出有效的算法.

参考文献

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

2 Aucsmith D. Information hiding: second international workshop. Lecture Notes in Computer Science, Vol. 1525, Berlin: Springer-Verlag, 1998

3 Qi Dong-xu. Skills of image hiding. China Computer User, 1999-8-23: 25～26
(齐东旭. 图象信息的隐藏技巧. 中国计算机用户,1999-8-23:25～26)

4 Ding Wei, Qi Dong-xu. Digital images information hiding and disguising technology. Chinese Journal of Computers, 1998, 21(9):838～843
(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 Wei-qi, Ding Wei, Qi Dong-xu. Image sharing based on interpolation. In: Chen Hou-peng, Gu Jian-hua eds. Proceedings of the 6th International Conference on Computer Aided Design & Computer Graphics. Shanghai: Wen Hui Publishers, 1999. 867～871

6 Shamir A. How to share a secret. Communications of the ACM, 1979,22(11):612～613

7 Naor M, Shamir A. Visual cryptography. In: deSantis A ed. Advances in Cryptology-Eurocrypt'94. Lecture Notes in Computer Science, Vol. 950, Berlin: Springer-Verlag, 1995. 1～12

8 Su Zhong-min, Lin Xing-liang. The secret of arbitrary sharing. Chinese Journal of Computers, 1996,19(4):293～299
(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 Lu Kai-cheng. Computer Cryptography (Version 2). Beijing: Tsinghua University Press, 1998
(卢开澄. 计算机密码学(第2版). 北京:清华大学出版社,1998)

11 Sommerville D M Y. Analytical Geometry of Three Dimension. Cambridge, Cambridge University Press, 1951

12 Sederberg T W, Saito T, Qi Dong-xu *et al*. Curve implication using moving lines. Computer Aided Geometric Design, 1994,11:687～706

13 Sederberg T W, Chen Fa-lai. Implicitization using moving curves and surfaces. In: Cook R ed. Proceedings of the SIGGRAPH'95. Los Angeles: ACM Press, 1995. 301～308

An Image Sharing of Many Frames Based on Moving Lines

YAN Wei-qi[1] DING Wei[1] QI Dong-xu[1,2]

[1](*CAD Laboratory Institute of Computing Technology The Chinese Academy of Sciences Beijing* 100080)

[2](*CAD Research Center North China University of Technology Beijing* 100041)

Abstract Shamir gave the (t,n)-Threshold Secret Sharing Scheme of cryptography based on Lagrange interpolation. In this paper, the authors introduce it into image sharing and give a new kind of algorithm for image sharing based on moving lines. The mathematical scheme of moving lines is presented in this paper. Hereby, when an image is shared, the authors consider more original images, compute with rational curves of high degree, compare the differences between Lagrange interpolation and moving lines on image sharing of many frames, and give the application fault of Lagrange interpolation with high degree in image sharing. Finally, some experimental results for image sharing based on moving lines are presented.

Key words Information hiding, move line, secret sharing, digital image sharing, (t,n)-threshold secret sharing scheme.