基于频率水印的智能电网实时数据认证方法

陈 晟[1],黄 茜[2],张 宇[3]
(1. 江苏省电力公司,江苏 南京 211102;2. 江苏泰州供电公司,江苏 泰州 225300;
3. 浙江大学 电气工程学院,浙江 杭州 310027)

摘要:针对智能电网建设中通信网络数据安全问题,结合智能电网通信网络特点,提出一种将电网频率信息应用于实时交互数据认证的方法。针对电网实时频率检测网络进行频率水印建模,利用分数阶傅里叶变换在发送的数据中嵌入频率水印,根据嵌入的水印对接收的数据进行安全认证。分数阶傅里叶变换分散了嵌入信息在传统时频域的能量分布,安全性好。仿真与实验结果表明,基于分数阶傅里叶变换的频率水印嵌入算法具有较高的安全性,并对常规的噪声攻击、低通滤波攻击和下采样攻击具有抵抗能力。

关键词:智能电网;频率;水印;认证;傅里叶变换;数据安全
中图分类号:TN 911.7;TN 918.912 **文献标识码**:A DOI:10.3969/j.issn.1006-6047.2014.07.028

0 引言

智能电网是将现代先进的传感测量技术、通信技术、信息技术、计算机技术和控制技术与物理电网高度集成而形成的新型电网,因此智能电网的构建需要新一代大容量、高速实时、具有业务感知能力的信息通信系统[1]。在智能电网建设中其通信网络数据安全问题引起广泛关注。智能电网中的各智能终端(例如智能电表)可能通过开放的网络甚至无线网络接入服务器,其传输的电能信息成为黑客攻击的潜在目标。如何保证智能电网中海量实时信息的安全直接关系电力企业运行、管理及控制系统的安全,成为智能电网建设中亟待解决的重大问题[2-3]。数据加密及认证技术是保证网络信息安全的重要手段。

利用电网本身特征对电网数据进行加密是一种突破传统密码系统[4-5]的智能电网加密方法。由于发配电单位及各种类型负载的不同,电网不同区段不同时刻的交流电频率及相位存在差异,这种随机差异难以伪装。频率水印技术就是在传统安全技术的基础上,将电网中实时变化的频率量值作为加密用的"指纹",构造保证信息安全性的"第二把钥匙",力图实现对重要信息的认证与定位,以保证其在公用网络流动的安全性[6]。

对电网动态频率信息的提取与利用日益得到了研究者的重视[7-8]。2000 年,美国多高校联合建立了 GPS 同步的电网实时频率监测系统(FNET)[9],对美国境内各地区电网频率差异进行实时监测并建立了频率数据库。频率数据库的建立为进一步利用频率信息进行交互数据认证提供了实现基础。2007 年,Catalin Grigoras 等人研究了将电网频率信息用于计算机音视频数据安全认证的方法[10-11],其提出的方法主要应用于安全监控系统,但为频率信息在智能电网中的应用提供了思路。随后,Daniel、Catalin 和我国的姚秋明等人研究了将电网频率及相位信息用于数据认证的算法,但其应用大多局限于监控系统的音频和视频数据认证[12]。近年来,我国电力部门和各高校开始联合研究电网实时 FNET,着手构建统一的国家电网频率数据库,利用 GPS 和 Internet 进行同步和数据通信[13],并提出了将 FNET 的频率数据进行数据认证的前沿课题。该系统的建立对于国家电网电能质量监督和智能电网构建具有重要意义。

本论文针对智能电网通信网络特点,提出一种将电网频率信息应用于实时交互数据认证的方法,其主要内容包括:针对电网实时频率检测网络进行频率水印建模;分数阶傅里叶变换频率水印嵌入算法;频率水印提取与认证方法;噪声与常规攻击下的频率水印鲁棒性等。由于分数阶傅里叶变换分散了嵌入信息在传统时频域的能量分布,因此本文提出的方法伪装性很强。基于电网频率实验数据库的仿真与实验结果表明,分数阶傅里叶变换的频率水印嵌入算法具有较高的隐秘性和安全性,并对常规的噪声攻击、低通滤波攻击和下采样攻击具有抵抗能力。

1 基于电网实时频率监测网络的频率水印嵌入模型

电网实时频率监测网络的核心是与精确频率记录仪和强大的中央处理系统相连的广域通信网。通过电网频率特征参数的提取、记述、变换、加工和表现方法可以对电网频率水印进行建模。

虽然电网的理想频率为 50 Hz,但由于发配电机组的差异、负载的不平衡,实际电网频率在 50 Hz 附近变化。对电网实时信号进行采样,得到的采样电压理想波形与实际波形分别如图 1(a)、(b)所示,经傅里叶变换得到的幅度谱分别如图 1(c)、(d)所示。

收稿日期:2013-09-28;修回日期:2014-06-04

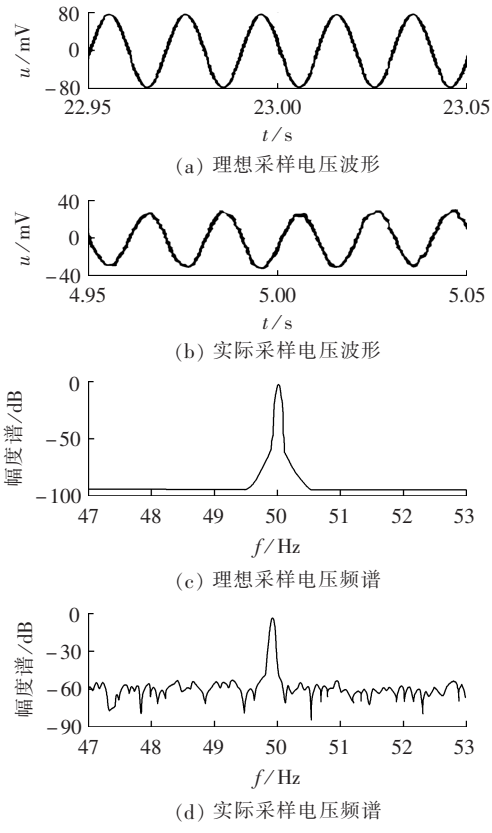

图 1 理想与实际采样电压波形与频谱示意图

Fig.1 Waveforms of ideal and actual sampled voltages and corresponding spectra

因此,实际电网频率应表示为:

$$f=50\ \text{Hz}\pm\Delta f \tag{1}$$

其中,Δf为某时刻的频移量。

电网中任何不同时刻和地点其频移量都是不同的,提取频移曲线有不同方法,如图 2 所示为 2 种频移特征提取方法的时–频域谱图。图 2(a)用灰度表示了 14000 采样点的时–频域谱图,图 2(b)为加短时窗的时–频域谱图。

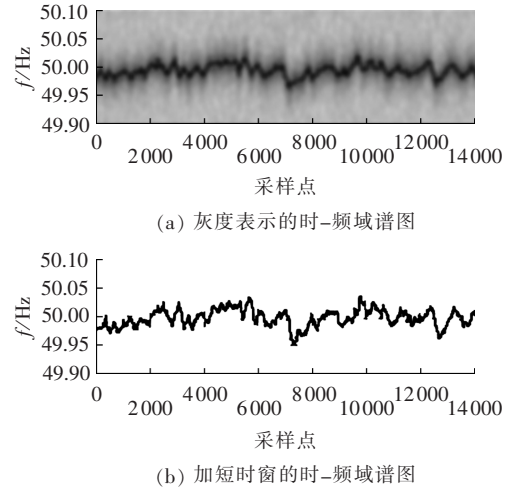

图 2 频移曲线的 2 种时–频域谱图

Fig.2 Two time-frequency spectrograms of frequency-shift curve

因此,电网频移信息为实时变化的随机信号,提取该随机信号的特征可用于频率水印的建模。在智能电网中,传送数据的终端设备利用本地电网频移信号生成并嵌入水印,接收设备从接收数据中提取水印,恢复嵌入的频移特征,与电网实时频率监测网络中记录的该地该时刻频移特征进行比对,通过决策系统即可判别数据是否被篡改。电网频移信号所提取的特征用于生成频率水印,水印嵌入模型见图 3。

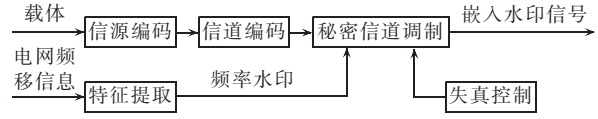

图 3 水印嵌入模型

Fig.3 Model of watermarking embedding

2 基于分数阶傅里叶变换的频率水印嵌入算法

选择秘密信道嵌入频率水印有多种方法,如:最低有效位(LSB)隐藏方法,即通过将载体数据的最小权值位用代表秘密数据的二进制位替换,将频率水印嵌入[14];基于统计量的隐藏方法,即将秘密信息嵌入到载体数据的某个统计值中,通过适当地修改某个统计值来嵌入水印;变换域法,即将秘密信息嵌入到载体数据的某个变换域中,以达到将秘密信息嵌入到载体中最重要部分的目的,这样,即使发生信道退化或者数据受到攻击破坏,嵌入信号中的水印信息也不会消失。

近年来,如何利用变换域进行隐秘数据嵌入成为研究人员广泛关注的热点和难点。分数阶傅里叶变换是傅里叶变换的一种广义推广形式。在时–频平面,如果将傅里叶变换线性算子看作是从时间轴逆时针旋转 $\pi/2$ 到频率轴,则分数阶傅里叶变换算子就是可旋转任意角度的算子。

p 阶分数傅里叶变换算法如下:

$$S_p(u)=F^p(s(t))=\sqrt{\frac{1-\mathrm{j}\cot p\pi}{2\pi}}\times \int_{-\infty}^{+\infty}\exp\left(\mathrm{j}\frac{u^2+t^2}{2}\cot p\pi-\frac{\mathrm{j}ut}{\sin p\pi}\right)s(t)\mathrm{d}t\quad 0<|p|<2 \tag{2}$$

进一步变换可得:

$$S_p(u)=\sqrt{\frac{1-\mathrm{j}\cot p\pi}{2\pi}}\exp\left(\mathrm{j}\frac{u^2}{2}\cot p\pi\right)\times \int_{-\infty}^{+\infty}\exp\left(\mathrm{j}\frac{t^2}{2}\cot p\pi-\frac{\mathrm{j}ut}{\sin p\pi}\right)s(t)\mathrm{d}t \tag{3}$$

令

$$s(t)=\exp\left(\frac{-\mathrm{j}\cot p\pi\cdot t^2}{2}+\frac{\mathrm{j}u_0t}{\sin p\pi}\right) \tag{4}$$

代入可得:

$$S_p(u)=\sqrt{\frac{1-\mathrm{j}\cot p\pi}{2\pi}}\exp\left(\mathrm{j}\frac{u^2}{2}\cot p\pi\right)\times$$
$$\int_{-\infty}^{+\infty}\exp\left(\mathrm{j}\frac{t^2}{2}\cot p\pi-\frac{\mathrm{j}ut}{\sin p\pi}\right)\times$$
$$\exp\left(-\mathrm{j}\frac{t^2}{2}\cot p\pi+\frac{\mathrm{j}u_0t}{\sin p\pi}\right)\mathrm{d}t=$$
$$\sqrt{\frac{1-\mathrm{j}\cot p\pi}{2\pi}}\exp\left(\frac{\mathrm{j}u^2}{2}\cot p\pi\right)\times$$
$$\int_{-\infty}^{+\infty}\exp\left[-\frac{\mathrm{j}(u+u_0)t}{\sin p\pi}\right]\mathrm{d}t=$$
$$\sqrt{\frac{1-\mathrm{j}\cot p\pi}{2\pi}}\exp\left(\mathrm{j}\frac{u^2}{2}\cot p\pi\right)\delta\left(\frac{u+u_0}{\sin p\pi}\right)\quad(5)$$

从上式可以看出，通过对 $s(t)$ 进行 p 阶分数傅里叶变换，在分数傅里叶域上形成了 δ 函数。而由于分数傅里叶变换满足 Parseval 准则，即：

$$\int_{-\infty}^{+\infty}f(t)g^*(t)\,\mathrm{d}t=\int_{-\infty}^{+\infty}f_p(u)g_p^*(u)\,\mathrm{d}u\quad(6)$$

因此根据能量守恒关系，从上式中可看出，在不同于 p 的 p_2 阶分数傅里叶变换信号的能量相对进行了扩散，而在 p 阶分数傅里叶变换中，高斯类函数具有能量聚焦特性。这一特性有助于隐藏信息的分离，提高信息隐藏的抗攻击性能。

下面以时域及频域方差最小为目标，通过理论分析不同嵌入位置对时域及频域产生的影响，寻找阶数 p 和最佳嵌入位置的关系。

如果在 p 阶分数傅里叶变换域嵌入水印隐秘数据，令：

$$\hat{X}_p(u)=X_p(u)+S_p(u)\quad(7)$$

其中，$S_p(u)$ 为傅里叶变换域上的隐秘信息。采用最小均方误差准则，则时－频域上的均方误差为：

$$J=E[\,\|x(t)-\hat{x}(t)\|^2+\|X(\omega)-\hat{X}(\omega)\|^2]=$$
$$E[\,\|s(t)\|^2+\|S(\omega)\|^2]\quad(8)$$

根据分数傅里叶变换的阶数叠加性，则有：

$$s(t)=[F^0(s(t))]=[F^p(s(t))]^{-p}=$$
$$[S(u_p)]^{-p}=S_{-p}(u_p)\quad(9)$$
$$S(\omega)=[F^1(s(t))]=[F^p(s(t))]^{1-p}=$$
$$[S(u_p)]^{1-p}=S_{1-p}(u_p)\quad(10)$$

代入式(8)可得：

$$J=E[\,\|S_{-p}(u)\|^2+\|S_{1-p}(u)\|^2]=$$
$$E\left\{\int_{-\infty}^{+\infty}[S_{-p}(u)S_{-p}^*(u)+S_{1-p}(u)S_{1-p}^*(u)]\mathrm{d}u\right\}=$$
$$E\left[(1+SS^*)\int_{-\infty}^{+\infty}S_{-p}(u)S_{-p}^*(u)\mathrm{d}u\right]\quad(11)$$

要使均方误差 J 最小，必须满足：

$$\frac{\partial J}{\partial u}=\frac{\partial\left\{E\left[(1+SS^*)\int_{-\infty}^{+\infty}S_{-p}(u)S_{-p}^*(u)\mathrm{d}u\right]\right\}}{\partial u}\bigg|_{u=0}=$$
$$E\left[(1+SS^*)\int_{-\infty}^{+\infty}\frac{\partial(S_{-p}(u))}{\partial u}S_{-p}^*(u)+\right.$$
$$\left.\frac{\partial(S_{-p}^*(u))}{\partial u}S_{-p}(u)\mathrm{d}u\right]_{u=0}\quad(12)$$

代入式(3)和式(4)，可得：

$$\frac{\partial J}{\partial u}=2E\left[(1+SS^*)\sqrt{\frac{1+\cot^2 p\pi}{2\pi}}\times\right.$$
$$\left.\int_{-\infty}^{+\infty}\cos\left(\frac{u_0}{\sin p\pi}+\frac{u_0^2}{2}\cot p\pi\right)\mathrm{d}u\right]\quad(13)$$

若上式为 0，对应均方误差 J 为最小，则式(14)必须成立：

$$1+\frac{\pi}{2}\sin(2p\pi)>0\quad(14)$$

一般简化取：

$$0<p\leqslant\frac{1}{2}$$

按此方法嵌入水印信息后，可得到：

$$x(t)=s(t)+\lambda\exp\left(-\mathrm{j}\pi\frac{u_0^2\cos^3 p}{\sin p}\right)\times$$
$$\exp(\mathrm{j}\pi 2u_0t\sin p)s'(t-u_0\cos p)\quad(15)$$

对应的频谱则为：

$$X(\omega)=S(\omega)+\lambda\exp\left(-\mathrm{j}\pi\frac{u_0^2\cos^3 p}{\sin p}\right)\times$$
$$\exp(-\mathrm{j}u_0\cos p)S'(\omega-2\pi u_0\sin p)\quad(16)$$

如果对 $x(t)$ 取自相关处理及自相关复倒谱处理，除主瓣有极值外，在 $u_0\cos p$、$u_0\sin p$ 及 u_0 处都没有极值，只有当变换到分数阶因子为 p 的分数傅里叶变换域上再进行自相关倒谱变换，在 u_0 处才能获得极值。换言之，如果未知分数阶因子 p，在时域和倒谱域上将无法发现隐秘信息的存在，在频域由于受到 $\exp(\mathrm{j}2\pi u_0t\sin p)$ 调制的影响，$x(t)$ 与 $s(t)$ 的时域波形和频谱结构可能会有所差异，但若无纯净原始数据比对则难以发觉这种差异，因此，在分数傅里叶变换域中嵌入频率水印数据具有极高的隐秘性。

3　基于电网频率数据库的终端数据置信度评价方法

利用频率水印进行数据认证的过程如图 4 所示。

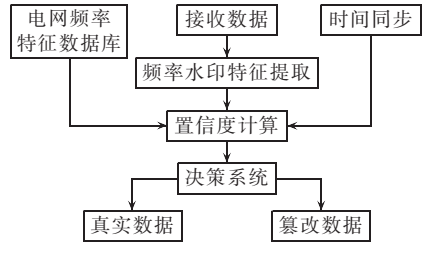

图 4　水印认证过程

Fig.4　Process of watermarking authentication

目前美国、加拿大等国家已经建立了比较完善的电网频率特征数据库，我国正在进行该数据库的研

究与建立工作,电网频率特征数据库的建立为基于频率水印的智能电网实时数据认证提供了基础。

当含有频率水印的终端数据在接收端解调后(解调算法由水印嵌入及秘密信道调制算法决定),所提取出的电网频率特征参数进入置信度评价系统,并最终作出决策[15]。采取多种特征参数加权的联合评分模型可以避免由于某一种评分模型的特异性造成的偏颇。整个评分过程分为3个部分:首先,验证频率水印的正确性,这可由隐马尔科夫或状态虚拟机算法完成,将频率水印与电网频率特征数据库中的该时刻频率模板中的数据比较,如果可以认定其为与预期的水印数据相同则进行下一步测试,如果结果差距较大则认为不正确,立刻结束当前评分;其次,对通过HMM测试的频率水印进行各特征矢量与模板库矢量的差距计算;最后,用加权拟合的方式得出分数,评分分数计算如式(17)所示。

$$\begin{aligned}\text{score}=&w_1\frac{100}{1+a_1(d_1)^{b_1}}+w_2\frac{100}{1+a_2(d_2)^{b_2}}+\cdots+\\&w_n\frac{100}{1+a_n(d_n)^{b_n}}\\&a_1,\cdots,a_n,b_1,\cdots,b_n>0\\&w_1+w_2+\cdots+w_n=1\end{aligned}\tag{17}$$

其中,d_1、d_2、…、d_n为各特征矢量与模板库矢量的距离;a_1、…、a_n和b_1、…、b_n皆为距离转换成分数的参数;w_1、w_2、…、w_n为各个特征的权重。

4 实验与仿真

电网频率实验数据库采集系统如图5所示,其中频率数据测量原理如图6所示。在此实验平台上对频率水印生成、嵌入、提取与认证进行实验和仿真,并对实验数据进行理论分析和评价。

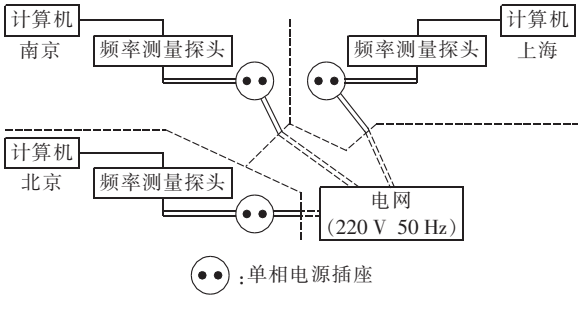

图5 电网频率实验数据库采集系统

Fig.5 Acquisition system of experimental grid-frequency database

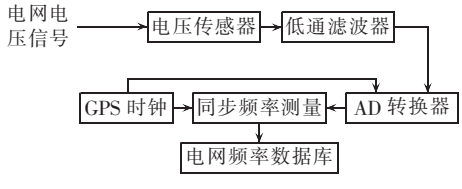

图6 频率数据测量原理

Fig.6 Principle of frequency measuring

信息检出率实验测试信息的隐秘性,即窃听方成功窃取隐藏信息的比率。检出率用P_c表示:

$$P_c=\frac{N_{\text{test}}}{N_{\text{all}}}\times 100\%\tag{18}$$

即为窃听方检出隐藏数据段数与总隐藏数据段数的比值,数值越低表示隐秘性越高。

本文对所提出的基于分数阶傅里叶变换隐藏方法和其他隐藏方法进行了检出率比较。其中分数阶傅里叶变换隐藏信息检出方法的流程如图7所示,假设检出方已知信息隐藏方法,但不知信息隐藏参数(分数傅里叶变换旋转因子)。其他3种信息隐藏方法分别是LSB隐藏方法、低频(LF)隐藏方法以及Hide4PGP V4.0隐藏工具。然后利用Johnson提出的隐藏分析方法[16]对上述包含隐藏信息的语音进行检测,检出率比较结果如图8所示。从图8中可以看出,本文提出的基于分数阶傅里叶变换的信息隐藏方法比其他3种算法的检出率明显降低,隐秘性更强。

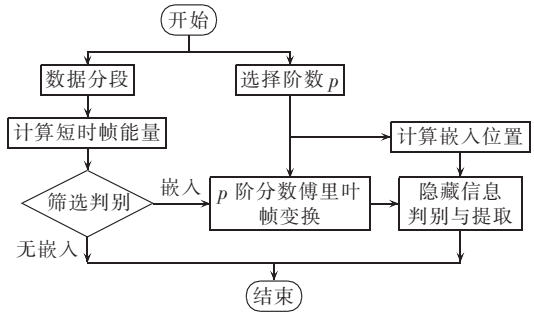

图7 分数阶傅里叶变换隐藏信息检出方法

Fig.7 Flowchart of hidden information detection by fractional Fourier transform

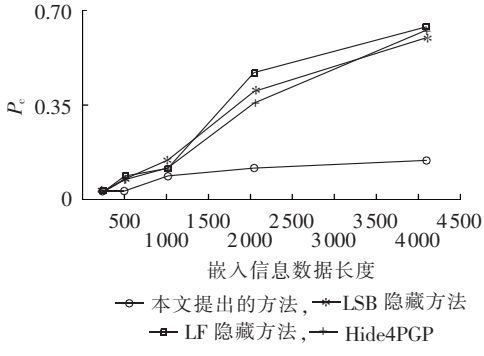

图8 4种隐藏方法的检出率

Fig.8 Detectable rate for four hiding methods

鲁棒性也称为自恢复性或可纠错性,其反映了信息隐藏技术的抗干扰能力。它是指隐藏信息后,数字媒体在传递过程中,虽然经过多重无意或有意的信号处理,但仍能够在保证较低错误率的条件下将秘密信息加以恢复,保持原有信息的完整性和可靠性。鲁棒性也是反映信息隐藏方法抵抗常规信号处理攻击能力的一项重要指标。对隐藏信息常用的攻

击类型有白噪声、有色噪声、低通滤波和下采样攻击等。在保证嵌入能量相同的情况下,本文比较了分数阶傅里叶方法、LSB 隐藏方法及 LF 隐藏方法对各种攻击的鲁棒性能。实验选择误比特率(BER)作为衡量鲁棒性的技术指标,即在各种攻击后提取得到的信息与原始信息间不同比特所占的百分率,其表达如下:

$$\mathrm{BER}=\frac{L_{\mathrm{err}}}{L}\times 100\% \tag{19}$$

其中,L_{err} 为提取的误比特数。

3 种隐藏方法在不同类型攻击下平均误比特率如表 1 所示。由表 1 可知,3 种隐藏方法在相同条件下,LSB 隐藏方法的平均误比特率最高,抗攻击能力最差;而本文提出的基于分数阶傅里叶变换的频率水印方法,由于其在时域和频域中嵌入水印信息,受时域或频域攻击相对影响较小,因此具有较高的抗攻击能力。

表 1　3 种隐藏方法在不同类型攻击下平均误比特率

Tab.1　Average bit error rates for three hiding methods under different attacks

攻击类别	LSB 隐藏方法		LF 隐藏方法		本文方法	
	L_{err}	BER/%	L_{err}	BER/%	L_{err}	BER/%
未攻击	0	0	0	0	0	0
白噪声	2432	59.38	443	10.30	221	5.4
有色噪声	2418	59.03	2232	54.49	254	6.2
低通滤波	3121	76.20	822	20.07	805	19.65
下采样	2218	54.15	946	23.10	768	18.75

5　结论

针对智能电网通信网络中的数据安全问题,本文提出了一种基于频率水印的实时数据认证算法,通过分数阶傅里叶变换嵌入频率水印,提高隐藏信息的伪装性和鲁棒性。电网频率实验数据库系统的仿真实验表明,相比于其他实时水印嵌入算法,本文算法在隐密性和抗攻击能力方面有明显提高。

参考文献:

[1] 陈树勇,宋书芳,李兰欣,等. 智能电网技术综述[J]. 电网技术,2009,33(8):1-6.
CHEN Shuyong,SONG Shufang,LI Lanxin,et al. Survey on smart grid technology[J]. Power System Technology,2009,33(8):1-6.

[2] 韩桢祥,曹一家. 电力系统的安全性及防治措施[J]. 电网技术,2004,28(9):1-6.
HAN Zhenxiang,CAO Yijia. Power system security and its prevention[J]. Power System Technology,2004,28(9):1-6.

[3] 钟金,郑睿敏,杨卫红,等. 建设信息时代的智能电网[J]. 电网技术,2009,33(13):12-18.
ZHONG Jin,ZHENG Ruimin,YANG Weihong,et al. Construction of smart grid at information age[J]. Power System Technology,2009,33(13):12-18.

[4] dos SANTOS A L M,TORREY M E,EI SHESHAI A. Supporting national public key infrastructures using smart cards[J]. International Journal of Computers and Applications,2005,27(1):1-6.

[5] 李明,郝晓玲,张嵩. 公开密钥基础设施体系脆弱性及其对策分析[J]. 哈尔滨工业大学学报,2007,39(4):665-668.
LI Ming,HAO Xiaoling,ZHANG Song. Vulnerability and counterm easure analysis of the public key infrastructure[J]. Journal of Harbin Institute of Technology,2007,39(4):665-668.

[6] LI L,MA Y Y,CHANG C C,et al. Analyzing and removing suresign watermark[J]. Signal Processing,2013,93(5):1374-1378.

[7] GARDNER R M,LIU Yilu. FNET:a quickly deployable and economic system to monitor the electric grid[C]//2007 IEEE Conference on Technologies for Homeland Security. Woburn,USA:[s.n.],2007:209-214.

[8] KOOK K S,LIU Y,BANG M J. Global behavior of power system frequency in Korean power system for the application of frequency monitoring network[J]. Generation,Transmission & Distribution,IET,2008,2(5):764-774.

[9] GRIGORAS C. Applications of ENF criterion in forensic audio,video,computer and telecommunication analysis[J]. Forensic Science International of ScienceDirect,2007,167(11):136-145.

[10] BRIXEN E B. ENF-quantification of the magnetic field[C]//32nd International Conference of Audio Engineering. Denver,USA:[s.n.],2008:1-6.

[11] DANIEL P N,ANTONIO A J. Evaluating digital audio authenticity with spectral distances and ENF phase change[C]//ICASSP 2009. Taipei,China:[s.n.],2009:1417-1220.

[12] 姚秋明,柴佩琪,宣国荣,等. 基于期望最大化算法的音频取证中的篡改检测[J]. 计算机应用,2006,26(11):2598-2601.
YAO Qiuming,CHAI Peiqi,XUAN Guorong,et al. Audio resamping detection in audio forensics based on EM algorithm[J]. Computer Applications,2006,26(11):2598-2601.

[13] 肖登明,徐欣,刘奕路. 基于 Internet 的频率监控网(FNET)[J]. 高电压技术,2001,27(2):39-49.
XIAO Dengming,XU Xin,LIU Yilu. Internet based frequency monitoring network(FNET)[J]. High Voltage Engineering,2001,27(2):39-49.

[14] 汪然,平西建,郑二功. 基于直方图局部平滑度的 LSB 匹配隐写分析[J]. 应用科学学报,2012,30(1):96-104.
WANG Ran,PING Xijian,ZHENG Ergong. Steganalysis of LSB matching based on local smoothness of histogram[J]. Chinese Journal of Applied Sciences,2012,30(1):96-104.

[15] KODOVSKY J,FRIDRICH J,HOLUB V. Ensemble classifiers for steganalysis of digital media[J]. IEEE Transactions on Information Forensics and Security,2012,7(2):432-444.

[16] JOHNSON M K,LYU S,FARID H. Steganalysis of recorded speech[C]//SPIE Symposium on Electronic Imaging 2005. San Jose,USA:[s.n.],2005:664-672.

作者简介:

陈　晟

陈　晟(1966-),男,江苏泰州人,高级工程师,硕士,从事电力系统运行管理分析研究工作(**E-mail**:chenshengtz@sina.com);

黄　茜(1987-),女,江苏泰州人,助理工程师,从事智能电网用户端管理分析研究工作;

张　宇(1993-),男,江苏姜堰人,主要从事信息隐藏与数据认证方法研究。

(下转第 173 页 continued on page 173)

LIAO Ruijin，ZHANG Yiyi，HUANG Feilong，et al. Power transformer condition assessment strategy using matter element analysis[J]. High Voltage Engineering，2012，38(3)：521-526.

[14] 李如琦，苏浩益. 基于可拓云理论的电能质量综合评估模型[J]. 电力系统自动化，2012，36(1)：66-70.
LI Ruqi，SU Haoyi. A synthetic power quality evaluation model based on extension cloud theory[J]. Automation of Electric Power Systems，2012，36(1)：66-70.

[15] 潘科，许开立. 区间可拓法在化工园区应急能力评价中的应用[J]. 东北大学学报：自然科学版，2012，33(9)：1344-1348.
PAN Ke，XU Kaili. Application of the interval extension method for the assessment of emergency response capability[J]. Journal of Northeastern University：Natural Science，2012，33(9)：1344-1348.

[16] HUANG Xiaoqing，JIANG Hao，XIA Anbang. SOA-based integration of electric utility in open electric market[C]//DRPT2008. Nanjing，China：IEEE：2245-2250.

[17] IEC. IEC61970-301 EMSAPI-part301：Common Information Model (CIM) base[S]. Geneva，Switzerland：IEC，2009.

[18] IEC. IEC61970-501 EMSAPI-part501：Common Information Model Resource Description Framework(CIM RDF) Schema[S]. Geneva，Switzerland：IEC，2006.

[19] CORMEN T H，LEISERSON C E，RIVEST R L. Introduction to algorithms[M]. 3rd ed. Cambridge，USA：The MIT Press，2009：603-610.

作者简介：

李功新

李功新(1964–)，男，福建福州人，高级工程师，副教授，博士研究生，主要从事电力系统自动化、电力设备在线监测、设备绝缘诊断等方面的研究工作；

周文俊(1959–)，男，湖北汉川人，教授，博士研究生导师，博士，主要从事高电压绝缘与测试技术、微电子设备防雷接地技术等方面的研究工作；

林静怀(1971–)，男，福建莆田人，高级工程师，硕士，主要从事电网调度工作；

江修波(1960–)，男，福建福州人，教授，主要从事电力系统运行、电力变压器绝缘老化测试等方面的研究工作(**E-mail**：1102517160@qq.com)。

Integrated dispatch control and anti-misoperation system based on D5000 platform

LI Gongxin[1,2]，ZHOU Wenjun[1]，LIN Jinghuai[2]，JIANG Xiubo[3]

(1. College of Electrical Engineering，Wuhan University，Wuhan 430072，China；
2. Fujian Electric Power Company，Fuzhou 350000，China；
3. College of Electrical Engineering and Automation，Fuzhou University，Fuzhou 350116，China)

Abstract：The application of extension theory in the domain of electric power dispatch control and anti-misoperation is studied. The essential knowledge base of dispatch control and anti-misoperation is developed and the intelligent deduction technology based on rhombus-thinking model is proposed for the generation of operation orders. The publish/subscribe mechanism is adopted to completely share the models，graphics and data of dispatch control system and the intelligent topology analysis is applied to realize the multi-layer check service of misoperation prevention. An integrated dispatch control and anti-misoperation system is developed based on D5000 platform，which，with higher anti-misoperation efficiency，adapts to the line connection type change，power grid capacity expansion and operation mode change.

Key words：dispatch control integration；D5000 platform；extension theory；rhombus-thinking model；topological anti-misoperation

(上接第 167 页 continued from page 167)

Data authentication based on frequency watermarking for smart grid

CHEN Sheng[1]，HUANG Qian[2]，ZHANG Yu[3]

(1. Jiangsu Electric Power Company，Nanjing 211102，China；2. Jiangsu Taizhou Electric Power Company，Taizhou 225300，China；3. College of Electrical Engineering，Zhejiang University，Hangzhou 310027，China)

Abstract：According to the features of smart grid communication network，it is proposed to apply the grid frequency information in the authentication of real-time interactive data to enhance data security. The frequency watermarking of real-time grid frequency monitoring network is modeled and then embedded in the transmitting data by the fractional Fourier transform. The received data are authenticated according to the embedded frequency watermarking for secure data communication. Because the energy of embedded information is distributed in traditional time-frequency domain，the security is high. Simulations and experiments demonstrate that the watermarking embedding algorithm based on the fractional Fourier transform has higher security and resistibility to regular noise attack，low-pass filtering attack and down-sampling attack.

Key words：smart grid；frequency；watermarking；authentication；Fourier transforms；security of data