

基于混沌的网络化制造文件安全传输系统设计

雷正桥

(重庆工业职业技术学院 计算机系, 重庆 401120)

摘 要: 利用一种新颖的混沌安全算法可以同时完成加密散列运算的特点, 设计和实现了一个网络化制造安全文件传送系统. 由于在系统设计中充分利用了算法的组合优点, 可以同时完成对文件的加解密和散列功能, 在很大程度上简化了文件安全传输系统, 使得整个系统具有安全性好、操作方便、运行效率高的特点, 实际推广潜力大.

关键词: 混沌; 加密; 散列; 网络化制造; 文件传输

中图分类号: TP391

文献标识码: A

文章编号: 1000-7180(2012)04-0118-05

Design Secure File Transmission System in Networked Manufacturing Based on Chaos

LEI Zheng-qiao

(Department of Computer, Chongqing Industry Polytechnic College, Chongqing 401120, China)

Abstract: Based on a chaotic security algorithm which can complete encryption and hashing in a combined manner, a secure file transmitting system was designed and developed. Since the merit of the algorithm is fully utilized, the overall transmission system is strong in security, convenient in implementation, and has high efficiency and potential to be generalized.

Key words: chaos; encryption; hash; networked manufacturing; file transmission

1 引言

如何解决异地协同开发制造环境中的信息安全问题, 防止重要商业数据被竞争对手恶意窃取、篡改和破坏, 保护企业的知识秘密, 是网络化制造研究领域的重要课题^[1]. 本文应用混沌密码学中的最新成果, 在某大型企业网络化制造平台设计中, 实现了一个安全高效的网络化制造环境下的文件安全传输系统.

2 混沌加密散列组合算法

混沌密码技术来源于信息科学和非线性科学两个学科的交叉融合. 对初始状态的高度敏感性、自相似性、复杂的动力学行为等是混沌系统的优点, 为其带来了在信息安全领域广阔的应用前景^[2-4].

本文所采用的混沌加密散列组合算法最初设计思路起源于文献[5], 属于分组密码. 算法在结构上一个很大的特点是引入了查找索引表(Look-Up Index Table), 图 1 所示为最初的查找索引表. 查找索引表的右边代表明文空间, 当明文按 n 位分组时, 相应的明文空间为 $M = \{s_0, s_1, \dots, s_{2^n-1}\}$, 其中 $s_i = i$; 查找索引表的左边代表索引空间 $T^n = \{T_0, T_1, \dots, T_{2^n-1}\}$, 其中 $T_i = i$. 查找索引表本质上是索引空间与明文空间之间的一种双射映射 $\phi: T^n \rightarrow M$. 在本算法中使用的混沌系统为一维分段线性映射:

$$F: x_{i+1} = \begin{cases} x_i/b & x_i \leq b \\ (1-x_i)/(1-b) & x_i > b \end{cases} \quad (1)$$

2.1 加解密过程

算法密钥为 $\text{Key} = \{x_0, b\}$, 其中, $x_0 \in (0, 1)$ 为混沌系统的初始值, $b \in (0, 1)$ 为混沌控制参数. 设明

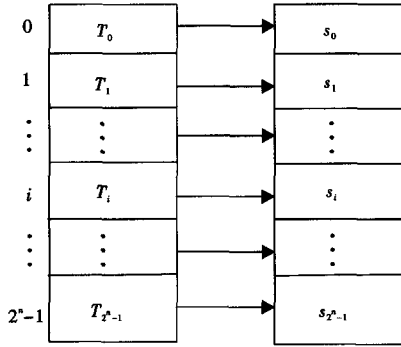


图1 最初的查找索引表

文可分为 r 个 n 位长的分组, 即 $m = m_1, m_2, \dots, m_r$. 加密具体过程如图2所示.

(1) 初始化查找表, 首先置 $\phi_0(T_i) = s_i, i = 0, 1, 2, \dots, 2^n - 1, s_i \in M$, 然后设定 x_0 为初始值, 迭代混沌系统 N ($N = 2^n$, 查找表大小) 次, 生成混沌序列 $\{x_0, x_1, \dots, x_i, \dots, x_{N-1}\}$, 长度为 N , 该序列被用于对查找表的置乱, 置乱后的查找表被称为 ϕ_1 . 置乱方法是通过将该混沌序列中每个元素乘以 256 取整后转化为新的整数序列 $\{y_0, y_1, \dots, y_i, \dots, y_{N-1}\}$, 将查找表中第 i 个索引项与其对应的第 y_i 个索引项进行交换.

(2) 置 $i = 1, x_0^1 = x_0, C_0 = g$, 其中, g ($0 \leq g \leq 2^n$, $g \in \mathbb{Z}^+$) 为常数, 可以任意选取.

(3) 以 x_0^i 为初始值迭代混沌系统 $it = 10$ 次, 并记混沌系统当前状态为 $\tilde{x} = F^{it}(x_0^i)$.

(4) 设 $D_i = \lfloor \tilde{x} \times 2^n \rfloor$, 并将其表示为 n 位的二进制整数 $D_i = (d_1 d_2 \dots d_n)_2$, 令 D_i 的奇数位和偶数位代表整数 P_i, Q_i , 即 $P_i = (d_1 d_3 \dots d_{2n-1})_2, Q_i = (d_2 d_4 \dots d_{2n})_2$, 其中 $d_j \in \{0, 1\}, j = 1, 2, \dots, 2\alpha, \alpha = \frac{n}{2}$.

(5) 若 $P_i = Q_i$, 置 $x_0^i = \tilde{x}$, 转到(3); 若 $P_i < Q_i$, 则令 $\tilde{m} = m_i \oplus C_{i-1}$; 若 $P_i > Q_i$, 则令 $\tilde{m} = m_i \oplus D_i$.

(6) 根据 $\tilde{m}$ 值来搜索查找表, 在查找表中找到与明文对应的项的索引值, 将其记为密文 C_i , 即: C_i 满足 $T_{C_i} = \phi_i^{-1}(\tilde{m})$.

(7) 若 $i = r$ 成立, 以 x_0^i 为初始值迭代混沌系统, 生成长度为 N 的混沌序列, 以步骤(1)中类似的方法置乱查找索引表, 算法结束, 并将最终的查找表的索引项作为整段明文的散列值; 否则更新查找表 (具体方法见 2.2 节), 记为 ϕ_{i+1} , 令 $i = i + 1, x_0^i = (x + \tilde{m}/2^n) - \lfloor x + \tilde{m}/2^n \rfloor$, 转步骤(3).

解密具体过程如图2所示.

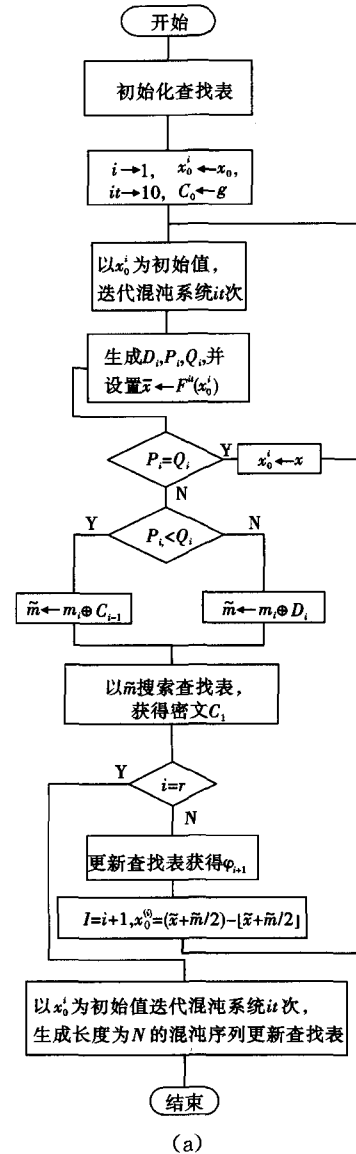
步骤(1)~(4)同加密过程中一样;

(5) 置 $\tilde{m} = \phi_i(T_{C_i})$;

(6) 若 $P_i = Q_i$, 置 $x_0^i = \tilde{x}$, 转到(3); 若 $P_i < Q_i$,

则第 i 组明文为 $m_i = \tilde{m} \oplus C_{i-1}$; 若 $P_i > Q_i$, 则第 i 组明文为 $m_i = \tilde{m} \oplus D_i$;

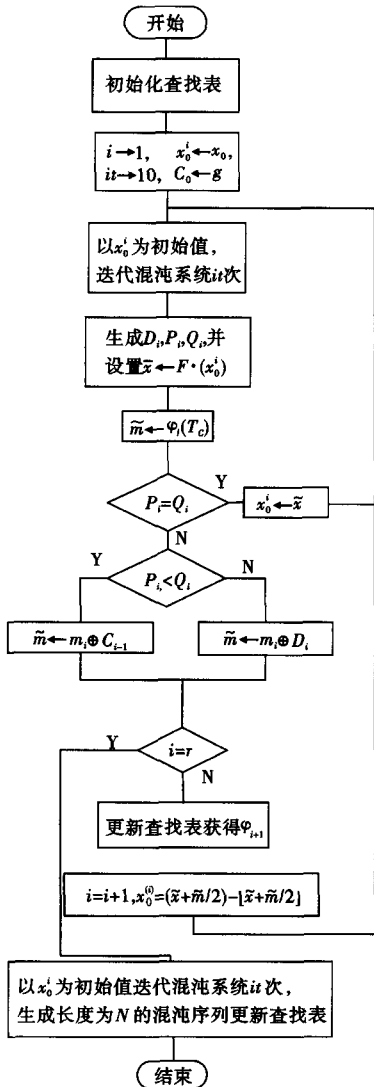
(7) 同加密过程中的步骤(7)一样. 当算法结束时, 最终查找表的索引项被取出作为散列值.



(a)

2.2 散列值的获取

查找表需要经过两次更新, 才能得到 Hash 值. 在每个明文块处理的过程中完成第一次更新, 原来的 ϕ_i 被变换成 ϕ_{i+1} , 这里的 ϕ_{i+1}, ϕ_i 代表明文空间与索引空间的映射. 图3中给出了更新过程. 在每块明文的加密过程中, 从当前明文块相应的索引项 T_{C_i}



(b)

图2 加密-解密过程

开始, P_i 内部的 Q_i 一组按以下规则实现交换:

$$T_{C_i \bmod N} \leftrightarrow T_{j \bmod N}, \quad T_{(C_i+P_i) \bmod N} \leftrightarrow T_{(j+P_i) \bmod N}, \\ \dots, T_{(C_i+Q_i \times P_i) \bmod N} \leftrightarrow T_{(j+Q_i \times P_i) \bmod N}$$

这里 $N=2^n$, n 是每个明文块的长度, 而

$$j = \begin{cases} C_i + \tilde{m} & \tilde{m} \neq 0 \\ C_i + 1 & \tilde{m} = 0 \end{cases}$$

假定: $\phi_i(T_{C_i}) = S_{C_i}$, 则更新后 $\phi_{i+1}(T_{C_i}) = S_{j_i}$.

当所有明文块被处理完毕, 开始第二次更新. 基于当前的初始值 x_0 , 一维分段线性映射被迭代 N 次 ($N=2^n$ 是查找表的项的个数), 获得一个混沌序列 $\{x_0, x_1, \dots, x_i, \dots, x_{N-1}\}$, 经过四舍五入的原则将该混沌序列转化成整数序列 $\{y_0, y_1, \dots, y_i, \dots, y_{N-1}\}$, 然后依次交换第 i 次索引项与相应的 y_i 次索引项.

查找表的更新过程与密钥和明文均相关, 确保

了加解密过程中算法的安全性, 同时完全由明文的内容来确定查找表的获得, 不同的明文所产生的最终查找表必定不同. 加密、解密的过程完全符合单向散列函数的定义, 而最终获得的查找表的索引项即为整段明文所对应的散列值. 可见, 该算法具备可以组合完成加解密和散列运算的特性. 查找表及新过程如图 3 所示.

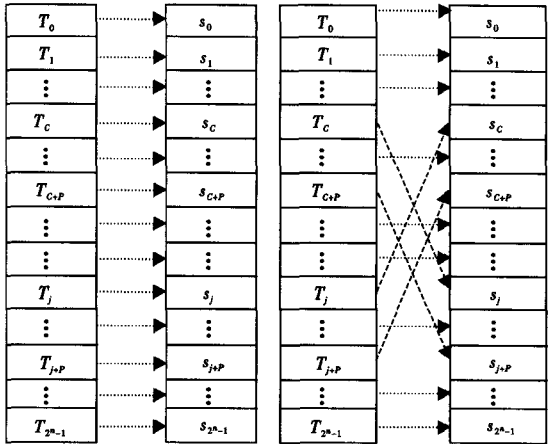


图3 查找表更新过程

3 网络化制造文件安全传输系统设计

利用上面的混沌加密散列组合算法, 论文设计了一个网络化制造环境下的文件安全传输系统. 该系统的主要功能有: 对需要存储和传送的文件进行加密、解密; 对传送的文件进行完整性检验等. 系统的具体实现原理如图 4 所示.

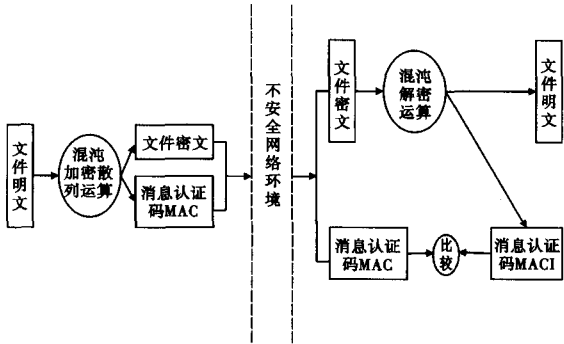


图4 基于混沌加密散列组合算法的安全文件传输系统原理图

发送方:

- (1) 经过混沌加密散列算法运算, 需要传送的文件明文被转换为文件密文及其消息认证码 MAC;
- (2) 通过网络环境传送文件密文和消息认证码 MAC.

接收方:

(1) 利用混沌解密算法,接收方所接收到的文件密文,被转换为文件明文和消息认证码 MAC1,同时接收方通过网络获得消息认证码 MAC;

(2) 接收方对还原的消息认证码 MAC1 和新得到的消息认证码 MAC 进行比较,根据两者相等与否,实现对文件传送完整性的检验,进而完成了文件的安全传输。

4 系统实现

4.1 系统的密钥管理问题

本系统的密钥管理问题分为两个部分:密钥产生和密钥传输。

密钥产生部分的任务是为传输系统中的加密散列算法生成相应的密钥。在产生混沌加密散列组合算法的密钥的注意事项是:需要保证初始值 $x_0 \in (0,1)$ 而控制参数 $b \in (0,1)$,使得一维分段线性映射产生混沌现象。

4.2 系统的开发环境及模块设计

本系统用 Visual C++ 开发实现,开发平台是安装 Windows 系列操作系统的普通 PC 机。

整体上,系统分为客户端和服务端两部分,分别由主控模块(用户界面)、文件加密散列模块和网络功能模块等共同组成。

在网络功能模块里,通过建立 MFC 的 CSocket 类的子类,分别调用 OnAccept() 和 OnReceive() 成员函数,实现建立连接、监听连接和保障通信等功能。

文件加密散列模块是系统的核心模块,主要在客户端和服务端分别完成文件加解密和散列功能,即对上面的混沌加密散列组合算法进行实现,它们在后台运行。在此过程中,将涉及双精度浮点数运算。由于 IEEE 754 浮点数标准事实上在 1980 年以后生产的所有计算平台上都能找到,本算法依据该标准实现。显然,只要都遵守 IEEE754 浮点数标准和相同的运算顺序,不论两个计算平台的操作系统、编程语言是否相同,在相同的密钥控制下产生的计算结果总是相同的。

在主控模块(用户界面)里,为用户和系统提供交互的界面,每个交互的阶段都有相应的窗口。比较有特色的部分是:在调用文件加密散列模块时,采用树性结构显示整个计算机中的各种文件信息,由于界面类似于 Windows 资源管理器,使用本系统的用户通过主菜单和鼠标快捷菜单,就可方便地实现对

文件的加密、解密、散列和网络传送等功能。

4.3 系统性能分析

以下样本明文被用于验证本系统加解密和散列性能实验:“ChongQing TIANRUI Chemical Engineering Equipment Company is a corporate enterprise constituted of the former ChongQing SHUDONG Air Finned Cooler Factory, the former ChongQing Chemical Engineering Machine Works and ChongQing Heat Exchanger Research Institute. Its main business scope includes the R&D, design and manufacturing of air finned cooler, air evaporative cooler and other efficient heat exchangers.”。

实验条件被设定为:明文分组长 $n=8$ 位,相应的明文空间为 $M=\{s_0, s_1, \dots, s_{2^n-1}\}$,其中 $s_i=i(i=0,1,\dots,2^n-1)$,混沌系统初始值 $x_0=0.232\ 223$,控制参数 $b=0.454\ 445, g=0$ 。

通过图 5,可以清楚地对比加密前后明文密文的统计特性。设明文共计 L 组,其中明文分组值为 w 的组数为 L_w 组, $w \in \{0,1,2,\dots,2^8-1\}$,横坐标表示 w ,纵坐标表示 $\frac{L_w}{L}$,按 8 位分组后,各组明文出现的频率如图 1 所示。对应的,设该密文共计 L 组,其中密文分组值为 u 的组数为 L_u 组, $u \in \{0,1,2,\dots,2^8-1\}$,横坐标表示 u ,纵坐标表示 $\frac{L_u}{L}$,加密后密文的频率如图 6 所示。通过比较上图和下图,可见密文与明文的统计特性有显著差别,而加密后的密文分布比较均匀。

通过图 6,可以对比明文的 ASCII 分布图 and 对应散列值的十六进制分布图。消息明文的 ASCII 码值比较集中地分布在一个较小的范围内,如上图所示;而十六进制 Hash 值则呈非常均匀的分散状态,如下图所示。可见,混乱、扩散保证了 Hash 值已不包含消息的任何信息。

香农理论告诉我们,算法的统计特性可以用于安全算法安全性的分析。如果加密/散列前后文件的统计特征变化越大,说明密文/散列值的分布越均匀,则算法抵抗基于统计的攻击能力就越强^[6]。

另外,在本系统中,查找表中与“预处理过的明文分组”对应项的索引值被记为密文,保持了密文/明文比恒为 1。这对于减少密文数据的传输量和增大唯一解距离都极为有利。

本系统还有一个特点。在网络化制造环境下进

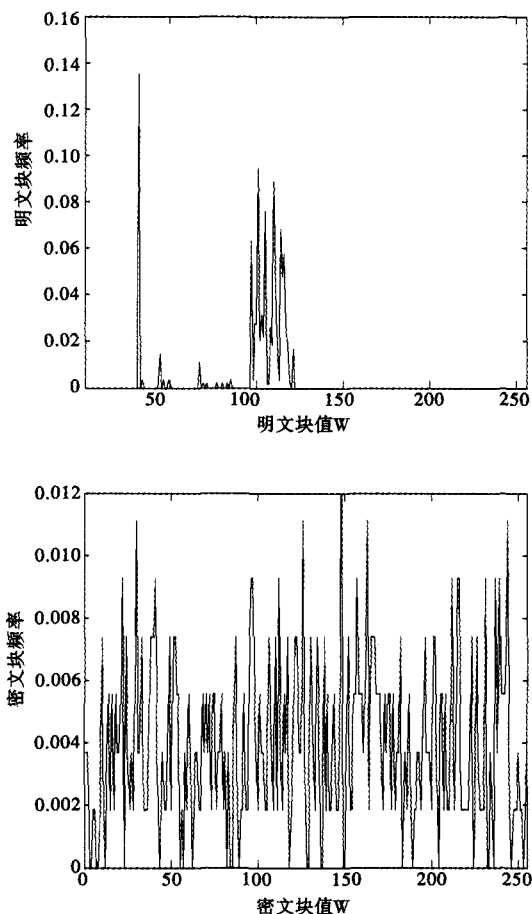


图5 加密前后明文密文统计特性对比

行文件传输时,既需要对明文加、解密运算又需要获得明文的散列值.为了适应这种需要,基于混沌的加密散列组合算法被巧妙地用于整个系统的核心,可以同时完成对文件的加解密和散列功能,在很大程度上简化了文件安全传输系统.与分别单独实现这些功能的其它算法相比,本系统可以极大地提高文件处理的效率.

5 结束语

本文基于某大型企业网络化制造平台的开发实践,以混沌密码学的混沌加密散列组合算法为核心,设计和实现了一个网络化制造文件安全传输系统,可以完成对文件的加密/解密、散列和完整性检验等功能.该系统操作方便、安全高效,可以在网络化制造过程中安全高效地传送文件,具有很大的实际推广潜力.

参考文献:

- [1] 林婷婷,王晓峰.面向网络化制造环境的多功能门限数字签名[J].计算机集成制造系统,2009,15(8):1645-1649.

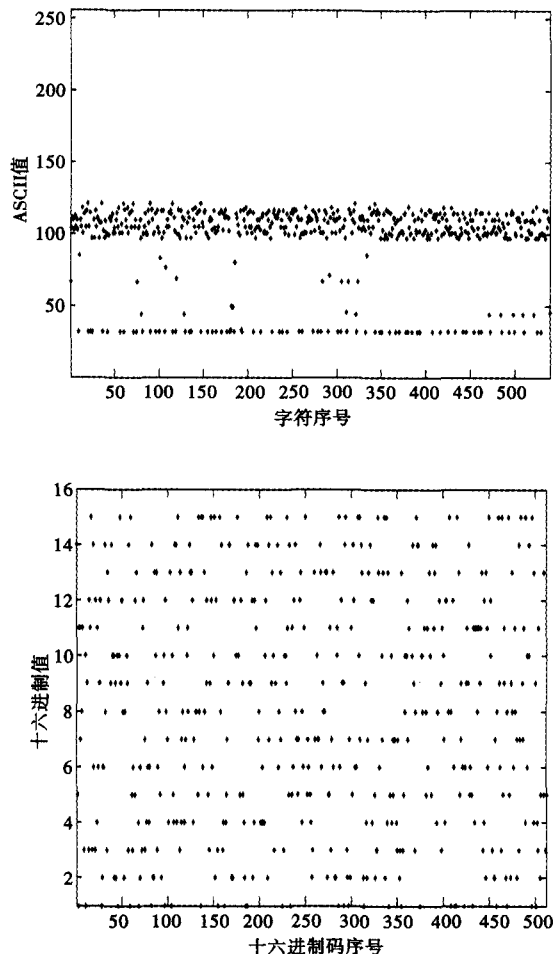


图6 明文的 ASCII 分布图和对散列值的十六进制分布图

- [2] 盛苏英,吴新华.一种混沌图像加密算法的研究与改进[J].微电子学与计算机,2010,27(10):61-68.
- [3] 周蕊,于晓明,焦占亚.一种基于混沌序列的数字图像加密算法[J].微电子学与计算机,2010,27(12):62-64.
- [4] 盛苏英,吴新华.一种新的图像加密算法研究与应用[J].微电子学与计算机,2011,28(2):124-128.
- [5] Deng Shaojiang, Xiao Di, Li Yantao, et al. A novel combined cryptographic and hash algorithm based on chaotic control character [J]. Communications in Non-linear Science and Numerical Simulation, 2009, 14 (11): 3889-3900.
- [6] Xiao Di, Liao Xiaofeng, Wong Kwok-Wo. Improving the security of a dynamic look-up table based chaotic cryptosystem [J]. IEEE Transactions on Circuits and Systems-II, 2006, 53 (6): 502-506.

作者简介:

雷正桥 男,(1973—),硕士研究生,讲师.研究方向为制造业信息化、网络安全技术.