第 38 卷 第 4 期
Vol.38 No.4

计 算 机 工 程
Computer Engineering

2012 年 2 月
February 2012

• 安全技术 •

文章编号：1000—3428(2012)04—0116—03 文献标识码：A 中图分类号：TP391

多载体图像分存隐写算法研究

陈够喜[1,2]，沈红雷[1]，伍玉良[1]，陈俊杰[2]

(1. 中北大学电子与计算机科学技术学院，太原 030051；
2. 太原理工大学计算机与软件学院，太原 030024)

摘 要： 针对图像分存隐写容量小、安全性差的问题，提出一种基于 Bernstein 多项式的载体图像分存隐写算法。构建图像分存的隐写模型，分析 Bernstein 多项式性质并证明图像分存原理，并给出隐秘信息的嵌入与提取算法。实验结果表明，该算法能增大隐写容量，抵抗随机剪切攻击和加噪攻击。

关键词： 图像分存；信息隐藏；Bernstein 多项式；隐写；安全性；感知质量

Research on Sharing and Steganographic Algorithm for Batch Cover Image

CHEN Gou-xi[1,2], SHEN Hong-lei[1], WU Yu-liang[1], CHEN Jun-jie[2]

(1. School of Electronics and Computer Science Technology, North University of China, Taiyuan 030051, China;
2. School of Computer and Software, Taiyuan University of Technology, Taiyuan 030024, China)

【Abstract】 This paper proposes a cover image sharing steganographic algorithm based on the Bernstein polynomial for the problem of small steganography capacity and poor security of image sharing. It constructs image sharing steganographic model, describes the properties of Bernstein polynomial and proves sharing principle. Algorithms of embedding and extraction are given, experiments of image sharing steganography and anti-attack are completed. Experimental result and analysis show that the algorithm increases embedding capacity, reduces the perceived quality of cover image and improves security of secret information.

【Key words】 image sharing; information hiding; Bernstein polynomial; steganography; security; perceived quality

DOI: 10.3969/j.issn.1000-3428.2012.04.038

1 概述

基于数字图像的信息隐藏包括数字水印、隐写术和图像分存 3 个类型[1]。目前，针对前 2 种技术研究的文献较多，而对后者关注较少。图像分存主要研究如何把一幅隐秘数字图像分解成几幅无意义或杂乱无章的图像，并嵌入到几幅有意义的图像中进行存储或传输[2]。

文献[3]提出了彩色图像可视加密方案，文献[4-5]实现了基于动直线、二次剩余定理等技术的图像分存，文献[6]阐述了多幅图像的分存算法。上述文献均为单纯的图像分存，隐写容量较小且隐秘信息的安全性较差。Kawaguchi Y[7]提出图像比特面复杂度的概念，文献[8]进一步完善了最低多有效位(Multiple Least Significant Bits, MLSB)替换隐写思想。

本文基于 Bernstein 多项式变换和 MLSB 提出一种在图像分存中进行信息隐藏的模型，实现了图像分存与隐写的有机结合，增大了载体的隐写容量，提高了隐秘信息的安全性。

2 基于多载体图像的分存隐写模型

目前，信息隐藏技术主要是对隐秘信息进行加密处理，然后运用某种嵌入算法将其嵌入载体图像中，或将其分存到不同的载体图像中，达到隐蔽通信的目的。本文提出了基于 Bernstein 多项式的分存隐写模型，如图 1 所示。该模型采用 Bernstein 多项式对隐秘信息的载体进行变换，实现隐秘信息载体的分存，隐写过程产生在分存所得的子载体之中，其核心是隐写载体即隐写密钥。载体图像取灰度图像记为 C，经像素值调整后的载体图像为 C_1。$C_{11}\sim C_{1n}$ 是 Bernstein 多项式变换(B)后的载体图像集，称为分存子图。S 为隐秘图像，S_1~S_n 为 S 分块处理后的隐秘信息的集合。将获得的隐秘信息集合通过一定的方法嵌入到不同的分存子图中。经 Bernstein 逆变换 (B^{-}) 得出携密载体 C_1'，对其修正后得到携密载体 C_1''。

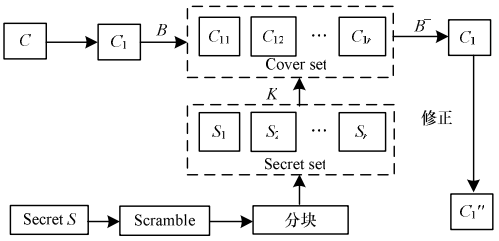


图 1 基于 Bernstein 多项式的分存隐写模型

定义(载体分存密钥隐写系统) 假设 $T=(T_c,T_s)$，T_c 是载体分存变换算法，T_s 是隐秘信息分块处理变换算法，C 为载体，$[C_1,C_2,\cdots,C_n]$ 为载体的集合，M 为隐秘信息的集合，$[M_1,M_2,\cdots,M_n]$ 为 M 分存后得到的隐秘信息集合，K 是私钥的集合：$K=[K_1,K_2,\cdots,K_n]$。如果存在以下公式：

(1) $T_c:T_c\times C\rightarrow[C_1,C_2,\cdots,C_n]$

(2) $T_s:T_s\times M\rightarrow[M_1,M_2,\cdots,M_n]$

基金项目： 国家自然科学基金资助项目(60773004)；山西省科技攻关计划基金资助项目(20090322004)

作者简介： 陈够喜(1966－)，男，副教授、博士、CCF 会员，主研方向：信息隐藏，图像处理；沈红雷、伍玉良，硕士研究生；陈俊杰，教授、博士生导师

收稿日期： 2011-07-20 **E-mail：** chengouxicgx@163.com

(3) $E_k : C\times M\times K\to C'$

(4) $D_k : C'\times K_1\to M_1$

则有下式成立：

$\forall m,c,k\in[M_i,C_i,K_i|1\leqslant i\leqslant n]$

$D_k(E_k(c,m,k),k)=[M_1,M_2,\cdots,M_n]$

那么，六元组 $H=(C,T,M,K,E_k,D_k)$ 称为一个载体分存密钥隐写系统。

3 基于载体图像分存的信息隐藏

3.1 Bernstein 多项式

设 P_m 是次数不超过 m 的代数多项式的集合，$C[a,b]$ 表示 $[a,b]$ 上全体连续函数的集合，$f(x)\in C[0,1]$，$f(x)$ 的 $m(m\geqslant 1)$ 阶 Bernstein 多项式定义为：

$$B_m(f;x)=\sum_{k=0}^{m} f(\frac{k}{m})C_m^k x^k(1-x)^{m-k}$$

其中，$C_m^k=\dfrac{m!}{(m-k)!k!}$，显然 $B_m(f;x)\in P_m$。

设 $f^{(p)}(x)\in C[0,1]$，$p\in \mathbf{Z}^+$，由 Bernstein 多项式性质得：

$$\lim_{m\to\infty}\max_{0\leqslant x\leqslant 1}|f(x)-B_m(f;x)|=0 \quad (1)$$

式(1)表明 Bernstein 多项式能够逼近在 $[0,1]$ 上的任意连续函数，即 m 足够大时，$B_m(f;x)$ 可代替 $f(x)$。

3.2 载体图像分存

载体图像分存的主要步骤如下：

(1)由于载体图像的像素值介于 0～255，因此根据式(1)，在 Bernstein 多项式变换之前，需将图像像素值转换为 [0,1] 之间的双精度数值。

(2) $\forall a,b\in\mathbf{Z}, f(x)=ax+b, a\neq 0$，由式(1)可得：

$B_n(ax+b,x)=ax+b$

$$x=\frac{f(x)-b}{a}=\frac{B_n-b}{a}\ (0\leqslant x\leqslant 1)$$

(3)设 C_k 为分存得到的分存子图，$k=0\sim n$，x 为载体图像中的像素值，根据 Bernstein 多项式定义可得：

$$C_k=\binom{n}{k}f\left(\frac{k}{n}\right)x^k(1-x)^{n-k} \quad (2)$$

根据步骤(2)中的已知条件，可得分存载体图像的像素值 $x\in(0,|a|)$。

(4)对步骤(3)中所得 x 值进行调整，由 $x=x/|a|$，使得 $x\in[0,1]$。

3.3 隐秘信息嵌入与提取

假设分块隐秘信息 $S_1\sim S_n$ 相互独立，满足下列条件：

$$E_k:[C_{11},C_{12},\cdots,C_{1n}]\times[S_1,S_2,\cdots,S_n]\times K\to[C_{11},C_{12},\cdots,C_{1n}] \quad (3)$$

根据式(3)，进行嵌入的载体图像集中的隐秘信息像素值经 Bernstein 变换时需相互独立，且式(4)：

$$[C_{11},C_{12},\cdots,C_{1n}]\times B^{\neg}\to C_1' \quad (4)$$

中的参数 $B^{\neg}$ 为 Bernstein 逆变换。根据 $B^{\neg}$ 变换，由 $B_n(ax+b,x)=ax+b$，可得复原后的携密载体图像为：

$$C_1'=(B_n-b)/a=(\sum_{k=0}^{n}A_k-b)/a$$

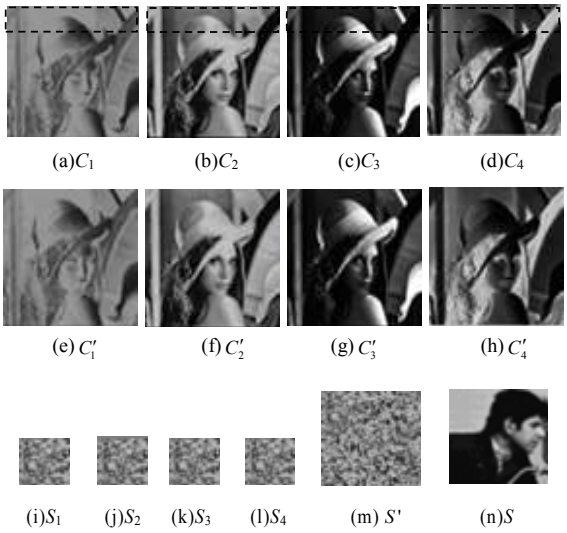
由于分存载体像素值经过 $x=x/|a|$ 调整，因此需对恢复图像的像素值进行修正，修正后的携密图像为：

$$C_1''=(\sum_{k=0}^{n}A_k\times|a|-b)/a$$

在提取隐秘信息时，首先运用 Bernstein 变换将 C_1'' 分解，再从 $C_{11},C_{12},\cdots,C_{1n}$ 中分别提取出分块后的隐秘信息。

4 实验结果与分析

选取 $n=3$，$a=3$，$b=3$，$k=0\sim 3$。由式(2)可将载体图像分解为 4 个分存子图，载体图像为 256×256 像素的 Lena 灰度图像，由 Bernstein 多项式变换所得分存载体图像如图 2 中的 $C_1\sim C_4$ 所示。根据式(3)采用 MLSB[8]算法将隐秘信息 $S_1\sim S_4$ 嵌入到分存载体 $C_1\sim C_4$ 中，得到的携密图像如图 2 中的 $C_1'\sim C_4'$ 所示，虚线框指示隐秘信息嵌入位置。根据 Bernstein 逆变换，由 $B_n(ax+b,x)=ax+b$，可得复原后的携密载体图像 C。隐秘信息预处理是运用 Logistic 系统产生的混沌序列，然后对大小为 64×64 像素的 man 灰度图像置乱。提取出的秘密信息块如图 2 中的隐秘信息块 $S_1\sim S_4$ 和 S' 所示。如图 2 中的 S 是根据所获取的随机序列得到的隐秘信息。对比载体图像及载密图像，载密图像的视觉效果良好，是不可察觉的，而且可正确提取出隐秘信息。



(a)C_1 (b)C_2 (c)C_3 (d)C_4

(e)C_1' (f)C_2' (g)C_3' (h)C_4'

(i)S_1 (j)S_2 (k)S_3 (l)S_4 (m)S' (n)S

图 2 载体分存及提取的隐秘图像

4.1 容量分析

选取载体图像大小为 $R\times T$，隐秘图像为 $p\times q$，隐秘信息等分为 n 份。例如 $n=3$，载体分存为 4 份，根据 MLSB 嵌入规则(设位平面数为 r)，分存子图的隐写容量 M_i 为：

$M_i=8r\cdot(p\times q)/(n+1)\ (0\leqslant i\leqslant n)$

将分块的隐秘信息分别嵌入到不同的分存子图中，由 Bernstein 多项式进行合并，修改像素量降低为直接利用 LSB 算法的 $r/(n+1)$，嵌入总容量为 $(R\times T)\times 8r$，相比文献[6]算法的隐写容量提高了 $r\cdot(R\times T)/(p\times q)$ 倍。

4.2 抗攻击能力分析

在实际传输过程中，携密图像可能受到剪切和噪声等相关攻击。携密图像 C 的 PSNR = 39.367 dB，图像的感知误差 Watson 质量为 $W=58.702$JNDs，JNDs 是指图像变化的临界差异。

随机剪切攻击：剪切携密载体图像 C 中任一部分，提取隐秘信息。C_1 和 C_2 是由携密载体图像随意剪切后得到的图像，G' 是从载体图像 C_2 中提取的隐秘图像。实验结果如表 1 和图 3 所示。

表 1 随机剪切攻击数据

实验	PSNR/dB	JNDs
实验 1	28.756	54.637
实验 2	23.342	50.173

(a)携密图像C (b) C_1 (c) C_2 (d) G'

图 3 抗随机剪切攻击效果

加噪攻击：携密载体图像分别加 5%、10%、20%的椒盐噪声，实验结果如表 2 和图 4 所示。

表 2 加噪攻击数据

加噪比例/(%)	PSNR/dB	JNDs
5	27.976	212.748
10	25.099	335.285
20	22.082	606.876

(a)加噪 5% (b)加噪 10% (c)加噪 20% (d) G'

图 4 抗加噪攻击效果

根据 B^{-}运算获取载体分存图像，并从中分别提取出加密的隐秘图像，如图 4 所示。图 4 中的 G'是采用 20%的椒盐噪声时获取的隐秘图像。

综合攻击(随机剪切和加噪)：对图 3 的携密载体图像 C 综合采用 2 种攻击方法，实验结果如表 3 和图 5 所示。

表 3 综合攻击数据

加噪比例/(%)	PSNR/dB	JNDs
5	17.976	412.748
10	15.099	535.285
20	12.082	806.876

(a)剪切加噪 5% (b)剪切加噪 10% (c)剪切加噪 20% (d) G'

图 5 抗综合攻击效果

图 5 给出同时为对携密载体图像进行剪切及加椒盐噪声综合攻击的不同情形。图 5 中的 G'为剪切及加噪 10%时获取的隐秘图像。

以上实验表明，基于 Bernstein 多项式的图像分存隐写算法，降低了隐秘载体的像素修改率，扩大了隐写容量，同时具有有较强的抗攻击能力。

5 结束语

本文基于 Beinstein 多项式，提出了多载体图像分存的隐写算法，扩大了图像分存的隐写容量，提高了隐秘信息的安全性。此算法若与空域变换方法(最低比特位)、频域变换方法(离散余弦变换、离散小波变换)及各种频域改进的隐写算法相结合，图像分存的隐写容量将会进一步提高。但在载体分存过程中，若分存系数选取不合理可能出现像素值溢出问题，影响载密图像的感知质量，这些将在今后的工作中进一步探讨。

参考文献

[1] 王朔中, 张新鹏, 张卫明. 以数字图像为载体的隐写分析研究进展[J]. 计算机学报, 2009, 32(7): 1247-1263.

[2] Shamir R. How to Share a Secret[J]. Communications of ACM, 1979, 22(11): 612-613.

[3] Lukac R, Plataniotis K N. Colour Image Secret Sharing[J]. Electronics Letters, 2004, 40(9): 529-531.

[4] 闰伟齐, 丁 玮, 齐东旭. 一种基于动直线的多幅图像分存方法[J]. 软件学报, 2000, 11(9): 1176-1180.

[5] 邓绍江, 胡春强, 王方晓, 等. 基于二次剩余定理的数字图像分存方法[J]. 计算机工程, 2009, 35(15): 124-126.

[6] 李洪安, 刘晓霞, 朱玲芳. 基于分存的多幅图像信息隐藏方案[J]. 计算机应用研究, 2009, 26(6): 2170-2172.

[7] 郭云彪, 尤新刚, 张春田, 等. 面向信息隐藏的图像复杂度研究[J]. 电子学报, 2006, 34(6): 1048-1052.

[8] Nguyen B, Yoon S, Lee H. Multi Bit Plane Image Stegana-Graphy[C]//Proceedings of International Workshop on Digital Watermarking. Jeju Island, Korea: [s. n.], 2006: 61-70.

编辑 张正兴

(上接第 111 页)

数据包端到端延迟随车辆移动速度增加而增加；链路吞吐率随速度增加而逐渐降低，当移动速度达到 25 m/s~30 m/s 范围后，链路吞吐率降低幅度大，并逐渐接近 0；车辆移动速度的增加使得数据包传输率逐渐降低。同时，采用 LED-AODV 路由算法的网络中数据包端到端平均延迟更小。当车辆移动速度分别在 15 m/s~20 m/s、20 m/s~25 m/s 和 25~30 m/s 等范围时，相比较 AODV 算法，LED-AODV 算法使得链路吞吐率更高，其增加幅度分别为 112.24%、352.13%和 514.58%，且在使用 LED-AODV 算法的网络中，报文投递率也明显更高。

5 结束语

本文在 VANET 高速公路场景中，对 AODV 路由算法的路由寻找、路由回溯和路由维护进行优化，提出改进的路由算法 LED-AODV，减轻了 RREQ 广播洪泛，降低了 VANET 中链路频繁中断对网络带宽的消耗。LED-AODV 算法能使得链路传输过程持续、稳定，提高链路传输性能。通过仿真结果表明，在数据包端到端延迟、传输吞吐率及报文投递率等方面，LED-AODV 路由算法具有更好的性能。下一步工作将考虑链路持续时间，并针对持续时间可能的变化趋势进行研究分析，进一步改善 VANET 的传输性能。

参考文献

[1] 常促宇, 向 勇, 史美林. 车载自组网的现状与发展[J]. 通信学报, 2007, 28(11): 116-126.

[2] 苏金树, 胡乔林, 赵宝康. 容延容断网络路由技术[J]. 软件学报, 2010, 21(1): 119-132.

[3] 路 伟, 鲍远律, 白 皓. 单向交通流中车-车间通信性能研究[J]. 计算机工程, 2011, 37(4): 107-109.

[4] Dhurandher S K, Misra S, Obaidat M S, et al. Efficient Angular Routing Protocol for Inter-vehicular Communication in Vehicular Ad Hoc Networks[J]. The Institution of Engineering and Technology, 2010, 4(7): 826-836.

[5] Li Fan, Wang Yu. Routing in Vehicular Ad Hoc Networks: A Survey[J]. IEEE Vehicular Technology, 2007, 2(2): 12-22.

[6] 刘期烈, 祝孟伟, 黄 巍, 等. 机会网络中无线链路统计特性研究[J]. 计算机工程, 2011, 37(7): 1-3.

[7] Taleb T, Sakhaee E, Jamalipour A. A Stable Routing Protocol to Support ITS Services in VANET Networks[J]. IEEE Transactions on Vehicular Technology, 2007, 56(6): 3337-3347.

编辑 金胡考