第44卷　第4期　　《新疆师范大学学报》(自然科学版)　　Vol.44,No.4
2025年12月　　Journal of Xinjiang Normal University　　Dec. 2025
(Natural Sciences Edition)

基于提升小波随机数的一种文本加密方法

曹航宾,王　刚*
(新疆师范大学 数学科学学院,新疆 乌鲁木齐 830017)

摘　要:文章利用小波随机数算法与卷积公式,研究了一种新的文本信息加密方法。首先,提出一种简单、快速加密文本信息的算法,是一种基于小波随机数的文本加密算法(TCAWRN)。其次,引入基于小波随机数的文本破译算法(TDAWRN),利用接收数据和私钥对原始文本进行恢复,该私钥包括初始随机值和小波基。第三,通过实例说明这种针对文本信息的加密传输方法。最后,讨论算法的安全性,包括小波随机数、小波基函数和运行时间。

关键词:小波随机数;小波重构公式;卷积
中图分类号:TP309.7　　**文献标识码:**A　　**文章编号:**1008-9659(2025)04-0010-10

在数字化通信时代,敏感数据的安全传输已成为一项至关重要的议题。文本信息作为关键数据传输的主要形式,对稳健加密技术的需求日益凸显。尽管传统加密手段在一定程度上保证了信息安全,但其依赖于复杂的数学理论,计算成本高昂,且有潜在的安全隐患。学术界在小波域信息隐藏与小波域信息加密领域进行了广泛而深入的研究。文献[1]~[5]给出了文本加密方法的相关结论。部分研究成果表明,通过小波变换技术,可以有效实现文本信息在多种载体介质中的隐蔽传输。例如,Yang等人提出了一种在载波图像的DWT域中通过混沌映射和BCH码隐藏文本信息的方法[6]。Sakkara等人提出了一种新的文本和图像隐写集成方法[7],利用小波技术提高安全性和数据保护力度。然而,Olga等人基于小波的隐写方法,将文本隐藏于音频信号中,旨在提高系统对未经授权操作的鲁棒性[8-9]。另一方面,Fei等人还讨论了二维工程图形的分析方法,并基于属性特征和几何特征对现有的信息隐藏算法进行了分类[10]。Beram提出一种基于浮点小波变换和最优系数调整的隐写方法,通过可变比特长度嵌入与随机密钥优化数据隐藏[11]。Sabir提出了一种在声波文件中隐藏加密数据的方法,利用DES加密并在时频域嵌入密码文本[12]。此外,Gupta等人[13]描述了一种新的文本隐写方法,利用DWT处理输入图像,将其划分为子带,重点是抗噪声和安全攻击。为确保文本的安全传递,Zhou利用小波数字水印方法讨论了文本信息的隐藏和恢复问题,将秘密信息嵌入噪声信号中,并通过公钥机制传输密码文本[14]。随着深度学习的算法研究,相关技术也被应用于信息隐藏与信息安全方面。Rehman设计了基于GAN的动漫隐写方案,以高隐蔽性和大容量实现安全信息隐匿传输[15]。Kang提出了一种基于深度学习理论的计算机化信息安全通信方法[16]。这些研究展示了小波变换隐藏文本信息在不同载波介质中的各种应用和技术。

本研究提出了一种基于小波提升变换随机数生成的文本信息加密传输方案。该方案旨在为文本数据的加密与传输提供一个安全性高且效率优化的解决策略。该算法的创新之处在于其采用了新颖的随机数生成机制,实现了快速计算,从而显著提升了加密操作的效率和安全性。

[收稿日期]2024-12-19　　[修回日期]2025-02-18
[作者简介]曹航宾(1999-),男,硕士研究生,主要从事小波分析及其应用方面研究,E-mail:48310585@qq.com.
*[通讯作者]王　刚(1971-),男,教授,主要从事小波分析及其应用方面研究,E-mail:angelayy@sina.com.

1 方法与技术

文章引入小波随机数与卷积运算来讨论文本信息加密传输的方法与技术,包括一种生成提升小波随机数、卷积和反卷积的公式。

1.1 一种生成提升小波随机数的方法

可以通过白噪声去噪方法生成标准正态随机数。为了简单,先回顾提升方法构造小波。

假设$\phi(x), x \in R$是一个尺度函数,$\psi(x)$是其对应的多小波,满足两尺度方程

$$\begin{aligned}\phi(x) &= \sqrt{2}\sum_{k\in Z} h_k \phi(2x-k)\\ \psi(x) &= \sqrt{2}\sum_{k\in Z} g_k \phi(2x-k)\end{aligned} \tag{1}$$

其中,h_k和g_k分别是低通滤波器与高通滤波器,假设它们是有限个非零的,同时有对偶尺度函数$\tilde{\phi}(x)$与对偶小波函数$\tilde{\psi}(x)$,它们分别满足两尺度方程

$$\begin{aligned}\tilde{\phi}(x) &= \sqrt{2}\sum_{k\in Z} \tilde{h}_k \tilde{\phi}(2x-k)\\ \tilde{\psi}(x) &= \sqrt{2}\sum_{k\in Z} \tilde{g}_k \phi(2x-k)\end{aligned} \tag{2}$$

其中,$\tilde{h}_k$和$\tilde{g}_k$分别是低通滤波器与高通滤波器。定义两尺度符号$h(t), g(t)$和$\tilde{P}(\omega), \tilde{Q}(\omega)\tilde{h}(t), \tilde{g}(t)$如下

$$h(t)=\sum_{k\in Z} h_k e^{-ikt}, g(\omega)=\sum_k g_k e^{-ikt}, \tilde{h}(t)=\sum_{k\in Z}\tilde{h}_k e^{-ikt}, \tilde{g}(t)=\sum_k \tilde{g}_k e^{-ikt}$$

双正交条件定义为

$$\left\langle \phi(x-k), \tilde{\phi}(x-l)\right\rangle = \delta_{k,l}, \quad \left\langle \psi(x-k), \tilde{\phi}(x-l)\right\rangle = 0$$

$$\left\langle \psi(x-k), \tilde{\psi}(x-l)\right\rangle = \delta_{k,l}, \quad \left\langle \phi(x-k), \tilde{\psi}(x-l)\right\rangle = 0$$

其中,$\langle\cdot,\cdot\rangle$是空间$L^2(R)$内积。进一步地,双正交条件等价于两尺度符号满足

$$h(t)\tilde{h}(t)+h(t+\pi)\tilde{h}(t+\pi)=2$$

$$h(t)\tilde{g}(t)+h(t+\pi)\tilde{g}(t+\pi)=0$$

$$\tilde{h}(t)g(t)+\tilde{h}(t+\pi)g(t+\pi)=0$$

$$\tilde{g}(t)g(t)+\tilde{g}(t+\pi)g(t+\pi)=2$$

该方程组也表示完全重构条件。若定义矩阵$M(t)$

$$M(t)=\begin{pmatrix} h(t) & h(t+\pi)\\ g(t) & g(t+\pi)\end{pmatrix} \tag{3}$$

类似定义对偶矩阵$\tilde{M}(t)$,完全重构条件可以表示为

$$M(\omega)\tilde{M}(\omega)^{*}=2I_2 \tag{4}$$

在相位多项式中,双正交性的条件用一个简单的乘积表示。符号$h(t)$的相位多项式可以表示为

$$h(t)=\frac{1}{2}\left(h_e(2t)+h_o(2t)e^{-it}\right)$$

其中,奇数相位多项式$h_e(t)$和偶数相位多项式$h_o(t)$表示为

$$h_e(t)=\sum_{k\in Z} h_{2k} e^{-ikt}$$

$$h_o(t)=\sum_{k\in Z} h_{2k+1} e^{-ikt}$$

奇数相位与偶数相位$\tilde{h}_e(t), \tilde{h}_o(\omega), g_e(t), g_o(t)$和$\tilde{g}_e(t), \tilde{g}_o(\omega)$分别类似于$h_e(t)$和$h_o(t)$,多相位矩阵$H(t)$表示为

$$H(t)=\begin{pmatrix}h_e(t) & h_o(t)\\ g_e(t) & g_o(t)\end{pmatrix}=\sum_{k\in Z}\begin{pmatrix}h_{2k} & h_{2k+1}\\ g_{2k} & g_{2k+1}\end{pmatrix}e^{-ikt} \tag{5}$$

可直接证明双正交条件等价于满足完全重构条件

$$H(t)\tilde{H}(t)^{*}=I_2$$

引理1 假设有两个紧支撑的小波函数族,它们满足双正交的条件,并且共享一个尺度函数$\phi(x)$. 定义函数族$\{\phi,\psi_A,\tilde{\phi}_A,\tilde{\psi}_A\}$和$\{\phi,\psi_B,\tilde{\phi}_B,\tilde{\psi}_B\}$. 假设这些函数符号为$\{h(t),g_A(t),\tilde{h}_A(t),\tilde{g}_A(t)\}$和$\{h(t),g_B(t),\tilde{h}_B(t),\tilde{g}_B(t)\}$,那么

$$\begin{aligned}g_B(t)&=T(2t)(g_A(t)+S(2t)h_A(t))\\ \tilde{h}_B(t)&=\tilde{h}_A(t)-\left(S(2t)\right)^{*}\tilde{g}_A(t)\\ \tilde{g}_B(t)&=\left(T(2t)\right)^{-1}\tilde{g}_A(t)\end{aligned} \tag{6}$$

其中,$S(t)$和$T(t)$是有限多项式。

证明详见文献[17-18].

根据引理1的结论,提升步骤可以阐述如下:

(1)初始小波:选择一个初始小波函数$h_0(t)$和$g_0(t)$.

(2)提升:对于$n=0,1,2,\cdots$,进行以下步骤:

①分裂:将$h_n(t)$和$g_n(t)$分别分裂为两个相同长度的小波$h_{n+1}(t)$和$g_{n+1}(t)$;

②预测:根据$h_{n+1}(t)$和$g_{n+1}(t)$预测出$h_{n+1}(t)$;

③更新:根据预测结果和原始的$h_n(t)$更新出$h_{n+1}(t)$.

(3)生成的小波:经过多次提升后,得到的小波函数$h_N(t)$和$g_N(t)$,即最终的小波。其中,N是提升的次数,$h_n(t)$和$g_n(t)$是第n次提升后的小波函数。

引理2[19] 假设分形整合过程$I(d),|d|<\frac{1}{2}$的随机数序列X_t均值为0,且$d_{j,k}$为X_t在尺度参数j和平移参数k下的小波系数,那么$d_{j,k}\sim N(0,\sigma^2 2^{-2jd}),j\to 0$,其中$\sigma^2$为有限常数。

引理2的证明详见文献[19].

引理3[19] 假设分形整合过程$I(d),|d|<\frac{1}{2}$的随机数序列X_t均值为0,且$d_{j,k}$为X_t在尺度参数j和平移参数k下的小波系数,那么关于尺度参数j和平移参数k的小波系数$d_{j,k}$是渐近独立的。

引理3的证明详见文献[19].

在文献[19]中,给出了小波系数的衰减性,在时间空间中以$O(\left|k_1-k_2\right|^{2(d-m)-1})$衰减,在尺度空间中以$O(2^{2j(d-m)-1})$衰减,$m$表示小波的消失矩。因此,小波的消失矩越高,小波系数衰减越快。合适的提升格式有助于不断提升小波函数的消失矩,使其具备更好的衰减性。

提升方法常常用来构造双正交小波,如双正交小波Bio9/7,双正交小波Bio5/3等。生成提升小波随机数的算法如下:

算法1

(1)选取初始随机数x_0. 利用取整函数分别计算x_0的整数部分$a_{11}=[x_0]$和小数部分$d_{11}=x_0-[x_0]$,其中,$[x_0]$表示不超过实数x_0的最大整数;

(2)将a_{11}和d_{11}分别看作是近似系数$c_{j,k}$和细节系数$d_{j,k}$. 利用小波重构算法

$$c_{j+1,n}=\sum_{k\in Z}h_{n-2k}c_{j,k}+g_{n-2k}d_{j,k} \tag{7}$$

其中,$\{h_k\}$和$\{g_k\}$分别是低通滤波器与高通滤波器,计算得到随机数x_{11},x_{12}. 进一步地,利用取整函数分别

计算x_{11},x_{12}的整数部分$a_{21}=[x_{11}],a_{22}=[x_{12}]$和小数部分$d_{21}=x_{11}-[x_{11}],d_{22}=x_{12}-[x_{12}]$;

(3)将a_{21},a_{22}和d_{21},d_{22}分别看作是近似系数$c_{j,k}$和细节系数$d_{j,k}$.利用小波重构算法(式(7)),计算得到随机数$x_{21},x_{22},x_{23},x_{24}$.进一步地,利用取整函数计算其整数部分$a_{31}=[x_{21}],a_{32}=[x_{22}],a_{33}=[x_{23}],a_{34}=[x_{24}]$和小数部分$d_{31}=x_{21}-[x_{21}],d_{32}=x_{22}-[x_{22}],d_{33}=x_{23}-[x_{23}],d_{34}=x_{24}-[x_{24}]$.

将上述过程迭代N次,通过小波重构公式(式(7))得到2^N个随机数$x_{N1},x_{N2},\cdots,x_{N2^N}$.

上述三步便是小波随机数生成算法,由此所得的随机数序列$x_{N1},x_{N2},\cdots,x_{N2^N}$可称为小波随机数。

该随机数序列未经过处理,所以其分布是未知的。如文献[4]所述,用小波去噪方法处理后可以标准正态化,即可以转化为标准正态随机数序列。考虑到对文本信息的保护,不知道随机数的分布可能比知道随机数更安全。这种算法简化了过程,提高了计算速度。

1.2 卷积公式与去卷积

卷积和去卷积应用于各种领域的数学算子,包括图像处理和深度学习等。 在数据分析和信号处理中,卷积是一种数学运算,描述了两个函数结合形成第三个函数的方式。它通常用于建模系统的输出,是输入信号和系统响应特性的组合。两个函数$f(t)$和$g(t)$的卷积是由这两个函数的内积定义的,记为$f*g(t)$,公式如下

$$(f*g)(t)=\int_{-\infty}^{+\infty}f(x)\,g(t-x)dx \tag{8}$$

这个算子在图像处理中十分重要,表示通过具有特定响应函数(内核)的系统来模糊图像的过程。假设有一个输入信号$f[n]$和一个卷积核(或滤波器)$g[n]$,则离散卷积F可以表示为

$$F[n]=\sum_{-\infty}^{+\infty}f[k]\cdot g[n-k] \tag{9}$$

其中,$F[n]$是卷积信号的结果;$f[n]$是来自输入信号的一个采样,$g[n-k]$是卷积核在$n-k$时刻的值。从负无穷到正无穷,对所有可能的k值进行求和。在实际应用中,由于信号和核是离散的,求和通常只考虑有限数量的样本点,受输入信号和核长度的限制。

此外,离散卷积用矩阵乘法来表示更加直观和有效,特别是在处理图像等二维信号时。它等价于托普利茨矩阵与输入信号列向量之间的矩阵向量乘法。

根据卷积信号$F[n]$,通过反卷积可以恢复原始的输入信号$f[n]$.在实际应用中,经常考虑盲去卷积,它包括使用迭代算法,如最大似然估计(MLE)或非局部均值算法来逐步估计未知信号和脉冲响应。这些算法利用数据点与先验知识之间的相关性来减少搜索空间,找到一个可行的解决方案。

2 文本加密方法

文章提出了一种简单、快速加密文本信息的算法,即基于小波随机数的文本加密算法(TCAWRN),具体步骤如下:

步骤1 编码原始文本。所有的文本字符,包括常见的中文字符、数字、小写英文、标点符号、大写字母字符等,都列在一个数据集中。这些可以编码为

$$T=\{t_1,t_2,\cdots t_n\mid n\in Z^+\}$$

其中,n为所有所选字符的个数。原始文本可以编码为一维信号(数据)f.

$$f=[m_1,m_2,\cdots m_l]$$

其中,$m_i\in Z^+,t_{m_i}\in T,i=1,2,\cdots,l$,$l$是文本的长度。

步骤2 生成小波随机数序列。选取一个初始随机数x_0,根据文本的长度l,计算出满足不等式$2^{m-1}<l\leqslant 2^m$的正整数m.通过生成小波随机数的算法1,得到一个长度为l的小波随机数序列$g[n]$.

步骤3 计算卷积。通过对文本信号$f[n]$和小波随机数序列$g[n]$进行卷积计算,得到离散卷积数据$F[n]$.

上述步骤被称为基于小波随机数的文本加密算法(TCAWRN)。该算法是基于小波随机数和卷积公式提出的,利用离散小波重构公式生成小波随机数,这是一个多项式算法。步骤3中的卷积是一种具有多项式时间复杂度的算法。具体来说,两个向量卷积的计算复杂度是线性的,即$O(l)$,其中l是文本的长度。在加密过程中,使用小波随机数对文本信息的数码进行加密。文本的原始代码是一个整数值向量,文本的加密代码是一个双精度数值向量。这种加密能够确保文本的原始数码被破坏,使其在没有相应解密密钥的情况下不可读。最后,加密后的文本通过一个安全通道被传输至接收方。

3 文本解密过程

在接收端,加密后的文本可以通过接收到的数据$F[n]$和初始随机值x_0进行解密。基本思想是接收端利用初始随机值x_0生成加密过程中相同的小波随机数序列,并应用于去卷积过程来恢复文本数值的原始数据。然后将这些数据转换回文本表示,显示原始文本信息。基于小波随机数的文本解密算法(TDAWRN)破译步骤如下:

步骤1 生成小波随机数序列。根据接收到的信号数据$F[n]$,计算出文本的长度l. 算法1可以计算出小波重构公式的迭代次数m,满足$2^{m-1}<l\leqslant 2^m$. 可以由私下保存的初始值x_0和小波函数生成长度为l的小波随机数序列$g[n]$.

步骤2 通过去卷积来获取文本数码。根据接收到的信号数据$F[n]$和小波随机数序列$g[n]$,可通过去卷积公式对文本的数码$f[n]$进行恢复。

步骤3 恢复原始文本。根据私存的文本数据集T,可以从一维数据$f[n]$中恢复原始文本。

上述步骤被称为小波随机数的文本破译算法(TDAWRN)。这是一种多项式算法,类似于通过小波随机数进行的文本加密算法(TCAWRN)。文本解密过程是一种具有多项式时间复杂度的算法。

4 数值算例

举例讨论小波随机数对文本信息的密码传输方法。

步骤1 考虑一个文本字符数据集T作为一个简单的例子,如

T={abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ.,?/\@123456789}

事实上,这个集合可能更复杂,比如带有重复字符和打乱顺序的文本集、短篇故事文本等。

给出一个测试的文本

“In this paper, a ciphered transmission approach for text information is presented by wavelet random number.”

通过计算,这个文本的编码构成了一个数组f,如下所示

f=[35,14,68,20,8,9,19,68,16,1,16,5,18,54,68,1,68,3,9,16,8,5,18,5,4,68,20,18,1,14,19,13,9,19,19,9,15,14,68,1,16,16,18,15,1,3,8,68,6,15,18,68,20,5,24,20,68,9,14,6,15,18,13,1,20,9,15,14,68,9,19,68,16,18,5,19,5,14,20,5,4,68,68,2,25,68,23,1,22,5,12,5,20,68,18,1,14,4,15,13,68,14,21,13,2,5,18,53]

步骤2 选取初始随机数x_0 = 20.240524. 根据文本的字符长度l = 108,得到一个整数7满足$2^6<108\leqslant 2^7$. 将算法1中的小波重构公式迭代7次,可得到长度为108的小波随机数序列$g[n]$,其中小波函数为Db3. 小波随机数序列$g[n]$如图1所示。x轴表示随机序列的序数$g[n]$,y轴表示随机序列$g[n]$的值。从图1可以看出,小波随机数的分布并不容易。该随机数据通过复合正态性的雅克-贝拉假设检验,服从正态分布。

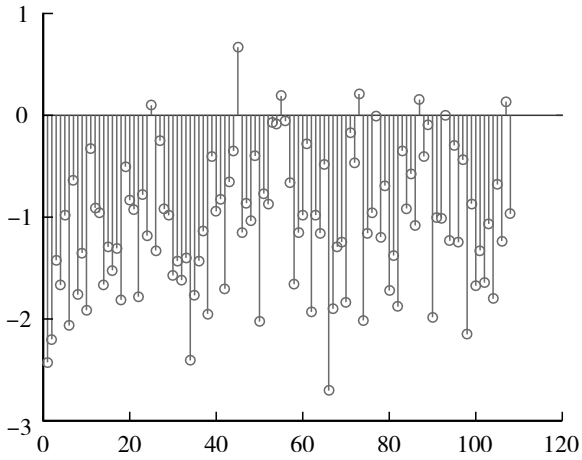

图1 小波随机数的杆型图

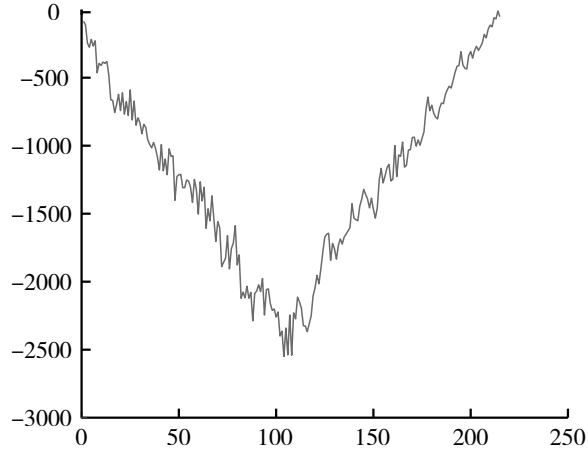

图2 卷积数据$F[n]$的图

步骤3 离散卷积数据$F[n]$可以通过对文本信号$f[n]$和小波随机数$g[n]$进行卷积来计算。由于$f[n]$和$g[n]$的长度都为108,所以卷积数据$f[n]$的长度为215(图2). x轴表示卷积数据$F[n]$的序号,y轴表示卷积数据$F[n]$的值。

由此,文本信息被隐藏在数据$F[n]$中。一般来说,$f[n]$和$g[n]$的长度都是L,那么卷积数据$F[n]$的长度是$2*L-1$.

因此,数据$F[n]$的长度是潜在的解密信息。如果接收方知道初始值x_0的同时也知道小波基,接收数据$F[n]$后,可以通过以下3个步骤进行解密。

步骤1* 根据接收到的信号数据$F[n]$,得到$F[n]$的长度l:215,然后用公式

$$l=\frac{length(F[n])+1}{2} \tag{10}$$

计算文本的长度l:108. 由此计算出算法1中小波重构公式的迭代数$m=7$,并满足

$$2^{m-1}<l\leqslant 2^m$$

长度为l:108的小波随机数序列可以由私存的初始值$x_0=20.240524$和小波函数生成。由于初始值x_0不变且小波基相同,因此小波随机数序列$g^*[n]$与第2节中步骤2的结果相同。

步骤2* 根据接收到的信号数据$F[n]$和小波随机数序列$g[n]$,可以通过反卷积公式进行文本数码$f^*[n]$的恢复。恢复后的代码如下

f^*=[35,14,68,20,8,9,19,68,16,1,16,5,18,54,68,1,68,3,9,16,8,5,18,5,4,68,20,18,1,14,19,13,9,19,19,9,15,14,68,1,16,16,18,15,1,3,8,68,6,15,18,68,20,5,24,20,68,9,14,6,15,18,13,1,20,9,15,14,68,9,19,68,16,18,5,19,5,14,20,5,4,68,68,2,25,68,23,1,22,5,12,5,20,68,18,1,14,4,15,13,68,14,21,13,2,5,18,53]

步骤3* 根据专用文本数据集T和恢复的文本数码$f^*[n]$,原文可恢复如下

"In this paper, a ciphered transmission approach for text information is presented by wavelet random number."

以上实例介绍了通过小波随机数和卷积方法进行文本信息加密的方法。因为这种方法的复杂性是多项式的,因此简单快捷。值得注意的是,卷积数据$F[n]$在整个过程中都是唯一公开传输的。初始值和小波基构成了一个用于解密的私钥,可以总结如下:

公钥:卷积数据$F[n]$.

私钥:初始随机数和小波基。

明文:“In this paper, a ciphered transmission approach for text information is presented by wavelet random number.”

5 分析和结论

文章提出了一种基于小波随机数和卷积的文本信息新型加密传输方法。先讨论其安全性。尽管这是一种简单快速的方法,但在文本解密过程中,如果没有初始值x_0,对于攻击者来说,其仅仅为盲去卷积。为了方便讨论文本代码初始值x_0的安全性,选择一个实数作为初始值x_0 = 20.240524. 如果其他条件保持不变,考虑以20.240524为中心的1000个数字作为初始值,分析去卷积结果与文本数码之间的偏差。通过范数度量去卷积结果与文本代码之间的距离,其中范数采用如下公式

$$\| f^* - f \| = \sqrt{\sum_{n=1}^{l} (f^*[n] - f[n])^2}$$

如果$\| f^* - f \| = 0$,就意味着原始文本的数码已被成功破译。所以图3中的圆点表示成功破译的位置。此外,图3中的曲线显示范数近似趋于0,因为穷尽初始值保持接近真实初始值x_0. 上述结果基于Db3小波函数。

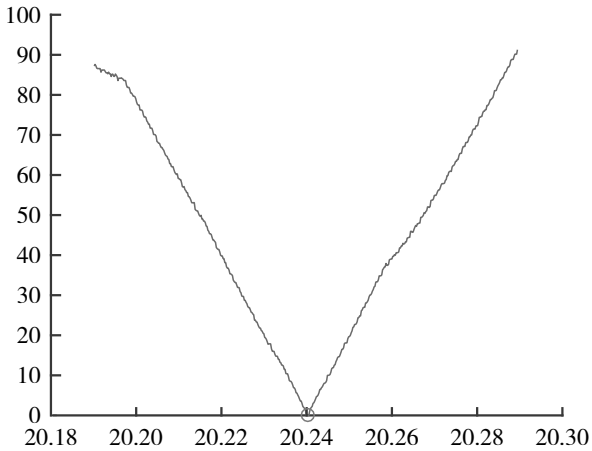

图3 去卷积结果与文本数码的偏差范数图

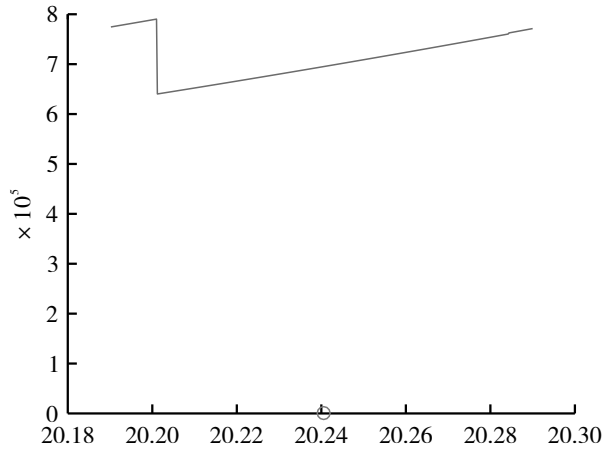

图4 利用Haar小波的去卷积结果与文本数码的偏差范数图

接下来,简要分析小波函数对解密文本代码的影响。假设其他条件保持不变,考虑使用Haar小波函数。计算范数以测量反卷积结果与文本代码之间的距离。在图4中,圆点表示成功解密的位置。曲线显示,当穷举的初始值不断接近真实初始值x_0时,范数并不趋向于0. 这表明,在文本解密过程中,小波函数与加密过程不一致,即使初始值不断接近真实初始值,反卷积的文本代码也与原始文本代码相去甚远。

此外,即使选择初始值x_0 = 20.240524,randn函数生成的随机数也与算法1生成的随机数不同。图5中,randn函数生成的随机数与图1中的差异较大。因此,文本数码无法轻易恢复。

一个包含所有文本字符的数据集也是恢复原始文本的最关键元素。这个数据集只由发送方和接收方保存,不会被攻击者截获。

为了估计运行时间,对1000组不同长度的文本进行测试,来展示这种基于小波随机数的新文本信息加密传输方法。表1和表2列出了运行时间的估计平均值。在表1中,第一行给出了加密文本的长度,第二行给出了文献[14]中小波数字水印方法的运行时间估计平均值,第三行给出了本方法中小波随机数和卷积的运行时间估计平均值。在表2中,第一行给出了解密文本的长度,第二行给出了小波数字水印方法的运行时间估计平均值,第三行给出了本方法中小波随机数和卷积的运行时间估计平均值。括号中的数据表示表1和表2中的估计标准偏差(S.D.)。

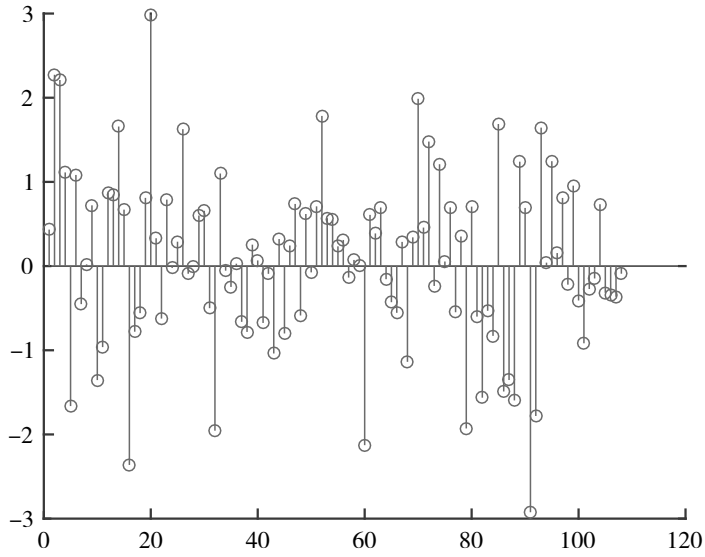

图5 randn函数生成的随机数图

表1 加密不同长度文本运行时间的估计平均值和标准差 单位:秒

Length	11	24	160	1600
Mean	0.0065	0.0066	0.0075	0.0173
(S.D.)	(0.0026)	(0.0026)	(0.0017)	(0.0052)
Mean	0.0017	0.0023	0.0036	0.0087
(S.D.)	(0.0011)	(0.0008)	(0.0009)	(0.0019)

表2 解密不同长度文本运行时间的估计平均值和标准差 单位:秒

Length	11	24	160	1600
Mean	0.00086	0.00088	0.00097	0.0016
(S.D.)	(0.0293)	(0.0297)	(0.0311)	(0.0401)
Mean	0.0019	0.0022	0.0037	0.0092
(S.D.)	(0.0011)	(0.0008)	(0.0009)	(0.0019)

隐藏过程中的不同长度文本内容如表3所示。

表3 不同长度文本内容

Length	Content
11	Hide Text!
24	“wavelet random number”
160	Leveraging Coverless Image Steganography to Hide Secret Information by Generating Anime Characters Using GAN [J]. Expert Systems with Applications, 2024, 248: 123420.
1600	文本内容过长,故省略。

与文献[14]中文本信息的加密方法相比,该文本的加密方法更简单、更快捷。但该文本破译方法比文献[14]中的小波数字水印方法慢。根据表1和表2中估计的标准差(S.D.),利用小波随机数和卷积的方法,加密文本过程和破译文本过程是稳定的。与小波数字水印方法[14]相比,采用小波随机数和卷积的方法估计的标准差更小。

最后,文章提出一种基于小波提升随机数和卷积公式的创新性文本信息编码技术。该技术采用小波提升随机数和小波基作为加密密钥,可以有效提升文本信息的安全防护水平。

6 研究展望

今后的研究中,进一步优化编码算法,提高编码速度和效率,以满足大数据时代对文本信息处理的高效需求。如,探索更多基于小波变换的加密方法,增强文本信息的安全性,抵御日益复杂的网络攻击。又如,将该编码方法应用于其他领域,如图像、音频等,实现跨媒体信息安全传输。研究编码方法的抗攻击性能,针对不同类型的攻击手段,提高系统的鲁棒性。同时,结合人工智能技术,实现编码方法的智能化,自动调整加密策略以应对不断变化的网络环境。

参考文献:

[1] DAUBECHIES I. Ten Lectures on Wavelets[M]. Sayam:SIAM,1992.

[2] PERCIVAL D B,WALDEN A T. Wavelet Methods for Time Series Analysis[M]. Cambridge:Cambridge University Press,2000.

[3] STINSON D R. Cryptography:Theory and Practice[M]. Boca Raton:Chapman an Hall/CRC Press,1995.

[4] ZHOU X H,GU G D. An Algorithm of Generating Random Number by Wavelet Denoising Method and its Application[J]. Computational Statistics,2022,37:107-124.

[5] FEKRI F, DELGOSHA F. Finite-field Wavelets with Applications in Cryptography and Coding[M]. Hoboken: Prentice Hall, 2011.

[6] YANG S G,LI C X,SUN S H. Text Information Hiding Method based on Chaotic Map and BCH Code in DWT Domain of a Carrier Image[C]. International Conference on Wavelet Analysis,2007,4:1754-1758.

[7] SAKKARA S, AKKAMAHADEVI D H, SOMASHEKAR K, et al. Integer Wavelet based Secret Data Hiding by Selecting Variable Bit Length[J]. International Journal of Computer Applications,2012,48(19):7-11.

[8] ALDAWLA N N H,KAZIM M M,KALE K V. Steganography Enhancement by Combining Text and Image Through Wavelet Technique[J]. International Journal of Computer Applications,2012,51(21):975.

[9] VESELSKA O,LAVRYNENKO O,ODARCHENKO R,et al. A Wavelet-based Steganographic Method for Text Hiding in an Audio Signal[J]. SENSORS(BASEL,SWITZERLAND),2022,22(15):5832.

[10] FEI P,HONG L L. A Steganalysis Method for 2D Engineering Graphics based on the Statistic of Geometric Features[J]. International Journal of Digital Crime and Foressics,2011,3(02):35-40.

[11] BERAM F G,DEZFOULI M A,YEKIAIE M H,et al. A New Steganography Method based on Optimal Coefficients Adjustment Process(OCAP)[J]. International Journal of Computer Applications,2014.

[12] SABIR F A. Hiding Encrypted Data in Audio Wave File[J]. International Journal of Computer Applications,2014,87(02):28-32.

[13] GUPTA S,JAIN R. An Innovative Method of Text Steganography[C]. Third International Conference on Image Information, 2015.

[14] ZHOU X H. Text Information Hiding and Recovery via Wavelet Digital Watermarking Method[J]. Scientific Reports, 2023,23(01):9532.

[15] REHMAN H A,BAJWA U I,RAZA R H,et al. Leveraging Coverless Image Steganography to Hide Secret Information by Generating Anime Characters Using GAN[J]. Expert Systems with Applications,2024,248:123420.

[16] KANG Y. A Computerized Information Security Communication Method based on Deep Learning Theory[J]. Applied Mathematics and Nonlinear Sciences,2024,9(01):2249.

[17] SWELDENS W. The Lifting Scheme:A Custom-design Construction of Biorthogonal Wavelets[J]. Appl Comput Harmon Anal, 1996,3(02):186-200.

[18] ZHOU X,GU G. The Construction of Multi-wavelets with Matrix Dilation via the Lifting Scheme with Several Steps[C]// Chinese Intelligent Systems Conference. Springer,Singapore,2019,592:11-23.

[19] JENSEN M J. Using Wavelets to Obtain a Consistent Ordinary Least Squares Estimator of the Long Memory Parameter[J]. Journal of Forecasting,1999,18(01):17-32.

A Boosted Wavelet Random Number Text Encryption Scheme

CAO Hang-bin ,WANG Gang*

(*School of Mathematical Sciences*,*Xinjiang Normal University*,*Urumqi*,*Xinjiang*,*830017*,*China*)

Abstract: Using the wavelet random number algorithm with convolution formula, a new encryption method for text messages is studied. First, an algorithm for simple and fast text message encryption is proposed. It is a text encryption algorithm based on Wavelet Random Number (TCAWRN). Second, a text decryption algorithm based on Wavelet Random Number (TDAWRN) is introduced. This algorithm uses the received data and a private key to recover the original text. This private key consists of an initial random value and a wavelet basis. Third, this encrypted transmission method for text messages is illustrated by an example. Finally, the security of the algorithm is discussed, including the wavelet random number, the wavelet basis function, and the running time.

Keywords: Wavelet Random Number; Wavelet reconstruction formula; Convolution