一种基于盲源分离的数据保密方法

焦卫东[1),2)] 杨世锡[1)] 吴昭同[1)]

[1)](浙江大学机械工程系,杭州 310027) [2)](浙江嘉兴学院机电与建筑工程学院机电系,嘉兴 314001)

摘 要 盲源分离是一种很有希望的信号处理技术,具有独特的盲信息处理和波形保持能力。为了获得可靠的数据保密效果,通过引入虚拟观测,将盲源分离在消噪方面的应用思想加以扩展,形成了一种新的基于完全覆盖策略的数据保密方法。该方法不仅可行,且具有相当高的可靠度。实验结果表明,此方法简单有效,有很多吸引人的特点,可用于多种类型数据(如文本、声音及图像等)的保密。因此,在信息安全领域有较大应用潜力。

关键词 独立分量分析 盲源分离 数据保密 噪声消除 完全覆盖

中图法分类号: TP309.7 **文献标识码**: A **文章编号**: 1006-8961(2005)06-0710-07

A Method for Data Secrecy Based on Blind Source Separation

JIAO Wei-dong[1),2)], YANG Shi-xi[1)], WU Zhao-tong[1)]

[1)] (*Mechanical Engineering Department, Zhejiang University, Hangzhou* 310027)

[2)] (*Mechanical & Electrical Department, Mechanical and Architecture Engineering School, Jiaxing University, Jiaxing* 314001)

Abstract Blind source separation is a promising technique for signal processing, which has such features as blind information processing and waveform restoral. In order to keep the data secret reliably, the applicable principle of BSS in noise removal was extended to form a kind of new method for data secrecy based on the strategy of complete covering, by the introduction of virtual observation. This new method is not only feasible, but of very high security. The results of experiments verified that this new method for data secrecy was simple and effective and had many charming features. For example, it was very simple to use, and has considerable flexibility to implement. Therefore, this method can be used for keeping secrecy of many kinds of different data such as text, speech and image. All of these implied its great potential in information security field.

Keywords independent component analysis, blind source separation, data secrecy, noise removal, complete covering

1 引 言

信息保密技术最初主要应用于军事、外交等领域。进入 20 世纪 90 年代,随着计算机和通信设备的广泛应用,已扩展至诸如工业、商业以及金融等部门。在这些部门中,有很多机密敏感数据需要存储和交换。为防止这些机密数据外泄,必须利用先进的保密技术加以保护[1]。目前,随着世界经济一体化进程加剧,对信息保密的需求和使用正在快速增长。

用密码技术对数据进行加密是迄今公认的比较有效的数据保密手段,例如密码技术正被用来满足电子资金汇兑和电子数据交换等领域的要求。密码曾一度被认为只具有军事和外交意义。现在,由于电信技术的飞速发展,密码对于计算机行业变得极端重要,密码保护已成为正规商业活动不可缺少的部分[2,3]。

2 基于密码保护的数据加密——对称与非对称加密算法

密码保护,即利用数据变换使数据仅对其指定用户才是可以理解的,在局外人看来则都是些完全

基金项目:国家自然科学基金(50205025);浙江省自然科学基金(5001004)

收稿日期:2003-05-29;**改回日期**:2004-11-01

第一作者简介:焦卫东(1970~),男,讲师。2003 年于浙江大学机能学院获博士学位,浙江大学博士后。主要研究方向为智能检测与信号处理、状态监测与故障诊断。E-mail:jiaowd1970@mail.zjxu.edu.cn

随机的字符。在暴露媒体上安全传送和存储数据的一个通用手段,就是使用某种形式的加密。加密算法通常需要一个用以加密的密钥,加密处理所得的结果称为密文。为了能在收端读出原始消息,就需要一个解密密钥把密文转换回明文。加密密钥和解密密钥通常均为二进制代码[2,3]。

典型的加密算法有两种,即对称加密算法和非对称加密算法。对称算法采用相同的加密密钥和解密密钥,而非对称算法则要求产生一个秘密密钥和一个公开密钥,公开密钥用来加密明文消息,它可以对任何希望向收方送消息的人公开。收方保密的秘密密钥则用来解密发送来的消息。对称加密算法意在保护两点之间敏感数据的传输。非对称算法则可用来验证消息,特别适于中心点同其他任意数量点之间敏感数据的传输。本文提出的保密算法中,加密密钥为解密密钥的一部分,但两者又不完全相同,可以视为是属于对称加密算法和非对称加密算法之间的一种特殊算法[1]。

3　基于盲源分离消噪的数据保密方法

对一个观测 $\boldsymbol{x}(n)$,其中,n 为离散数字序列的采样点数,设其中真正信号为 $\boldsymbol{s}(n)$,含有噪声 $\boldsymbol{u}(n)$,若 $\boldsymbol{x}(n)$可表示为

$$\boldsymbol{x}(n) = \boldsymbol{s}(n) + \boldsymbol{u}(n) \tag{1}$$

则称 $\boldsymbol{x}(n)$中含有加法性噪声。若 $\boldsymbol{x}(n) = \boldsymbol{s}(n)\boldsymbol{u}(n)$,则说 $\boldsymbol{x}(n)$中含有乘法性噪声。大部分情况下,噪声都是加法性的,而乘法性噪声处理起来较困难[4]。

众所周知,信号处理中噪声一般被认为是有害的,即它"污染"了信号,干扰了对观测中有用信息的获取[4]。然而,世界上任何事物都具有两面性,当从不同角度看待理解同一对象时,可能会得到截然相反的结论。通常信号处理中的有害噪声干扰,在数据保密应用领域中则变得很有价值。由前述,作为一种有效的信息安全防护手段,密码保护的核心思想在于采用合适的数据变换对数据进行有效的加密和解密。由式(1)可知,如果将信号 $\boldsymbol{s}(n)$视为待保护的数据(即原文),则外来干扰噪声 $\boldsymbol{u}(n)$可以看成是一种特殊的加密密钥。于是通过加性变换,上式(1)将信号 $\boldsymbol{s}(n)$(原文)转换(加密)为带噪观测 $\boldsymbol{x}(n)$(即密文)。这种带噪观测由指定的接收方接收后,经过特殊消噪算法(亦即解密密钥)处理即可获得所需的原文。从而,传统数据保密工作中的加密与解密过程,可由信号处理中的加噪与消噪过程来等效实现。

显而易见,这种新的数据保密方法的性能取决于如下因素:(1)外加噪声的多样性以及量值;(2)消噪算法的复杂性、稳定性、运行效率以及消噪精度等等。理论上,所加噪声干扰越复杂多样,噪声在观测中所占的比重越大,则消噪越困难。从数据保密角度意味着加密效果越好,别人越难以破解原文。但从数据解密角度,这通常也意味着需采用更复杂的解密密钥(消噪算法)来进行消噪(解密),且算法的稳定性、运行效率及去噪精度可能越难以控制。加噪(密)的种类与所加噪声量值通常可人为设定,关键在于采用合适的解噪(密)算法,它在以上性能影响因素中占据主导地位。因此,对先进可靠的信号消噪技术与方法的研究,是本方法研究中的重点。

传统的噪声去除方法有很多,比如著名的相干平均(或称时域平均)以及小波变换[4]等等。不过,这些方法往往有很多局限性[4,5],在实用中会遇到困难。例如,相干平均法假设真实信号 $\boldsymbol{s}(n)$为确定性信号,这与实际情况特别是数据加密应用背景严重不符。另外该法具体实施中不仅需大量观测样本,且每次观测相加时还须"对齐"。还有小波方法,通常需先定位真实信号的特征频段,以便在合适的频段进行信号提取。如果对信号的特征频段没有先验的了解,则难以进行满意的信噪分离。另外,它的去噪精度相对于数据加密应用要求来说也不够。所有这些,都极大限制了这些方法的实际应用。

近年来,信号处理领域出现了一种新颖有效的阵列信号处理方法——盲源分离(blind source separation, BSS),其理论基础为独立分量分析(independent component analysis, ICA)。BSS 通常假设观测信号由几个本底源经线性混叠而成[6],其处理的一般模型如下:

$$\boldsymbol{x} = \boldsymbol{A}\boldsymbol{S} + \boldsymbol{n} \tag{2}$$

其中,$\boldsymbol{x}$ 为 M 维观测向量,$\boldsymbol{s}$ 为 N 维源向量,$\boldsymbol{A}$ 为一个 $M \times N$ 的列满秩线性混合矩阵,$\boldsymbol{n}$ 为噪声向量。在源 $\boldsymbol{s}$ 各分量统计独立假设下,BSS 仅从已知观测 $\boldsymbol{x}$ 出发,即可获得对未知混合矩阵 $\boldsymbol{A}$ 辨识以及本底源信号 $\boldsymbol{s}$ 的估计。如此的盲信息处理优势,使得 BSS 迄今已广泛应用于诸如语音图像处理、地震监测以及生物医学等领域[7,8]中信号的消噪、解卷及特征提取等方面。BSS 算法有多种,其中以 JADE(jointly

approximate diagonalisation of Eigen-Matrices)算法[9]较具代表性。JADE 是一种数值稳定、鲁棒的代数方法,它首先白化观测信号,即

$$\begin{aligned} \boldsymbol{z}(t) &\overset{\text{def}}{=} \boldsymbol{W}\boldsymbol{x}(t) = \boldsymbol{W}[\boldsymbol{A}\boldsymbol{s}(t) + \boldsymbol{n}(t)] \\ &= \boldsymbol{U}\boldsymbol{s}(t) + \boldsymbol{W}\boldsymbol{n}(t) \end{aligned} \tag{3}$$

从而,一个 $M \times N$ 的矩阵 $\boldsymbol{A}$ 的确定问题,转化为一个 $N \times N$ 酉矩阵 $\boldsymbol{U}$ 的确定。式中,t 为连续时间,$\boldsymbol{W}$ 为白化矩阵。$\boldsymbol{U}$ 的估计有赖于高阶累积量(通常是 4 阶)。对任意 $N \times N$ 矩阵 $\boldsymbol{M}$,其 4 阶累积量矩阵定义为

$$\boldsymbol{N} = Q_z(\boldsymbol{M}) \overset{\text{def}}{\Leftrightarrow} n_{ij} = \sum_{k,l=1}^{n} Cum(z_i, z_j^*, z_k, z_l^*) m_{lk} \tag{4}$$

其中,$1 \leqslant i,j \leqslant n$,$Cum$ 为累积量计算函数。

通过以下参照函数的最大化,实现累积量矩阵集合 $\hat{\boldsymbol{N}}^e = \{\hat{\lambda}_r \hat{\boldsymbol{M}}_r \mid 1 \leqslant r \leqslant n\}$ 的联合近似对角化,从而求得酉阵 $\boldsymbol{U}$。

$$c(\boldsymbol{V}, \boldsymbol{N}) \overset{\text{def}}{=} \sum_{r=1}^{s} |\operatorname{diag}(\boldsymbol{V}^{\mathrm{H}} \boldsymbol{N}_r \boldsymbol{V})|^2 \tag{5}$$

其中,s 为累积量矩阵集合中矩阵的数目。

理论上,BSS 算法本身存在着估计波形幅值与相位的不确定性[10]。而数据保密则对解密的精度提出了十分严格的要求,即必须准确无误地解密原文。由后面可以看到,对 BSS 这种不确定性,利用 BSS 独具的波形保持特性[6],用数据某些先验知识作为解密密钥,基本可得到完全消除。

另外,BSS 通常只能处理多维观测,因此当对如式(1)的 1 维观测去噪时,需引入适当的虚拟观测,以将 1 维观测扩展为可以处理的多维观测。这里考虑观测外加 M 种噪声情形,此时式(1)的噪声部分变为 $\boldsymbol{u}(n) = \sum_{i=1}^{M} a_i \boldsymbol{u}_i(n)$,其中,$a_i$ 为第 i 种噪声 $\boldsymbol{u}_i(n)$ 的权重。若引入 $\boldsymbol{u}(n)$ 中的各分量作为虚拟观测 $\boldsymbol{x}_{\text{virtual}}$,则式(2)模型可改写为

$$\begin{aligned} \boldsymbol{x} = \boldsymbol{A}\boldsymbol{s} \Rightarrow \boldsymbol{x} &= \begin{bmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \\ \vdots \\ \boldsymbol{x}_{M+1} \end{bmatrix} = \begin{bmatrix} s + \sum_{i=1}^{M} a_i \boldsymbol{u}_i(n) \\ \boldsymbol{u}_1(n) \\ \vdots \\ \boldsymbol{u}_M(n) \end{bmatrix} \\ &= \begin{pmatrix} 1 & a_1 & \cdots & a_M \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \begin{bmatrix} s \\ \boldsymbol{u}_1(n) \\ \vdots \\ \boldsymbol{u}_M(n) \end{bmatrix} \end{aligned} \tag{6}$$

式(6)意味着待处理加噪观测 $\boldsymbol{x} = \boldsymbol{x}_1$ 中引入 M 个噪声分量后形成 $M+1$ 维新的观测向量,BSS 可通过对虚拟混合矩阵 $\boldsymbol{A}$(特别是其中各种噪声的权重 a_i)的辨识,恢复虚拟源 $s(n)$ 和 $\boldsymbol{u}(n)$,从而实现真实信号的噪声消除,从数据保密角度即意味密文的解密。当然 $\boldsymbol{x}_{\text{virtual}}$ 的实际选取,必须考虑加密过程中所施加的干扰噪声的种类与性质。基于 BSS 消噪的数据保密方法整体结构与实现流程如图 1 所示。

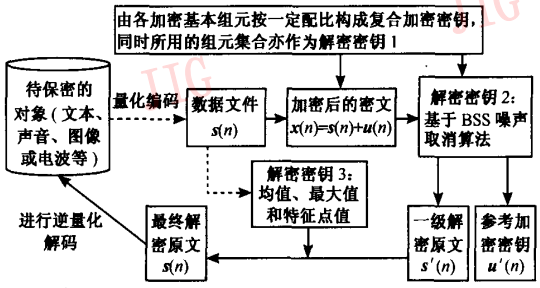


图 1 基于 BSS 消噪的数据保密方法的整体结构与实现流程

Fig. 1 Total implementation of the data secrecy based on BSS de-noising

理论上,加密密钥各组元可以是与待保密数字文件不同的任何数据序列,例如各种噪声序列(白噪声、脉冲噪声等)以及各种由自然文本、语音图像(如特定的人的声音、面孔或指纹等)或电波经过数字化形成的数字序列,只要满足长度与明文数据文件 $s(n)$ 相等这个条件即可。

实际的加密密钥是由 $\boldsymbol{u}_1(n), \cdots, \boldsymbol{u}_M(n)$ 按照一定的配比,由 $\boldsymbol{u}(n) = \sum_{i=1}^{M} a_i \boldsymbol{u}_i(n)$ 构成,其中 $\boldsymbol{u}_i(n)$ 为第 i 个加密密钥组元,a_i 为该组元在加密密钥中的权重。最简单的为 $\boldsymbol{u}(n) = a_1 \boldsymbol{u}_1(n)$ 单组元单配比形式。假设加密密钥由组元集合 $\boldsymbol{C} = [u_1, u_2, \cdots, u_M]$ 按照配比集合 $\boldsymbol{B} = [a_1, a_2, \cdots, a_M]$ 复合而成,那么加密密钥的一种编码方式可能为 $\boldsymbol{CB}$。多组元多配比加密策略的提出,主要目的是为了获得最佳的加密效果。实用中组元种类性质及配比大小的确定,应根据不同性质的加密对象由数据发送方确定。

由图 1 可以看到,加密密钥中的组元集合 $\boldsymbol{C}$ 也构成了解密密钥 1。因为,在实施 BSS 消噪前引入的虚拟观测就是组元集合 $\boldsymbol{C}$。对于解密,配比集合 $\boldsymbol{B} = [a_1, a_2, \cdots, a_M]$ 则不是必要的。当然,数据发送方和接收方亦可共同约定:在特定的时间只使用某一特定的、双方共知的组元集合。从而,可在解密密

钥中隐藏组元集合代号,进一步地提高数据传输的保密度。解密密钥 2,就是所用到的 BSS 消噪算法,比如 JADE 算法可以用 J 来表示。当然,解密密钥 2 亦可由双方预先约定隐藏。解密密钥 3 为加密前数据序列的均值、经过去均值处理后序列的最大值和一个非零特征点,以 M_e、M_a 和 X_m 来表示,其中 m 表示特征点位置。这 3 个量用来消除 BSS 算法幅值和相位的不确定性。从而,一个完整的解密密钥可归纳为(C) - (J) - M_e M_a X_m,其中带括号项为可隐藏项。当然,无论是加密还是解密密钥,其具体标识方式应由发送和接收方共同研究确定,而且,为了提高密钥本身的保密性,标识方式应定期更换。

本保密策略中,无论是对象数字化时所用的量化编码还是消噪后恢复明文所用的逆量化解码,均可利用一般的文件数字化通用技术。当然,为了提高保密度亦可自定编码。不过为使算法简单起见,不推荐采用特别复杂的自定编码方式。如想更可靠加密,可采用密钥分层策略,即在解密密钥前端设置文件读取权限密码作为表层密钥,而前面提到的解密密钥则作为最终恢复文件的深层密钥。

4　仿真实验

一般文本、声音、图像以及电波等文件,采用通用的量化编码技术均可方便地转化为数字序列。为简化实验,首先随机选取了一段纯英文文本如下:

> Machine sound always carries information about the working of the machine. But in many cases, the sound has a very low SNR. To obtain correct information, the background noise has to be removed or the sound must be purified. A de-noising method is given in this paper and is successfully used in feature sound extraction. We can easily diagnose a machine using the purified sound. This de-noising method is based on the wavelet technique and uses the Morlet wavelet as the mother wavelet, because its time-frequency resolution can be adjusted to adapt to the signal to be analyzed. The method is used for extracting the sound of some vehicle engines with different types of failure. The feature sound is extracted successfully.

该段文本连同标点符号、空格在内,共有 727 个字符。这里采用自定编码,不计字母的大小写以及空格(因为它们对理解原文并不会造成什么影响),规定:字母 a ~ z 对应数字 1 ~ 26,逗号、句号和减号对应数字 27 ~ 29。从而文本被转化为一个如图 2 的数字序列。原序列 $s(n)$ 均值12.082 4,将去均值后序列的第一点0.917 6取为特征点。

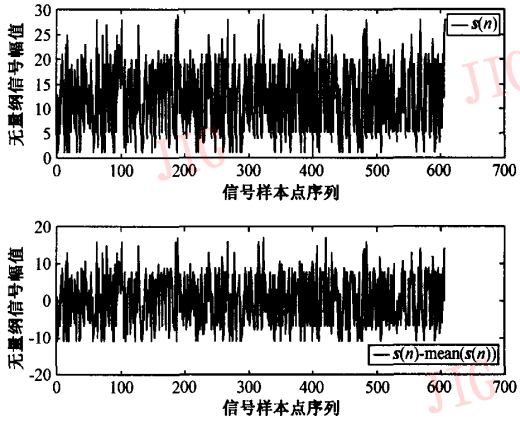


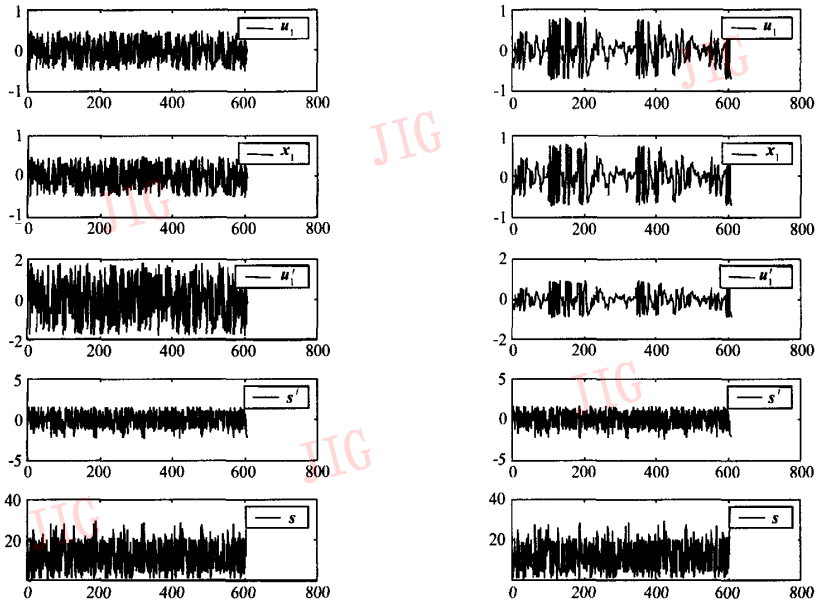
图 2　文本经过自定编码后形成的数字序列

Fig. 2　Numeric sequence formed by text with self-defined coding

首先考虑单组元单配比这种最简单的加密策略,亦即加密密钥构成为 $u(n) = a_1 u_1(n)$,其中密钥组元 $u_1(n)$ 依次选取为高斯白噪声和一段自然声音两种情况,配比 a_1 取 1 000 000,可完全覆盖待加密的数字序列。引入密钥组元 $u_1(n)$ 作为虚拟观测,应用本文提出的解密算法解密,结果如图 3 所示。算法总体解密性能采用以下二次残差(*VQM*)指标定量测度[11]:

$$VQM = 10\log_{10}\left(\frac{E(y_i - s_i)^2}{E[s_i^2]}\right)(\mathrm{dB}) \qquad (7)$$

由图 3 可以看到,经过加密密钥——1 000 000 倍噪声 u_1 的超强覆盖,原文 $s(n)$ 已完全隐藏于干扰噪声中而形成密文 x_1。将此加密密钥组元作为虚拟观测——解密密钥 1 引入,利用解密密钥 2——BSS 算法 JADE,可获得一级解密原文 s' 和参考加密密钥 u_1'。由于 BSS 自身的幅值与相位的不确定性,一级解密文 s' 相对于真实原文 s(图 2)出现了幅值(减小)与相位(180 度倒相)偏差。而借助解密密钥 3——真实数字序列的均值、去均值后序列的最大值和特征点,可基本完全消除这种不确定性,获得解密数字序列 s。应用式(7)的计算结果显示:两种加密情况信噪比由加密后的212.482 2

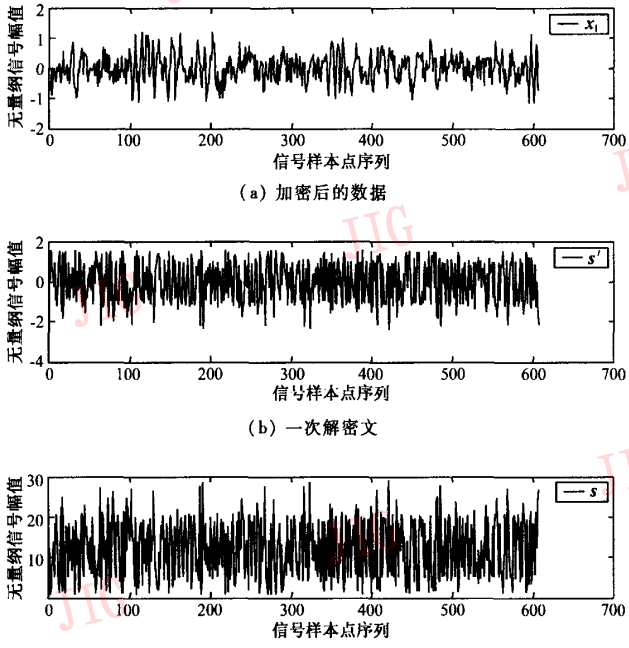


(a) 密钥组元为高斯白噪声　　(b) 密钥组元为自然声音

图 3　基于 BSS 消噪加密算法的文本加密与解密结果

(单组元单配比,横坐标为信号样本点序列,纵坐标为无量纲信号幅值)

Fig. 3　Covering and de-covering results of text based on the algorithm with BSS de-nosing(only one component)



(a) 加密后的数据

(b) 一次解密文

(c) 最终解密原文

图 4　基于 BSS 消噪加密算法的文本加密与解密结果(多组元多配比)

Fig. 4　Covering and de-covering results of text based on the algorithm with BSS de-nosing(more components than one)

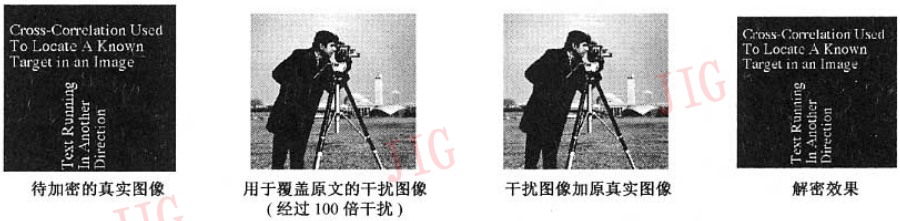
和201.372 2剧降为 -120.740 3和 -67.582 5。

另外,选取以上两种加密组元(高斯白噪声和自然声音),配比仍取为1 000 000,按照 $\boldsymbol{u}(n) = a_1\boldsymbol{u}_1(n) + a_2\boldsymbol{u}_2(n)$ 构成复合加密密钥。应用本加

密算法得图 4 所示的结果。图 4 中上、中和下子图依次为加密后的数据、一次解密文和最终解密原文。应用式(7)计算,信噪比由加密覆盖后的215.261 3降为 -66.950 5,获得完全解密、准确无误的原文。

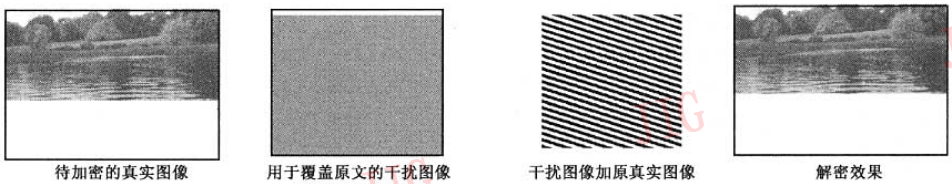
为进一步验证本方法对其他类型文件的保密与解密的有效性,从 Matlab5.3 的图像处理工具箱中任意选取了几个黑白与彩色图像进行分析。所采取的图像量化编码格式为 RGB 格式,即分别取出图像的红、绿和蓝色 3 种基元数据。

图 5(a)为黑白图像应用本方法所得的结果。可以看到,经过 100 倍干扰,原图像已被完全覆盖。利用本解密方法,只从干扰图像和覆盖后的图像,即轻松准确地获得了原来图像中的信息,图像中的文本内容丝毫没有丢失。



待加密的真实图像　用于覆盖原文的干扰图像(经过 100 倍干扰)　干扰图像加原真实图像　解密效果

(a) 黑白图像应用本方法的加密解密效果



待加密的真实图像　用于覆盖原文的干扰图像(经过 100 倍干扰)　干扰图像加原真实图像　解密效果

(b) 彩色图像应用本方法的加密解密效果

图 5　基于 BSS 消噪加密算法的图像加密与解密结果(多组元多配比)

Fig. 5　Covering and de-covering results of image based on the algorithm with BSS de-nosing(more components than one)

随后,又利用 10 000 倍的高斯白噪声和正弦信号分别对彩色图像(如图 5(b)中的第 1 幅图像)进行了超强覆盖,得到覆盖后的图像(第 2 和第 3 幅图像)。由此出发,引入所加的干扰噪声信号作为虚拟观测,利用本解密算法进行覆盖消除。结果表明:对外加高斯白噪声覆盖算法失效,所得结果相对于带噪图像几乎没有任何改进。而对于正弦干扰,算法则给出了极佳的解密结果(如第 4 幅图像),几乎完全保留了原图的信息。

理论上,ICA 只能解决非高斯源向量(其中至多只有一个高斯源分量)的盲分离问题。本算法之所以对图像加密中的高斯覆盖失效,主要是因为实验图像的基元数据本身便呈现出较强烈的高斯分布,与覆盖的高斯白噪声干扰发生强相关。其结果是:BSS 模型中独立源假设不再成立,良好的图像解密效果难以获得。因此,在文件加密过程中,应避免选择与待加密对象量化参数相关的覆盖,这可以作为选择加密覆盖信号的一个基本原则。

5　结　论

事实上,在文件加密过程中,所选择的覆盖配比 $a_i, i=1,2,\cdots,M$ 并不是恒定值。在应用本算法解密时,只要引入各覆盖组元 $\boldsymbol{u}_i, i=1,2,\cdots,M$ 作为虚拟观测即可,配比的大小不需要知道也不影响本算法的解密精度。由式(6)可清楚看出:在虚拟混合矩阵 $\boldsymbol{A}$ 和虚拟源向量之间交换一比例因子,对 BSS 算法的估计结果并无本质影响。由此带来的幅值与相位不确定性,通过解密密钥 3(均值、最大值以及特征点值)即可完全得到消除。当然,如所用解密算法不合适,即便知道覆盖组元,亦无法实现文件解密。从而,文件加密过程中多组元多配比策略的采用,以及解密过程中解密密钥 1、2 和 3 之间相互制约、相互影响,共同形成了本保密算法。对文本和图像的实验结果,清楚地表明了本方法的有效性和潜在的应用价值。本文提出的基于 BSS 消噪的数据

保密方法,归纳起来具有如下几个特点:

(1)传统的加密方法偏重于对文件的复杂编码,这同时也导致解密的复杂与困难。例如,战争中对接收的无线电波的解码,往往需要复杂的解密码本,不仅保存不便,且一旦丢失极易导致灾难性后果。本文的方法则对编码的复杂度要求不高,采用通常的量化编码技术即可。通过完全覆盖策略和特殊的信号处理技术,可轻松地实现数据保密。

(2)采用多组元多配比加密策略,可通过组元种类、性质和权重大小灵活控制文件加密级别。例如,对普通、机密和绝密文件可采用复杂度依次递增的加密策略,甚至可引入具有唯一性的指纹等作为加密密钥组元,增加保密度。另外,还可以采用密钥分层策略,与传统的密码加密技术结合进一步提升保密能力。

(3)加密密钥中基本组元的类型和配比大小,对本算法的解密精度无任何影响。这意味着实际应用中可采用足够大的配比,将原数据文件完全覆盖以获得超强加密效果。而且可以有意识地选择某些特殊的加密组元,以实现特定的目的。如在军事斗争或商业对抗中,可采用与原文相反或具有误导性的信号完全覆盖真实信息。这样,在传输过程中即便被对手截获,不仅无泄密之忧,而且还可以籍此误导对手以达到己方的特定目的。

事实上,前述的加密覆盖组元不相关原则,反过来也意味着:可以选用同种组元(如用文本、声音和图像)覆盖待加密的文件对象(其他的文本、声音和图像),亦可选用不同种类的覆盖组元(如用声音覆盖文本、图像或反之),只要覆盖组元数据与待加密文件数据满足不相关条件即可,这赋予了本方法相当的灵活性。目前,ICA 理论研究不断扩展深化,已出现多种新的算法[12],可有效分析处理非稳态、非线性数据,这些都必将进一步拓展 ICA 的实际应用领域。从而,也将进一步促进这种 BSS 基数据保密技术的完善与发展。

参考文献(References)

1 Yu Z G. Information secrecy and selection for secrecy technology[J]. Sichuan Communication Technology, 1998,**16**(3): 15 ~ 19. [于增贵. 信息保密和保密技术选择[J]. 四川通信技术, 1998, **16**(3):15 ~ 19.]

2 Zhang H G, Tan Z P. Development of secrecy technology for computer security[J]. Traffic and Computer, 1996,**14**(1): 2 ~ 6. [张焕国, 覃中平. 计算机安全保密技术的发展[J]. 交通与计算机, 1996,**14**(1): 2 ~ 6.]

3 Zhang W Z, Meng Q Z. Unit three: Secrecy technology in communication[J]. Computer Application, 1998, **18**(6): 35 ~ 38. [张文政, 孟庆志. 第三讲:通信保密技术[J]. 计算机应用, 1998,**18**(6): 35 ~ 38.]

4 Hu G S. Digital signal processing——Theory, algorithm and implementation[M]. Beijing: Tingshua University Press, 1997:11 ~ 12. [胡广书. 数字信号处理——理论算法与实现[M]. 北京: 清华大学出版社, 1997:11 ~ 12.]

5 Lyon R H. Machinery noise and diagnostics [M]. Boston: Butterworths, 1987:236 ~ 243.

6 Pierre Comon. Independent component analysis, a new concept? [J]. Signal Processing, 1994, **36**(10): 287 ~ 314.

7 Porrill J, Stone J V, Berwick J, *et al*. Analysis of optical imaging data using weak models and ICA[A]. In: Based on a workshop held after the 1999 International Conference on Artificial Neural Networks [C], Helsinki: Helsinki University of Technology, 2000: 598 ~ 606.

8 Vigario R, Sarela J, Oja E. Searching for independence in electromagnetic brain waves[A]. In: Based on a workshop held after the 1999 International Conference on Artificial Neural Networks[C], Helsinki: Helsinki University of Technology, 2000:678 ~ 683.

9 Cardoso J F, Souloumiac A. Blind beamforming for non-Gaussian signals[J]. IEEE Proceedings-F, 1993,**140**(6): 1 ~ 3.

10 Tong L, Liu R, Soon V, *et al*. Indeterminacy and identifiability of blind identification[J]. IEEE Transactions on Computer Science, 1991, **38**(3): 499 ~ 509.

11 Hoang-Lan Nguyen Thi, Christian Jutten. Blind source separation for convolutive mixtures[J]. Signal Processing, 1995, **45**(6): 209 ~ 229.

12 Te-Won Lee. Nonlinear approaches to independent component analysis[DB]. http://www.cnl.salk.edu/~tewon/ica_cnl.html, 2000-11-12.