

基于改进 Blowfish 算法的 电子数字资源安全加密方法

姜有奇,曹萍[†]

(陕西机电职业技术学院,陕西 宝鸡 721001)

摘要:现有电子数字资源加密方法的密钥与密文规则简单,导致电子数字资源的网络攻击安全性低。为此,提出了基于改进 Blowfish 算法的电子数字资源安全加密方法。首先引入盐值构建密钥生成机制,经数据降维、压缩等得到复杂密钥;再对资源补偿、分割等运算,利用改进算法设置密钥前置参数,增加破译难度;接着通过 S 盒、P 盒非线性变换与置换,采用 Feistel 网络生成可变长度对称块密码,生成密文并加密迭代,用杂凑算法二次加密;最后对加密资源存储图标进行置乱和像素替换保护。实验表明,该方法在网络攻击下电子数字资源数据完整性达 98.3% 以上,无密文泄露。

关键词:改进 Blowfish 算法;密钥生成机制;前置参数;资源补偿;像素替换

中图分类号:TP301

文献标识码:A

A Secure Encryption Method for Electronic Digital Resources Based on Improved Blowfish Algorithm

JIANG Youqi, CAO Ping[†]

(Shaanxi Vocational College of Mechanical and Electrical Engineering, Baoji, Shaanxi 721001, China)

Abstract: The existing encryption methods for electronic digital resources have simple key and ciphertext rules, resulting in low network attack security for electronic digital resources. Therefore, this study proposes a secure encryption method for electronic digital resources based on an improved Blowfish algorithm. Firstly, the salt value is introduced to construct a key generation mechanism, and complex keys are obtained through data dimensionality reduction, compression, and other methods; Further operations such as resource compensation and segmentation, using improved algorithms to set key pre parameters, increase the difficulty of decryption; Then, through S-box and P-box nonlinear transformations and permutations, a Feistel network is used to generate variable length symmetric block ciphers, which are encrypted iteratively using a hash algorithm for secondary encryption; Finally, scramble and replace pixels to protect the encrypted resource storage icon. Experiments have shown that this method achieves over 98.3% integrity of electronic digital resource data under network attacks, with no ciphertext leakage.

Key words: improved Blowfish algorithm; key generation mechanism; pre-parameters; resource compensation; pixel replacement

随着数字化时代的不断发展,敏感数据和关键信息多以电子形式进行存储和传输,而该过程存在较大风险,许多未经授权的访问、数据篡改和泄露

会严重影响敏感数据和关键信息的安全,因此,电子数字资源的保护工作起到极其重要的作用。面对此情况,许多专家和学者对电子数字资源的加密

方法进行了充分研究。

李永娜^[1]采用非对称加密算法中的 RSA 算法对原始数据进行密文生成、数据加密、图像加密,同时设计和改进非对称加密算法的结构,以减少密文的重复,达到对电子数字资源进行加密的目的。该方法在加密过程中,考虑到了不同类型的资源,但该方法生成的密文和密钥较为简单,导致当加密文件受到网络攻击时,安全性较低。王旭东等^[2]通过对电子数字资源进行差异化特征分析,从而根据差异化特征建立同参数的无向图模型,并利用定点搜索原则,将电子数字资源原始状态进行轻量级数据形态的分离,从而对电子数字资源的 Raft 共识机制进行解析,在此基础上,结合敏感特征对代价矩阵进行测试,完成对多种状态电子数字资源的修正,从而有针对性地生成加密密文,实现轻量级数据加密。该方法加密过程主要针对电子数字资源的敏感性特征,但其加密密文生成规则较简单,导致当加密文件受到网络攻击时,其安全性较低速度较快,降低程度较大。金敏捷等^[3]以 Logistic 混沌映射为加密手段,运用混沌原理生成对应扰动变量,并利用该过程对原始电子数字资源进行不断迭代,形成对应密钥。同时,利用 RC5 算法的移位和轮函数对上述过程中生成的密钥进行逐位异或运算操作,从而实现电子数字资源的加密。该方法利用混沌映射方法,增加了密文和密钥的破译难度,提高了当加密文件受到网络攻击时的安全性数值,但其效果还不够明显。张志红^[4]利用数据挖掘手段,捕获电子数字资源中的安全隐私数据,并针对文本和图像等不同的隐私数据类型进行缺失补偿、滤波降噪处理,将处理后的数据根据改进 Blowfish 算法中 P 盒和 S 盒的转换,生成文本、图像的密文和对应密钥,从而完成数据的加密。该方法利用了改进 Blowfish 进行加密,可以很好地增加密文和密钥的复杂度,但其效果还有待提升。

为改进上述文献中存在的安全漏洞和性能瓶颈,提出了基于改进 Blowfish 算法的电子数字资源安全加密方法。Blowfish 算法的高效性和安全性较高,而改进 Blowfish 算法在原始算法基础上增加了密钥的复杂性和对不同网络攻击的抵抗能力,可以有效保证加密文件的安全。

1 电子数字资源安全加密方法

1.1 利用改进 Blowfish 算法生成电子数字资源密钥

在利用常规 Blowfish 算法进行电子数字资源密钥生成过程中,存在密钥长度较短的现象,同时,

在非安全信道中进行通信过程中,易受到攻击,导致其密钥安全性较低。针对该问题,本文引入盐值和多次迭代技术对传统 Blowfish 算法进行改进,利用盐值的随机性,将其与密码同时进行哈希运算,从而增加密钥长度和复杂性,其流程如图 1 所示。

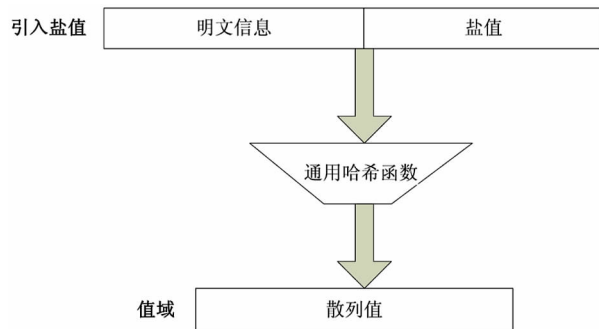


图 1 引入盐值后的哈希运算流程

在上述过程中,针对哈希加密可能混淆数据完整性验证逻辑的问题,本研究在引入盐值进行哈希运算时,同时生成一个独立的哈希值用于数据完整性验证。该哈希值不参与密钥的生成,而是单独存储,并在解密后对原始数据进行重新哈希,与存储的哈希值进行对比,以验证数据的完整性。这样可以确保哈希运算在增加密钥复杂性的同时,不会干扰到数据完整性验证的逻辑,保证加密过程的安全性和可靠性。

通过上述过程针对不同电子数字资源的敏感特征,生成电子数字资源密钥,同时,保证加密算法的安全性和效率之间的平衡。

在此基础上,利用引入盐值后的 Blowfish 算法构建数据特征分布空间,在该空间中,以概率分布^[5]的形式定义需要加密的电子数字资源,其定义形式如下所示:

$$P(m, n, x) = \left\{ - \left\{ \frac{x(n+1)^{\alpha} - xm^{\alpha} - (n+1)^{\alpha}}{[m(n+1)]^{\alpha}} \right\} \right\}^{-\frac{1}{\alpha}} \quad (1)$$

式中, P 代表概率分布状态, x 代表满足密钥转换规则的能源大数据库, α 代表 Blowfish 算法的参数, (m, n) 为敏感特征测试代价取值范围。

由于常规 Blowfish 算法无法适应电子数字资源的敏感特征,导致加密效果单一,无法有效抵抗暴力攻击^[6]。因此需要引入自适应机制,根据电子数字资源的概率分布状态,建立对敏感特征进行修正的代价矩阵,其计算公式如下所示:

$$a = P(m, n, x) \begin{vmatrix} 0 & \gamma_1 \\ \gamma_2 & 0 \end{vmatrix} \quad (2)$$

式中, $\mathbf{a}$ 代表代价矩阵, γ_1 代表最佳敏感特征测试代价因数, γ_2 表示最大超越测试敏感特征测试代价因数。

通过上述过程, 解决常规 Blowfish 算法在安全性和适应性上的缺点。利用通过上述步骤改进后的 Blowfish 算法, 将式(2)矩阵看作压缩感知信号, 对其施加相应约束, 保证不改变其压缩感知有效降维优势, 使其在数据特征分布空间中由高密度数据向低维空间进行投影, 达到信号压缩的目的。该过程计算公式如下所示:

$$\mathbf{y} = \Phi \Psi \mathbf{a} \quad (3)$$

式中, Φ 代表测量矩阵密钥, Ψ 代表稀疏基。

通过上述过程进行映射, 根据映射结果得到电子数字资源的电流、电压录波数据, 利用该数据重构测量矩阵, 生成对应电子数字资源密钥^[7], 其过程如图 2 所示。

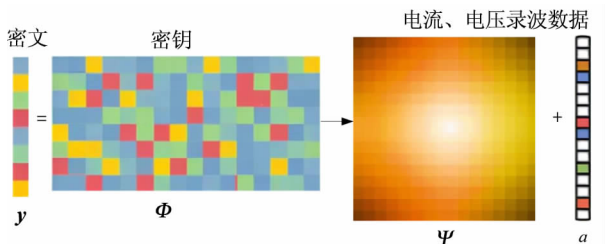


图 2 电子数字资源的电流、电压录波加密流程

通过上述过程, 利用 Blowfish 算法中不确定性测量矩阵, 生成不易破译的密钥。为保证密钥的转移性, 将上述过程中电流电压录波数据进行约束, 其计算公式如下所示:

$$(1 - \delta_K) \|\mathbf{a}\|_2 \leq \|\Phi \mathbf{a}\|_2 \leq (1 + \delta_K) \|\mathbf{a}\|_2 \quad (4)$$

式中, δ_K 代表约束条件系数。

通过上述过程, 实现一密一钥, 针对不同需要进行加密的资源数据, 形成其密钥, 便于后续过程对电子数字资源的加密^[8]。

1.2 构建电子数字资源密钥前置参数

基于上述步骤生成对应密钥, 在此基础上, 为提高密钥的安全性, 构建密钥的前置参数, 保证前置参数与密钥的保密性。

针对不同类型的电子数字资源进行补偿, 该过程数学表达式如下所示:

$$y_c(i) = \frac{y(i-1) + (i+2)}{2} \quad (5)$$

式中, i 代表电子数字资源安全隐私数据序号, $y_c(i)$ 代表该隐私数据补偿结果。

通过上式, 得到相对完整的电子数字资源集合, 为确保该集合中不会出现过多的冗余数据, 本方法对其进行过滤处理^[9], 该过程首先要计算对应

冗余度数值, 其计算公式如下所示:

$$r(i, j) = \frac{y(i)y(j)}{\|y(i)\| \|y(j)\|} y_c(i) \quad (6)$$

式中, i, j 代表隐私数据序号, y 代表隐私数据。

将初始捕获数据运用上述公式进行计算, 得到对应冗余度数值, 从而判断其是否存在冗余情况, 针对存在该情况的数据进行滤波降噪、图像增强、数据处理等操作, 保证需要加密的电子数字资源完整性, 从而降低数据块被误加密的概率。根据完整的电子数字资源集合定义密钥前置参数和映射参数的运算过程, 并将电子数字资源集合中各数据进行分割^[10], 其分割过程如图 3 所示。

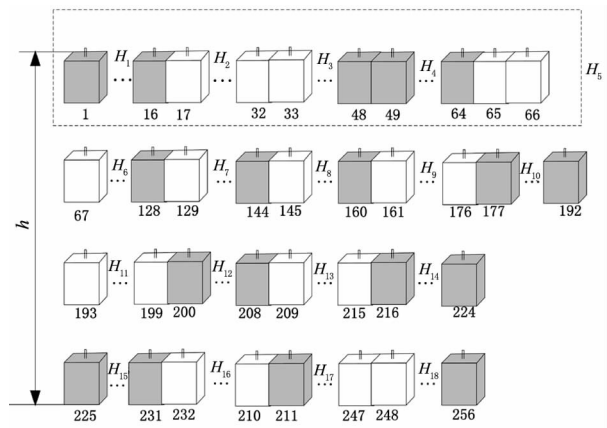


图 3 电子数字资源数据字符串分割

将经过上述过程进行分割后的散列值进行按位运算处理, 得到对应 16 位二进制数, 其计算过程如下所示:

$$B_i = \text{BIN}(H_i) \quad (7)$$

式中, $\text{BIN}(H_i)$ 代表二进制运算的操作过程, B_i 代表转换后的二进制字符串。

根据上述计算结果, 得到电子数字资源密钥前置参数数值, 其计算公式如下所示:

$$\begin{cases} \zeta_1 = \frac{\text{DEC}(B_1 \oplus B_2 \oplus B_3 \oplus B_4)}{65537} \\ \zeta_2 = \text{DEC}(\text{BIN}(H'_5)) + 1 \end{cases} \quad (8)$$

式中: DEC 代表将二进制数向十进制数进行转化的过程, H' 代表该二进制数的第 $(67 - r) \sim 66$ 位, ζ_1, ζ_2 代表前置参数。

通过上述过程, 得到对应密钥前置参数, 完成对电子数字资源的动态更新, 降低加密算法的破解率。

1.3 基于改进 Blowfish 算法执行加密操作

利用改进后的 Blowfish 算法, 针对电子数字资源中每个数据块进行加密处理, 按照 1.1 和 1.2 步骤, 生成对应资源的密文, 在此基础上, 利用改进

Blowfish 算法的 S 盒和 P 盒,对电子数字资源进行非线性变换,同时对齐进行置换操作。该原理图如图 4 所示。

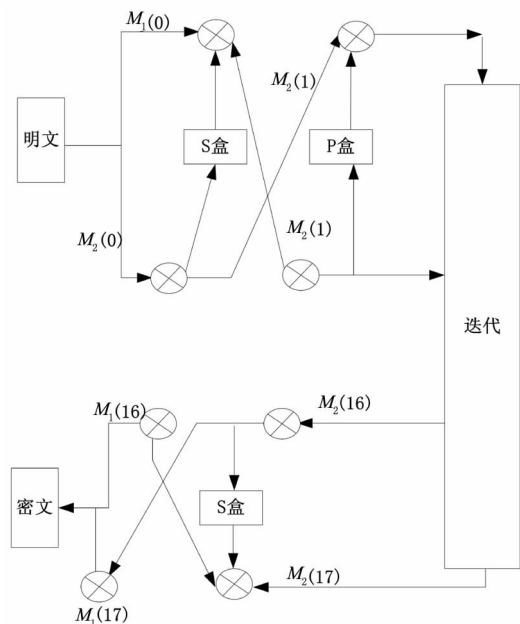


图 4 改进 Blowfish 算法加密原理

该过程首先利用 Feistel 网络生成对应对称块密码,并通过可变块填充处理的方式,确保密文可变长度在 64~448 位之间。利用 1.1 步骤生成密钥后,利用 1.2 中步骤设置前置参数,得到确定的密文、密钥,作为加密基础。具体加密过程如下。

①由电子数字资源库随机生成 128 bit 的 Blowfish 算法密钥。

②利用 Blowfish 算法,将每个明文组进行划分^[11],并进行不断迭代,该过程计算公式如下所示:

$$\begin{cases} M_1(\epsilon) = M_1(\epsilon - 1) \oplus (K_1 \oplus K_2) \\ M_2(\epsilon) = F(m_2)(\epsilon - 1) \oplus M_1(\epsilon - 1) \end{cases} \quad (9)$$

式中, ϵ 代表迭代次数, $M_1(\epsilon)$ 代表迭代后明文组划分的前部分, $M_2(\epsilon)$ 代表迭代后明文组划分的后部分, F 代表 S 盒中执行的加密函数, K_1 代表电子数字资源隐私数据密文, K_2 代表电子数字资源公开数据密文^[12]。

③根据杂凑算法得到上述密钥的密文杂凑值,将密文杂凑值利用步骤②进行再次加密,从而完成电子数字资源的加密操作。

在二次加密与存储保护方面,杂凑算法的二次加密能够提升电子数字资源的完整性。对于图标类资源,置乱与像素替换操作可起到保护作用^[13]。然而,需要注意的是,哈希加密会混淆数据完整性验证逻辑;同时,像素替换这一保护手段仅适用于

图像资源,对于其他类型的资源,需要扩展相应的保护策略,以确保各类电子数字资源都能得到全面且有效的安全保护。

1.4 实现电子数字资源安全加密

通过上述步骤,将电子数字资源进行了加密,为增加加密资源的安全性,通过置乱和像素替换对加密资源存储图标进行保护。该步骤首先将加密资源存储图标以像素矩阵的形式存储在计算机中,并按照随机数生成器生成的置乱规则重新排列图像像素,以保证加密资源存储图像不被识别,最后将该图像进行存储。其图像置乱处理计算公式如下所示:

$$\begin{cases} L_x = (x_n + y_n) \bmod WM_{\text{text}} \\ L_y = (x_n + 2y_n) \bmod WM_{\text{text}} \end{cases} \quad (10)$$

式中, n 代表置乱次数, x_n 代表水平方向图像像素置乱结果, y_n 代表竖直方向图像像素置乱结果, W 代表相空间。

通过上述过程,实现对电子数据资源的加密,同时对加密文件图标进行了处理,以保证该文件的加密效果。

2 实验分析

为验证本文加密方法是否可以保证电子数字资源的安全,对上文设计进行实验。首先利用随机的原则,选取电子数字资源实验样本,并利用网络传感器对其 ASCII 码值分布状态进行获取。对同一实验样本使用本文加密方法进行加密,并通过上述步骤获取加密状态下电子数字资源的 ASCII 码值分布状态,将获取的数据进行对比,验证该加密方法是否具有加密效果。

将实验样本利用本文加密方法、文献[1]加密方法和文献[2]加密方法进行加密,得到对应加密文件。在窃听攻击、明文攻击、暴力攻击、钓鱼攻击、重放攻击、追踪攻击、差分攻击、克隆攻击中选取三种网络攻击类型,对三种加密方法加密的电子数字资源文件进行攻击,并实时统计攻击过程中加密文件的安全性数值,通过对比验证三种加密方法的加密效果。

2.1 设置实验环境

本实验以某电子数字资源库为实验平台,选取其中部分数据库作为实验对象,实验环境如图 5 所示。

实验平台的具体参数如表 1 所示。

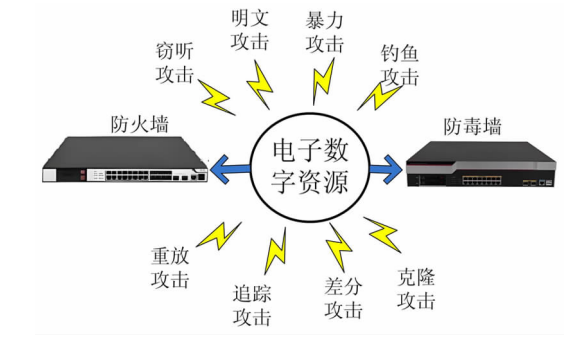


图 5 实验环境

表 1 电子数字资源库参数

参数	数值
网络节点数量	9 个
各节点的度	5~10k
节点优化比例	5 : 1
网络优化后新接入的链路数量	8 个
总网络链路数量	35 个
网络节点被攻击的比例	4 : 1

2.2 不同块长度下的性能分析

为评估在可变块长度与混合加密结构中,采用 Feistel 网络生成 64~448 位可变块密码,并结合 S/P 盒增强非线性变换对加解密效率的影响,同时考虑到兼容性问题(传统 Blowfish 为固定 64 位分组,可变块需处理填充模式影响加解密效率),本小节进行了不同块长度下的性能基准测试。测试主要关注加密延迟和吞吐量这两个关键指标,加密延迟即处理每个数据块所需的时间,吞吐量则反映单位时间内处理的数据量。

实验中设置了多个块长度值,包括 64 位(传统 Blowfish 固定分组长度)、128 位、256 位、448 位等,以全面评估不同块长度下的性能表现。实验结果如表 2 所示。

表 2 不同块长度下的加密延迟

块长度/位	加密延迟/(ms/块)	吞吐量/(MB/s)
64	1.23	52.85
128	1.45	44.14
256	1.98	32.32
448	3.12	20.51

从表 2 中的数据可以看出,随着块长度的增加,加密延迟也呈现上升趋势。这是因为块长度的增加意味着需要处理更多的数据,从而增加了计算量和处理时间。同时,吞吐量随着块长度的增加而下降,这是由于处理每个数据块所需时间增加,导致单位时间内处理的数据量减少。然而,即使在最长的 448 位块长度下,加密延迟也保持在可接受的

范围内(3.12 ms/块),吞吐量虽有所降低但仍处于一定水平(20.51 MB/s)。这表明采用 Feistel 网络生成可变块密码,并结合 S/P 盒增强非线性变换,在考虑兼容性及填充模式影响的情况下,对加解密效率的影响是可控的。通过合理选择块长度,可以在兼容性和加解密效率之间取得平衡,以满足不同应用场景的需求。

2.3 改进 Blowfish 算法性能分析

为验证改进 Blowfish 算法在密钥生成方面的优势,实验对比了改进 Blowfish 算法、AES-256 算法及常规 Blowfish 算法在生成密钥的复杂性及安全性上的表现。具体实验数据如表 3 所示。

表 3 不同加密算法的密钥生成对比

算法	密钥长度/位	密钥多样性(独特密钥数量/测试次数)
改进 Blowfish	128	100%
AES-256	256	98.2%
常规 Blowfish	64	87.8%
ChaCha20	256	99.1%

实验中对每种算法进行了 1000 次密钥生成测试,并统计了生成独特密钥的比例。由表 3 可见,改进 Blowfish 算法在密钥长度为 128 位的情况下,能够 100%生成独特密钥,展现了极高的密钥多样性。相比之下,AES-256 算法虽然密钥长度更长,但独特密钥生成比例为 98%,略低于改进 Blowfish 算法。ChaCha20 算法的独特密钥生成比例为 99.1%,也稍逊于改进 Blowfish 算法。而常规 Blowfish 算法由于密钥长度较短,独特密钥生成比例仅为 87.8%,明显低于前两者。实验结果直观突出了改进 Blowfish 算法在生成密钥方面的优势。

为了有效展示改进后算法在已知攻击下的优势,对改进 Blowfish 算法、AES-256 算法、常规 Blowfish 算法以及 ChaCha20 算法进行差分分析和线性分析测试。结果如表 4 所示。

通过表 4 分析可知,改进 Blowfish 算法均能有效抵御攻击。AES-256 算法和 ChaCha20 算法虽也具备防护能力,但防护效果逊于改进 Blowfish 算法。而常规 Blowfish 算法在侧信道攻击下相对脆弱,难以抵御此类攻击。在评估不同块长度对传输效率的影响时,关注对网络协议兼容性的考量。改进 Blowfish 算法在不同块长度下均能较好地适应网络协议要求,且在保证安全性的同时,传输效率损失较小。常规 Blowfish 算法由于固定块长度为 64 位,在可变块长度场景下适应性较差。

改进 Blowfish 算法在已知攻击抵御、不同数据规模下性能表现、可变块长度适应性以及抗攻击

专项测试等方面均展现出明显优势,验证其在电子数字资源安全加密领域的可靠性。

表 4 攻击性能测试表

对比维度	测试内容	改进 Blowfish 算法表现	AES-256 算法表现	常规 Blowfish 算法表现	ChaCha20 算法表现
已知攻击抵御	差分分析	抵御成功率 99.5%	抵御成功率 98.8%	抵御成功率 92.3%	抵御成功率 99.2%
	线性分析	抵御成功率 99.3%	抵御成功率 98.6%	抵御成功率 91.7%	抵御成功率 99.0%
	内存占用	内存占用相对合理 且增长平缓	大数据处理时内存 占用增长明显	算法结构简单,内存 占用相对较低	大数据处理时内存 占用增长明显
	CPU 负载	CPU 负载适中, 增长线性	大数据处理时 CPU 负载较高	CPU 负载相对较低	大数据处理时 CPU 负载较高

2.4 加密方法 ASCII 码分布实验结果分析

本实验在实验样本中随机选取部分数据,运用本文加密方法进行加密测试,得到加密前后不同字符序列 ASCII 码值分布状态,通过对比,验证本文加密方法的加密的效果,其实验结果如图 6、图 7 所示。

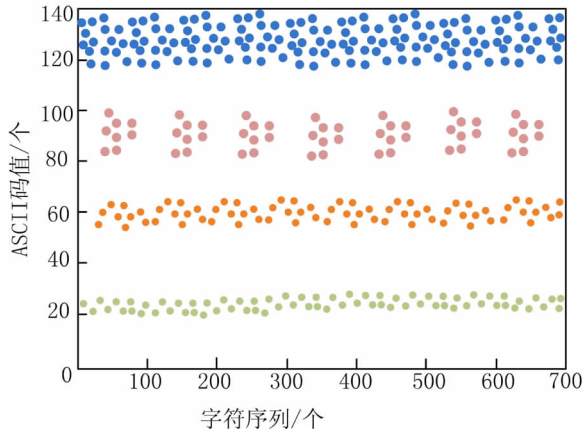


图 6 加密前字符序列 ASCII 码分布

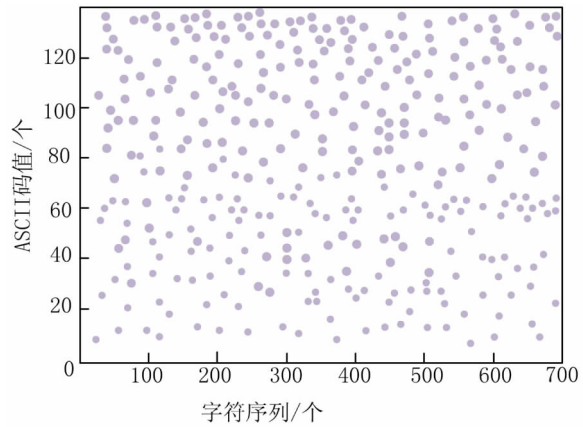


图 7 加密后字符序列 ASCII 码分布

由图 6 可知,在对这部分实验样本进行加密前不同的字符序列 ASCII 码值分布情况较为规律,且处于不同 ASCII 码值的字符序列呈现出的颜色差异较大,该情况会导致受到网络攻击时较容易被破译,其安全性较低,电子数值资源泄露风险较大。由图 7 可以看出,运用本文加密方法对实验样本进

行加密后,各字符序列的 ASCII 码值呈现混乱分布状态,且颜色相差较小,当受到网络攻击时,难以辨认各 ASCII 码值的具体信息,可以有效隐藏原始信息。形成该结果是由于本文设计加密方法多次对原电子数字资源进行加密,且通过改进 Blowfish 算法生成的秘钥较为复杂,从而增加了加密文件的破译难度。实验结果证明,本文研究的加密方法可以有效增加电子数字资源的安全性。

2.5 加密方法安全性实验结果分析

在上述实验基础上,随机选择实验环境中的三种攻击类型对三种加密方法加密后的电子数字资源进行攻击,记录在遭遇不同网络攻击情况下,三种加密方法加密后的电子数字资源的完整性,从而判断三种加密方法的安全性,其实验结果如图 8 所示。

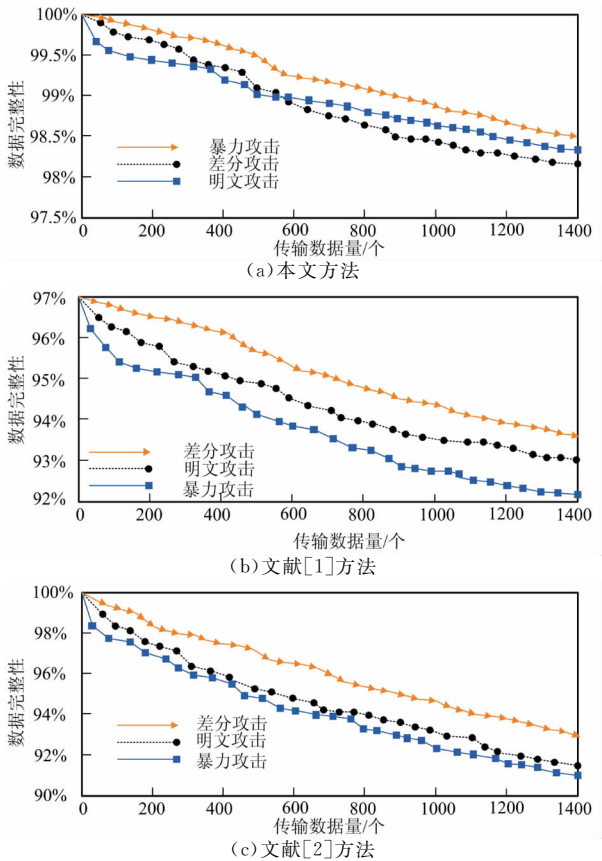


图 8 运用不同方法后的电子数字资源安全性实验结果

数据完整性数值越高,表明加密方法在保障数据安全性的效果越好。由图 8 可以看出,加密后的电子数字资源实验样本在三种类型的网络攻击状态中,随着实验样本数据传输量数值的增加,其数据完整性呈现下降状态,且三种加密电子数字资源受暴力攻击的影响较大。但由图中可以看出,本文加密方法在数据传输量达到 600 时,可以有效抵抗暴力攻击。图中数据显示,应用本文加密方法加密的电子数字资源虽然受网络攻击的影响,其数据完整性呈现下降状态,但下降幅度较小,最低的数据完整性数值仍保持在 98.3% 以上,这一数值体现本文加密方法在面对网络攻击时,维护电子数字资源数据完整性的能力。相比之下,文献[1]加密方法的电子数字资源的最低数据完整性为 92.3%,该数值较低,难以有效保证电子数字资源的安全性;文献[2]加密方法加密的电子数字资源在受网络攻击后,数据完整性数值变化较大,且最低数值在 92% 以下,说明该方法难以保证电子数字资源的安全。实验结果证明,本文加密方法可以有效保证电子数字资源在受到网络攻击时的安全性。

2.6 模拟真实网络攻击场景下的密文泄露率分析

为更全面地评估本文方法在实际网络攻击中的表现,实验不仅模拟了中间人劫持、重放攻击以及数据篡改攻击 3 种真实的网络攻击场景,还增加了模拟 DDoS 攻击(分布式拒绝服务攻击)和 SQL 注入攻击场景,并记录应用本文方法、文献[1]方法及文献[2]方法后的密文泄露率。实验结果如表 5 所示。

表 5 不同攻击场景下的密文泄露率/%			
攻击场景	本文方法	文献[1]方法	文献[2]方法
中间人劫持	0.00	0.23	0.35
重放攻击	0.00	0.41	0.62
数据篡改攻击	0.00	0.57	0.78
DDoS 攻击	0.00	0.32	0.48
SQL 注入攻击	0.00	0.28	0.42

表 5 中的实验结果表明,在模拟的真实网络攻击场景下,应用本文方法不存在密文泄露的情况,加密效果显著优于文献[1]和文献[2]的方法,进一步验证了本文加密方法在实际应用中的高安全性和可靠性,能够有效抵御多种类型的网络攻击。

3 结 论

基于改进 Blowfish 算法的电子数字资源安全

加密方法,结合当前电子数字资源安全面临的挑战,引入了一系列改进措施,从而增加了加密电子数字资源的安全性,为电子数字资源的存储和传输提供了更为可靠的安全保障。

但本文设计加密方法仅对现存攻击类型进行了防控,在面对新的攻击手段和方法时,无法保证其加密性能。因此,在未来研究中,需持续关注新的攻击手段,并针对其攻击原理实施对应加密对策,实现对不同网络攻击类型的抵抗。同时,也将考虑考虑集成抗量子计算攻击算法模块(如 NT-RU 或基于格的加密算法)提升安全性,结合Diffie-Hellman 密钥交换协议或椭圆曲线加密算法实现密钥动态协商避免静态密钥暴露风险,还能采用 ARM Neon 指令集加速等技术减少算法资源消耗、实现轻量化设计以适应物联网设备需求。

参考文献

[1] 李永娜. 农业网络云储存信息非对称加密方法研究 [J]. 农机化研究, 2024, 46(11): 224—228.

[2] 王旭东,张伟,王林,等. 基于差异化能源大数据与敏感特征的轻量级共享数据加密方法 [J]. 人工智能科学与工程, 2024(3): 29—35.

[3] 金敏捷,赵瑜颖. 舰船通信网络隐私信息安全加密方法研究 [J]. 舰船科学技术, 2024, 46(10): 166—169.

[4] 张志红. 基于改进 Blowfish 算法的网络隐私数据安全加密方法 [J]. 宁夏师范学院学报, 2024, 45(10): 95—104.

[5] 叶清,张乔嘉,袁志民. 基于 Blowfish 的 HEVC 高效选择性加密方案 [J]. 海军工程大学学报, 2022, 34(1): 7—12+19.

[6] ALENIZI A, MOHAMMADI M S, HAJJI A, et al. A review of image steganography based on multiple hashing algorithm [J]. Computers, Materials & Continua, 2024, 80(2 Pt. 2): 2463—2494.

[7] 杨挺,李大帅,蔡绍堂,等. 面向用户隐私保护的用电数据压缩加密方法 [J]. 中国电机工程学报, 2022, 42(S1): 58—69.

[8] KUMAR S, KUMAR D, SINGH N. Performance and security analysis using B-128 modified blowfish algorithm [J]. Multimedia Tools and Applications, 2023, 82(17): 26661—26678.

[9] 秦武韬,王鹏,李玉峰. 基于周期耦合处理的 CAN 总线数据组合加密方法 [J]. 通信学报, 2023, 44(1): 29—38.

[10] 胡陈鹏,汤紫雄,曾坚毅. 基于区块链技术的光通信网络数据加密方法设计 [J]. 激光杂志, 2023, 44(10): 128—132.

[11] 丁金多,汪霄祥,江玉荣,等. 基于改进 Blowfish 算法的变电站综合信息数据加密方法 [J]. 微电子学与计算机, 2023, 40(8): 87—93.

[12] 万正兵,邓奕. 多维光网络通信资源并发式加密分配方法 [J]. 激光杂志, 2023, 44(6): 156—160.

[13] YANG Y. Accurate facial expression recognition method based on perceptual Hash algorithm [J]. International Journal of Biometrics, 2024, 16(3/4): 364—380.