基于(t,n)门限的可防欺骗的图像隐藏方案

陈继超[1],谢 柯[2]
(1.合肥工业大学 管理学院,安徽 合肥 230009;
2.合肥工业大学 计算机与信息学院,安徽 合肥 230009)

摘 要:为了保证秘密图像可以在不安全的网络环境下安全的传输,设计了一个具体完整、实践性强的基于(t,n)门限的可防欺骗的图像隐藏方案。在保证方案的效率及安全性的基础上,通过二次拉格朗日插值算法完成共享秘密的分割以完成(t,n)门限的过程,同时,通过单向散列函数防止了攻击者篡改嵌入了共享秘密后的影子图像,也防止了欺骗者给出虚假的影子图像,保证了秘密的数字图像在不安全的网络环境中的安全传输,具有较好的理论和实践价值。

关键词:门限;拉格朗日插值;散列函数
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2006)09-0208-02

An Image Hiding Scheme Preventing Cheat Based on (t,n) Threshold

CHEN Ji-chao[1], XIE Ke[2]
(1.School of Management Science, Hefei University of Technology, Hefei 230009,China;
2.School of Computer and Information, Hefei University of Technology, Hefei 230009,China)

Abstract: In order to guarantee the safe transmission of a secret image through an unsafe network, this paper proposes a new preventing cheat image hiding scheme based on(t,n)threshold, that is complete and practicable. On the base of guaranteeing the efficiency and security of this scheme, it applies the method of Lagrange Interpolating Polynomial to divide the share secret and to complete the (t, n) threshold process. On the same time, it applies Hash function to prevent cheater tampering the image that contains the share secret and to prevent cheater giving false shadow image. So it guarantees the safe transmission of a secret image through an unsafe network, it is valuable in theory and practice.

Key words: threshold; Lagrange interpolating; Hash function

0 引 言

随着计算机技术和通讯技术的发展,网络上传输信息的模式发生了巨大变化,越来越多的信息以多媒体的形式在网络中传输。其中以数字图像形式的传播也变得越来越普遍。为了保证图像在不安全的网络环境下传输的安全性,传统的的做法是运用密码学中的种种算法对图像数据进行加密[1~3],但是这样做效率低且浪费时间,在许多应用中并不能保证图像的安全性,因对图像加密,本身已经标志了图像的重要性,同时也更会引起攻击者的注意。而图像隐藏技术为解决这个问题提供了良好的解决方法,它能让一幅秘密的图像,如一幅军用地图,嵌入到一幅或多幅无关的其他图像(称之为影子图像,可以是风景、生物等)中,以避免侦测和破坏。那么什么是(t,n)门限呢?Blakley[4]与Shamir[5]提出了(t,n)门限的概念,即把共享的秘密以某种方式分割为n份子秘密,再分配给n个参与者。对于这其中的任意t个参与者,如果$t \geqslant r$,则这t个人就可以得到这个秘密;如果$t < r$,则得不到秘密,这就是所谓的(t, n)门限的概念。把(t,n)门限思想应用于图像的隐藏是一个崭新的领域,在此之前,有许多学者做了大量的工作,比如Chin-Chen Chang[6]等人的运用门限方案的图像隐藏方案等,为了防止参与者在秘密图像的恢复过程中给出虚假的影子图像,此方案采取了逐像素点计算单向散列函数值并验证的方法,笔者认为这样会在实际应用中会造成效率问题,大量耗费系统资源。文中提出了一个具体完整的、实践性强的基于(t,n)门限的可防欺骗的图像隐藏方案,在保证方案的效率及安全性的基础上,通过二次拉格朗日插值完成(t,n)门限过程及通过单向散列函数防伪,同时亦防止了欺骗者给出虚假的影子图像。

收稿日期:2005-12-16

作者简介:陈继超(1980-),男,安徽合肥人,硕士研究生,研究方向为管理科学与工程;导师:刘心报,博士生导师,教授,研究方向为管理科学。

1 拉格朗日插值方法概述

设有方程如下:

$$f(x) = [a_1x + a_2x^2 \cdots + a_{t-1}x^{t-1} + K] \bmod p \quad (1)$$

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。

$$K = f(0) = \sum_{X_i \in T}(L_i \times f(x_i)) \tag{2}$$

这里 $L_i = \prod_{x_i,x_j \in T, x_j \neq x_i} - x_j/(x_i - x_j)$ (3)

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。

2　算法设计

该算法将以位图为例实现。位图的存储单位是一个字节的 8 位二进制数,化为十进制即为一个 0～255 之间的整数,其中靠左边的 5 位是最为重要的。这 5 位数值可以大体上表征函数的特征。选取一幅 8 位位图作为要隐藏的图像,n 幅24位位图作为影子图像,在8位的位图中,每个像素由一个字节构成,有相应的色表与之对应。在 24 位的位图中,每一个像素由 3 个字节构成,每一个字节表征了一种颜色,即 RED,GREEN,BLUE 三色。设需嵌入的秘密图像(位图)为 M,影子图像(位图)为 $S_i(i = 1,2,3,\cdots,n)$。

(1) 加密阶段具体的细节描述如下:

① 首先处理 $S_i(i = 1,2,3,\cdots,n)$,对 S_i 的每个像素而言,将其中的 3 个字节中每个字节的最左边的 5 位取出来,这样就得到了一幅肉眼基本上不能分辨出与 S_i 区别的图像 S_i',这里 S_i' 的每一个像素点就留出了 9 位可供以后用来隐藏要加密的图像,而 S_i' 本身依然是一幅完整的有意义的图像,完全可以起到隐蔽要加密的图像 M 的效果。

② 对于 M 中的每一个位置为 (x,y) 的像素点而言,选取 $(t-1)$ 次的多项式 $f_{(x,y)}$,具体为

$$f_{(x,y)}(V) = [a_1 v + a_2 v^2 + \cdots + a_{(t-1)}v^{t-1} + M_{(x,y)}] \bmod p$$

这里,$a_1,a_2,\cdots,a_{(t-1)}$ 都是小于 p 的随机数,p 可以取 251,这个多项式是保密的。为每一幅影子图像 S_i' 选取一个惟一的序列号 N_i,然后对 M 中的每一个像素点依次计算 $f_{(x,y)}(N_i)$,并把计算的结果化为 8 位二进制数后作为影子填充到 S_i' 中每一个像素点空闲的 9 个二进制位的前 8 个中以完成数据的嵌入。这里 $M_{(x,y)}$ 是 8 位的二进制数连接起来后的十进制表示。

这样 S_i' 就变为了 S_i'',两者不同的是 S_i'' 中的每一个像素点的有效数值变为了二进制的 23 位。

③ 此时,对于影子图像的每个像素点而言,就只剩下最后一个二进制位了,定义若填入这个像素点的 $f_{(x,y)}(N_i) > 128$,则最后一位填 1,否则填 0。

④ 把每个影子图像的所有像素点的最后一个二进制位提取出来并连接,都可以得到一个连接后的二进制数,再把每个二进制数变为十进制数,分别设为 $N_1,N_2,\cdots,N_n$。此时再计算这 N 个数的十六进制数表示单向散列函数值 $HV_1,HV_2,\cdots,HV_n$,注意在选取影子图像时,其像素点的总数比要隐藏的图像 M 的像素点的总数大一些,可以把 HV_i 覆盖一些 S_i'' 的像素点存入 S_i'' 中,进行单向散列函数运算的目的是为了防止影子图像的像素点的数值被篡改。

(2) 解密阶段的具体的细节描述如下:

① 当 N 个参与者收到各自的 S_i'' 后,要有至少 t 个人拿出自己的 S_i'' 才有可能恢复秘密。首先必须验证参与者拿出的 S_i'' 是否真实,对于每一幅 S_i'' 而言,首先提取每一个像素点的最后一个二进制位,连接起来化为十进制数后计算它的单向散列函数值 HV_i',然后取出藏在图像中的 HV_i,接着验证 HV_i 是否和 HV_i' 相等,若两者相等,则说明参与者拿出的 S_i'' 是真实的,反之若两者不相等,则说明参与者拿出的 S_i'' 是不真实的。

② 在验证完 S_i'' 的真实性后,以一个像素点为例,则从至少 t 个 S_i'' 中的每一个像素点中取出图像 M 的一个像素点的至少 t 个经过拉格朗日插值后的数值。通过拉格朗日插值算法可以计算出 M 的一个真实的像素点的值,按此方法恢复图像 M 中的每一个像素点,即可恢复图像 M。

3　算法的分析及与相关算法的比较

从以上讨论可知,Chin－Chen Chang[6] 等人虽然也运用了门限方案来解决图像隐藏问题,但是此方案在验证影子图像真伪时,要逐像素点计算单向散列函数值并验证,笔者认为这样在实际应用中会造成效率问题,大量耗费系统资源。而且把单向散列函数用 RSA 签名后的数据长度将取决于 RSA 方案中的 N 的大小,笔者认为加密后的数据长度不可能等于哈希值的 4 位的长度值。基于上述考虑,笔者设计了以下运用 (t,n) 门限方案的高效率的图像隐藏方案,同样可以防止欺骗者给出虚假的影子图像,但是由于在验证时只需要计算一次单向散列函数,大大提高了系统的效率,具有很强的实践性。

4　结束语

提出了一个具体完整的、实践性强的基于 (t,n) 门限的可防欺骗的图像隐藏方案,在保证方案效率及安全性的基础上,通过二次拉格朗日插值完成 (t,n) 门限过程及单向散列函数防伪,防止了欺骗者给出虚假的影子图像。

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

(下转第 212 页)

者所做出的推荐才有效。如图 3 中，甲图中 A 不会信任 D 的公钥，只有当出现如乙图或丙图中的情况时才可以说 A 信任 D 的公钥。

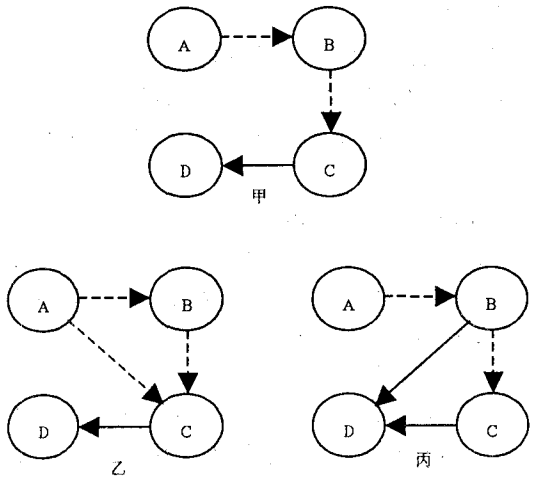

图 3 信任链图

(3) 用户可以拥多对公私钥，但在推荐别人或被别人推荐时建议只使用其中一对，这可避免不必要的误会。

3.6 PGP 信任模型的缺陷

PGP 信任模型的缺陷是：

(1) 由于 PGP 中信任链的长度最多为 2，即最多有一个推荐信任和一个公钥信任，因此不利于信任关系的传播。

(2) 没有反映推荐者对所推荐公钥的可信程度，而只是认为可信则签名，不可信则不签。

(3) 信任度只分 3～4 个等级，因此衡量信任度的粒度不够。

4 对 PGP 信任模型的改进

4.1 信任的度量

信任度由一个介于[0,1]区间内的值来表示，0 表示不了解；1 表示完全信任。可以在 0 和 1 之间划分若干个等级来表示不同的信任程度。

4.2 推荐信任可以传递

可以推荐值得信任的推荐者，一条信任链由若干个推荐信任和一个公钥信任组成。推荐者对所推荐的推荐者或公钥有一个信任值，将对方的用户 ID、公钥与此信任值一起签名，并要求此推荐值一定要大于 0，即不传递否定信任。

4.3 公钥信任的计算

用 T_{AB}表示 A 对 B 的公钥信任，T_{AB}'表示 A 对 B 的推荐信任，计算 T_{AE}时，如果存在由 A 到 E 的直接路径，则 T_{AE}即为 A 对 E 的公钥信任，如果不存在，则要穷举所有由信任方到该公钥的所有信任链，每一条链计算一个由所有中间的信任度的积得出信任值，最后将所有链的信任值平均得出最终的公钥信任[3]。如图 4 这种情况，则计算公式为：

$$T_{AE}=(T'_{AB}\cdot T_{BE}+T'_{AC}\cdot T'_{CD}\cdot T_{DE})/2$$

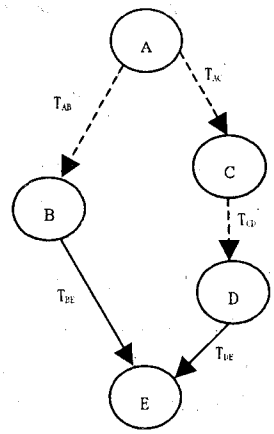

图 4 信任度计算图

5 结 论

通过对 PGP 信任模型的改进，得到了一个更加精确、更有利于信任传播的信任模型，为 Internet 这样的分布式环境下通信双方安全通信提供了一个可供参考的信任模型。

参考文献：

[1] Zimmermann P. Pretty Good Privacy User's Guide, Volume I and II[Z]. Distributed with PGP software, 1993.

[2] Blaze M, Feigenbaun J, Lacy J. Decentralized Trust Management[A]. In Proceedings of the IEEE Conference on Security and Privacy[C]. Los Alamitos: IEEE Computer Society Press, 1996. 164－173.

[3] Abdul－Rahman A, Hailes S. A Distributed Trust Model[A]. In Proceedings ACM New Security Paradigms Workshop '97 [C]. Cumbria, UK: ACM, 1997. 48－60.

[4] Abdul－Rahman A. The PGP Trust Model. EDI－Forum [EB/OL]. Available at http://www.cs.ucl.ac.uk/staff/F.AbdulRahman/docs/., 1997.

[5] Ellison C. SPKI/SDSI and the Web of Trust[EB/OL]. Available at http://world.std.com/cme/html/web.html, 2001.

(上接第 209 页)

Imaging, 1993, 2(4): 345－351.

[4] Blakley G R. Safeguarding Cryptographic Keys[A]. Proceedings of the National Computer Conference[C]. US: American Federation of Information Procession Societies, 1979. 242－268.

[5] Shamir A. How to Share a Secret[J]. Communication of ACM, 1979, 22: 612－613.

[6] Chang Chin－Chen, Lin Iuon－Chang. A new (t, n) Threshold Image Hiding Scheme for Sharing a Secret Color Image [A]. Proceedings of ICCT2003[C]. Beijing: Press of BJUPT, 2003.