文章编号:1674-7070(2010)02-0190-03

数字指纹技术在电力系统信息保护中的应用

王玉军[1]　丁妮[2]

摘要

针对电力系统中信息数据安全问题,提出运用数字指纹技术进行数据保护,并将基于混沌序列的数字指纹技术在电力系统开发过程中加以应用. 结果表明,该技术有助于电力系统中重要数据的保护.

关键词

数字指纹;数据保护;电力系统;混沌序列

中图分类号 TP309.2

文献标志码 A

0　引言

Introduction

计算机技术与网络技术在电力系统中应用广泛,它在推动电力系统信息化快速发展的同时,也给系统中的信息数据带来了安全隐患,使得电力系统中信息数据安全问题的研究成为热点. 数字指纹技术[1]通过进行指纹编码,将不同的码字序列嵌入到要保护的信息数据中,以达到数据保护的目的. 指纹编码的好坏直接决定数据保护的成功与否,是数字指纹技术的核心. 本文概述了数据指纹嵌入技术,提出了基于混沌序列的数字指纹编码方案,实现了基于混沌序列的数字指纹技术在电力系统中信息数据保护的应用.

1　数字指纹嵌入

Digital fingerprint embedding

1.1　信息隐藏

数字指纹嵌入技术使用信息隐藏[2]技术来实现. 信息隐藏主要是利用人的感觉器官对数字信息的感觉冗余,以数字媒体或数字文件为掩饰物将被隐藏信息掩藏于掩蔽信息之中. 信息隐藏的首要目标是达到隐藏的隐蔽性,也就是加入隐藏信息后的载体应没有明显变化[3]. 信息隐藏的一般传输模型见图1.

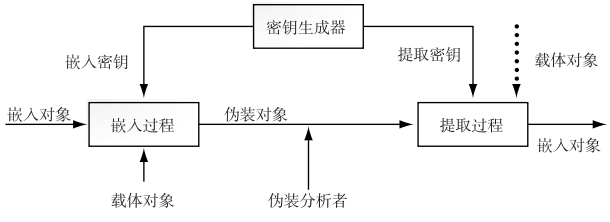

图1　信息隐藏系统的一般模型

Fig. 1　General model of information hiding system

用于隐藏数字化信息的载体可以是任何一种数字信息,如电力系统中的合同文本、竞价标书等内容. 信息隐藏技术一般包括信息嵌入算法和信息检测/提取算法两部分. 此外,在非机密文件受到各种处理(如图像压缩、格式变换等)后,信息隐藏还必须具备隐藏的机密信息免受破坏的免疫力. 但是,正如任何事物都具有两面性一样,在信息隐藏中,

收稿日期 2010-03-29

作者简介

王玉军,男,硕士,工程师,2007年南京信息工程大学系统分析与集成专业研究生毕业,研究方向为信息安全. wangyj@ naritech. cn

1　国电南瑞科技股份有限公司,南京,210061

2　南京信息工程大学 计算机与软件学院,南京,210044

隐藏的信息量与隐藏的免疫力始终是一对矛盾,不存在同时满足这两种要求的隐藏方法. 因此,在实际使用中,只能根据需求适当的予以平衡.

1.2 指纹嵌入

数字指纹嵌入时一般要注意以下几点:

1) 隐蔽性:指纹嵌入最基本的要求是不可见性,即指纹处理过程不会降低或破坏载体的视觉质量和商业价值.

2) 安全性:是指数字指纹所具有抵抗恶意攻击的健壮性.

3) 鲁棒性:指纹嵌入算法应能抵制标准的或恶意的数据处理所引入的任何失真.

需要指出的是,鲁棒性是数据信息保护所必须的性质,数字指纹的根本目标就是通过一种既不引起被保护产品感知上退化,又难以被用户删除的方式向数字产品中嵌入标记.

指纹嵌入时,在将指纹信息扩频处理后,嵌入指纹信息直接叠加到宿主信号(数据信息经过小波变换后的小波系数)中[4]. 假设宿主信号是用向量 $\boldsymbol{X}$ 表示,嵌入指纹后的数据为 $\boldsymbol{Y}=\boldsymbol{X}+\boldsymbol{S}$. 在指纹检测前,由于被破坏,数据可能会产生加性失真,因此有宿主信号 $\boldsymbol{X}$ 和失真 $\boldsymbol{Z}$ 两种干扰源阻碍检测,将这两种干扰合并表示为 $\boldsymbol{d}$ 以简化符号. 待检测数据 $\boldsymbol{Y}$,可以用数学表示为

$$\boldsymbol{Y}=\boldsymbol{S}+\boldsymbol{d}.$$

嵌入数据被认为是在噪声环境下要检测到的信号. 对于普通的扩频嵌入,可以通过下面简化的双极性模型的研究实现:

$$\begin{cases} H_0:\boldsymbol{Y}=-\boldsymbol{S}+\boldsymbol{d}, & b=-1, \\ H_1:\boldsymbol{Y}=+\boldsymbol{S}+\boldsymbol{d}, & b=+1. \end{cases}$$

式中$\{\boldsymbol{S}\}$为已确定的扩频序列,该序列每个分量通常被乘以一个合适的强度因子 α,α 由人眼视觉系统模型的感知差异(JND,Just Noticeable Difference)确定,b 用于 $\boldsymbol{S}$ 的双极性调制,$\boldsymbol{d}$ 为所有噪声.

采用小波域嵌入技术和扩频通信技术的指纹嵌入过程如图 2 所示.

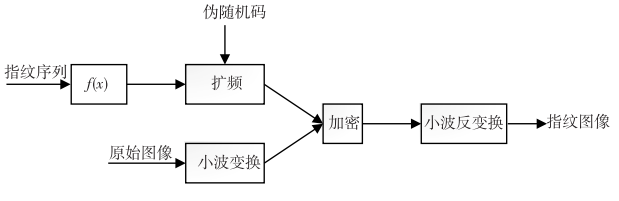

图 2 数字指纹的嵌入

Fig. 2 The embedding of digital fingerprint

2 混沌序列的指纹编码

Fingerprint coding of chaotic sequence

混沌序列的生成通常可采用一个简单的混沌系统 Logistic 映射[5]来实现,它可定义为

$$s_i+1=\mu s_i(1-s_i),\quad \mu\in[1,4],\quad i=0,1,2,\cdots.$$

初始值选为 $0<s_0<1$,这样得到的序列 s 的取值范围是单极性的,且 $0<s_i<1$. μ 通常选为接近 4 的实数. 本文采用的 s_0 初值为 0.88,μ 初值为 3.76. 为了将生成的实数序列 s 转化为二进制序列 p,可以采用如下两种方法:1)以 0.5 为阈值,若 $s_i\geqslant 0.5$,则对应的 $p_i=1$;否则 $p_i=1$. 2)由于 $0<s_i<1$,可将(0,1)区间分为 256 等分,每一等分用 8 位二进制数表示,例如若离第 7 个等分(标记为 6,二进制为 00000110)的中心值最近,则 $p_{i\times 8+1}=p_{i\times 8+2}=1$,而 $p_{i\times 8+7}=\cdots=p_{i\times 8+3}=p_{i\times 8}=0$. 因此,序列 p 的长度为序列 s 的 8 倍.

为了得到最后的嵌入内容 w,可采用将上面得到的二值序列 p 与二进制随机码字的用户 u 的指纹信息序列 a_u 直接异或的方法,即

$$w=\{w_i \mid w_i=p_i\oplus a_u i,\quad i=0,1,2,\cdots\}.$$

值得注意的是,有时为了得到双极性的序列,可以采用另一种 Logistic 映射如下:

$$s_{i+1}=1-\mu s_i^2,\quad \mu\in[0,2],\quad s_i\in[-1,1].$$

取 $\mu=2$ 的偶对称映射,此时轨迹点的概率密度为

$$\rho(x)=\frac{1}{\pi\sqrt{1-x^2}},\quad x\in[-1,1].$$

而对于一般的混沌映射 $s_{i+1}=f(s_i)$,概率密度 $\rho(y)$ 可由 Perron-Frobenious 方程得到为

$$\rho(y)=\sum_{\{s_i=f^{-1}(y)\}}\frac{\rho(s_i)}{\left|f'(s_i)\right|}.$$

设 $f(x)$ 是从 $[-1,1]$ 到 $[-1,1]$ 的偶对称映射,且它的概率密度也是偶对称的,因此,理论上每个混沌序列中 0 和 1 出现的概率相同.

3 算法实现

Algorithm implementation

下面是 Java 语言实现的混沌序列码的部分代码.

```
public class ChaosFinger {
    private int codeLength;
    private int repTimes;
    /*
     * 产生混沌序列类的构造函数
     * params:codeLength 编码码字长度,rep-
```

```
Times 重复嵌入次数;
        */
    public ChaosFinger(int codeLength,int repTimes) {
        this. codeLength = codeLength;
        this. repTimes = repTimes;
    }
    /*
     * 根据算法产生用户指纹,返回值是混沌序列的用户指纹
     */
    public StringBuffer createFinger( ) {
    }
}
```

4 结果分析
Results analysis

混沌序列对初值的敏感性高,即初值有微小的变化,将造成系统不可预测的改变. 所以,由混沌方法产生的二进制混沌序列具有良好的安全性. 实验中采取的初始值分别为 0.88、0.89、0.9,然而得到的二进制混沌序列却有很大的变化. 表 1 的数据说明了二进制混沌序列具有对初值的敏感的特性.

表 1 初值不同的二进制混沌序列

Table 1 Binary chaotic sequences with different initial values

初值	二进制混沌序列
0.88	000011100111110100001001100010100101000001101000011011001010000 1
0.89	101001000000110010101110100111011011001101011001001001100010111 1
0.90	000010110000100100101111100010111111110101110010111010111111100 1

混沌序列具有普通伪随机序列所没有的低通特性,以抵抗低通滤波. 混沌序列中的 $f(x)$ 是定义域上的偶对称映射,且它的概率密度也是偶对称的,因此,理论上每个混沌序列中 0 和 1 出现的概率相同.

上述混沌序列的初值敏感性和低通特性,对信息数据保护有着很好的效果,因此混沌序列适用于数字指纹的信息保护技术.

5 结束语
Concluding remarks

数字指纹技术是解决信息数据保护的有力工具. 基于混沌序列的数字指纹技术能更好地解决信息保护技术本身存在的一些问题,将其应用到电力系统中,有助于解决重要数据(如合同文本、竞价标书等)的保护,对于整个电力市场建设有着重要的现实意义.

参考文献
References

[1] 吕述望,王彦,刘振华. 数字指纹综述[J]. 中国科学院研究生院学报,2004,21(3):289-298
LÜ Shuwang, WANG Yan, LIU Zhenhua. A survey of digital fingerprinting[J]. Journal of the Graduate School ot the Chinese Academy Sciences, 2004, 21(3): 289-298

[2] 刘振华,伊萍. 信息隐藏技术及其应用[M]. 北京:科学出版社,2002
LIU Zhenhua, YI Ping. Information hiding technology and its aplication[M]. Beijing: Science Press, 2002

[3] 杨义先,钮心忻. 多媒体信息伪装综论[J]. 通信学报,2002,23(5):32-33
YANG Yixian, NIU Xinyi. Review of multi-media information camouflage[J]. Journal of China Institute of Communications, 2002, 23(5): 32-33

[4] 程正兴. 小波分析算法与应用[M]. 西安:西安交通大学出版社,2006
CHENG Zhengxing. Wavelet analysis algorithm and its application [M]. Xi'an: Xi'an Jiaotong University Press, 2006

[5] 王彦,吕述望,徐汉良. 一种二进制数字指纹编码算法[J]. 软件学报,2003,14(6):1172-1177
WANG Yan, LÜ Shuwang, XU Hanliang. A digital fingerprinting algorithm based on binary codes[J]. Journal of Software, 2003, 14(6): 1172-1177

The Application of digital fingerprint technology in data protection of the power system

WANG Yujun[1] DING Ni[2]

1 NARI Technology Development Co Ltd, Nanjing 210061

2 College of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044

Abstract To solve the problem in information security of the power system, a digital fingerprint method is proposed in data protection. The digital fingerprint technology based on chaotic sequence is applied in the development of the power system. Results indicate that the effective parts of the technology can aid data protection.

Key words digital fingerprint; data protection; power system; chaotic sequence