基于加密二维码的电力计量非电通信方法

白露薇，董永乐，张理放，毛永梅，殷超，席佳
（内蒙古电力科学研究院，内蒙古 呼和浩特 010020）

摘要：安全性是电力计量物联网必须要解决的关键核心问题。为使存储于公有云的外网数据和存储于私有云的内网数据完全隔离，实现由外网到内网的单向通信，提出了一种基于加密二维码的非电通信方法。该方法在外网侧利用彩色显示器生成包含计量送检信息的彩色二维码，在内网侧使用摄像头检测彩色二维码信息，使得外网数据只能单向传输至内网且内、外网之间无任何电气连接。同时为了提高安全性，该方法采用了颜色/信息混合加密方法，利用SM4算法对原始送检信息进行信息加密，进而生成单色二维码，然后利用彩色显示器色域丰富的特点，对生成的单色二维码利用不同颜色进行基于混沌的二次加密。实验表明，该方法在采用双重加密保障安全性的前提下，具有100%的加、解密正确率，同时不大于0.058 7 s的平均加、解密时间实现了准实时的数据传输，能够满足电力计量物联网在传输速率、安全性和可靠性等方面的要求。

关键词：电力计量；物联网；二维码；加密；非电通信
中图分类号：TM933 **文献标识码**：A **DOI**：10.19457/j.1001-2095.dqcd25684

Non-electric Communication for Power Measurement Based on Encrypted Two-dimensional Codes

BAI Luwei，DONG Yongle，ZHANG Lifang，MAO Yongmei，YIN Chao，XI Jia
（*Inner Mongolia Electric Power Research Institute*，*Hohhot* 010020，*Nei Mongol*，*China*）

Abstract：Security is a critical concern that must be addressed in the context of the electric power metering internet of things（IoT）. In order to achieve complete isolation between data stored in the public cloud（external network）and data stored in the private cloud（internal network），while enabling unidirectional communication from the external network to the internal network，a non-electric communication method based on encrypted QR codes was proposed. The method involved the generation of colored QR codes containing metering inspection information on the external network side. Data from the external network was transmitted unidirectionally to the internal network via these colored QR codes，with no electrical connection between the internal and external networks. To enhance security，a color/information hybrid encryption method was employed. The original inspection information was encrypted using the SM4 algorithm to generate monochrome QR codes. Subsequently，the monochrome QR codes were further encrypted using different colors by DNA and chaos，leveraging the rich color gamut of the display monitor. Experimental results demonstrate 100% accuracy in encryption and decryption，encryption and decryption computational speeds of less than 0.058 7 s，and linearly increasing time consumption. This method exhibits high accuracy and speed，meeting the requirements of electric power metering IoT systems in terms of transmission rate，security and reliability.

Key words：power measurement；internet of things（IoT）；two-dimensional code；encryption；non-electronic communication

随着我国电网规模不断扩大，各级电力计量中心接收的送检装置的数量和种类也日益增多，如何利用物联网、云计算等先进技术重组现有的计量装置、在保证数据安全性的前提下提升计量检测能力和质量，成为电力计量部门亟待解决的问题。

基于物联网架构的电力计量检定或测试的基本流程是：首先由客户提出送检需求，在基于

基金项目：内蒙古电力（集团）有限责任公司科技项目（2021-59）
作者简介：白露薇（1991—），女，硕士，工程师，主要研究方向为电力计量检测、图像处理，Email：18586208400@163.com

公有云的外网填写送检信息，并送检设备到客服中心；然后客服中心人员接收设备并检查设备是否可检，如果可检则将用户在外网录入的信息导入内部电力计量物联网后，再在内部电力计量物联网上补充完善信息并生成委托单；之后客服中心人员将被检样品分发到指定科室，室主任通过内部电力计量物联网把若干个检测任务分配给检测人员；随后检测人员领取样品，利用内部电力计量物联网所连接的若干个计量仪器对送检设备进行相应测试，相关测试过程数据自动上传到内部电力计量物联网，通过结论的对比，判断是否出具合格证书，并上传至内部电力计量物联网；然后测试人员归还样品及相关证书报告到客服中心，客服中心人员利用外网通知客户；最后客户到客服中心领取测试报告。

通过对上述电力计量检测流程的分析可知，内部电力计量物联网连接了计量检定仪器并存储了计量检定过程数据以及人员、检定任务等信息，其安全性要求高。目前有多种网络攻击形式，如拒绝服务（denial of service，DOS）攻击和恶性数据注入攻击（false data injection attack，FDIA）等[1-4]。为了使外网不能在未经授权的情况下访问内部电力计量物联网，同时使内部电力计量物联网数据不暴露到外网，必须在外网和内网之间采取安全隔离措施。目前常用的方法有两种，第一种是针对以电信号为基础的网络通信，采用物理隔离或逻辑隔离，诸如物理隔离卡、网络隔离组件[5-6]、自定义协议[7]、安全隔离网闸[8]等。第二种是非电通信，常见的实现形式是将外网数据复制到光盘、U盘等存储设备，再把存储设备数据复制到内网。第二种方式的优点是实现了外网数据到内网的单向传输，不存在内网数据外泄到外网的可能性，适用于电力计量场景，缺点是实时性差，不能实现内、外网数据的同步更新。利用二维码构成外网到内网的非电通信系统则可有效地克服第二种方式的缺点。二维码是用某种特定的几何图形按一定规律在平面（二维方向上）分布的、记录数据符号信息的图形，具有容量大、可靠性高等特点，一个二维码最多可以表示984个汉字字符或4 296个字母数据，完全可以满足电力计量外网送检数据存储的需要。同时二维码具有超高速识读的优点，可近似得到外、内网数据实时传输的效果。文献[9]提出了一种基于二维码的内外网物理隔离环境下的数据交换方法，并利用压缩算法来提高二维码携带信息的数量。此外从通信的连接方式上划分，二维码属于单工通信即数据传输方向是单向的，内网数据不会传输到外网，从根本上保证了电力计量的安全性。

虽然利用二维码实现电力计量物联网的非电通信具有诸多优势，但由于二维码属于可见光通信，二维码信息存在被恶意读取，进而造成内网数据外泄的风险，为此需要研究二维码的加/解密技术。信息加密是指对二维码数据分析之前的原始数据进行一次加密，再生成最终的二维码。已有的研究采用了多种加密算法来实现这一目标。文献[10]基于FES算法对原始数据进行加密生成单色二维码。文献[11]提出了一种结合了RSA和密钥的改进算法，对二维码原始数据信息进行加密。文献[12]提出了混沌加密数据的方法。但是上述这些单一的信息加密方式安全性低，一旦密钥泄露，很容易造成数据的外泄。

为提高安全性，文献[10]在用FES进行信息加密并生成二维码的基础上，再次使用FES对生成的二维码进行二次加密。文献[11]使用DES算法对二维码图形进行加密，使二维码原来有规律排列的黑白相间区域变成毫无规律排列的杂乱无章的黑白相间区域。但是上述这些方法依然是基于黑白二维码的改进，携带的数据量有限。

为提高传输数据量，文献[13]把DES算法、RSA算法两种加密算法结合使用对原始数据加密并生成彩色二维码。DES加密速度快，用于加密彩色二维码高容量数据信息；RSA加密安全性好，应用于DES密钥的加密。但是在此方法中RSA加密算法是对DES的密钥进行加密，并不是对数据本身进行混合加密。

除了上述基于密码学原理进行二维码加密的方法外，还有一些多学科启发性的研究。文献[14]强调对于数据权属的保证，实现了同时满足不同权限用户对于二维码信息的获取需求，通过分级加密的方式，将二维码信息进行分块加密处理。文献[15]针对嵌入水印的彩色二维码，提出了一种基于可变参数混沌系统的数字图像加密算法。文献[16]通过把DNA序列和SHA256算法的融合，实现对彩色二维码的加密和解密操作。文献[17]提出了一种基于光学理论中空间非相干光的二维码加密方法。文献[18]针对嵌入水印的彩色二维码，提出了一种基于可变参数混沌系统

的数字图像加密算法。文献[19]用元胞自动机模型来描述二维码加/解密过程,通过把状态空间设置为0和1,把ECA作为规则来构造加/解密算法,实验说明该方法在加/解密效率上有明显优势。上述这些加密算法计算量较高,安全程度相对较低,并且与二维码过程结合并不紧密,难以嵌入到二维码生成器中。

针对上述问题,本文提出了基于加密彩色二维码的非电通信方法,利用彩色显示器生成包含外网送检信息的颜色/信息双重加密的彩色二维码,内网计算机用摄像头捕获彩色二维码并进行解密来获取送检信息。这样既保证了加/解密效率,又保证了高安全性,体现在:1)SM4和3DES加密,加/解密速度快。2)利用彩色显示器生成加密彩色二维码,提高了传输的数据容量。3)对彩色二维码再进行混沌加密,保证了安全性。

1　系统组成

基于加密二维码的电力计量物联网非电通信方法的结构如图1所示。

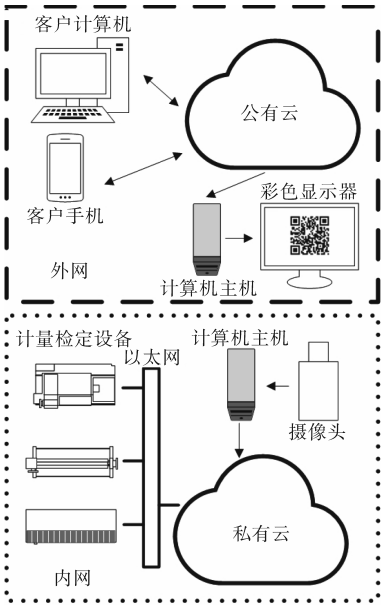


图1　基于加密二维码的电力计量物联网非电通信方法结构框图

Fig.1　Structure of the non-electric communication based on encrypted two-dimensional codes

用户通过PC、手机等终端访问基于公有云的外网,录入相关送检信息,运行于云端的应用程序将送检信息转换成加密二维码,并在彩色显示器上显示。目前常见的二维码有QR码、DataMatrix和PDF417等,这里选用QR码。从颜色上划分,二维码可分为单色二维码和彩色二维码。这里选用彩色二维码。其原因,一是彩色二维码比单色二维码的数据容量更大,例如16色彩色二维码的容量是单色二维码的4倍;二是利用二维码进行外、内网通信时,彩色显示器可以非常容易地显示出彩色二维码。

彩色二维码扫描器由摄像头和PC机构成,它捕获加密后的二维码图像,对其进行解密,然后将解密后的数据信息上传到内部电力计量物联网。内部电力计量物联网除了连接彩色二维码扫描器外,还与各种计量检定设备(如多功能功率电能比较仪等)相连,从而组成了全自动、智能化的计量网络。各类检测过程和结果数据可通过网络实时上传到私有云平台。

2　加/解密算法设计

2.1　加密算法流程

基于加密二维码的电力计量物联网非电通信方法的流程如图2所示。该算法首先对送检信息(即明文)利用SM4进行信息加密。

经过SM4加密后得到N位的密文,把这N位的密文按事先约定的规则分成m位一组、$N-m$位一组。对$N-m$这组数据进行单色QR二维码编码。

对于m位这组数据采用3DES进行加密。把单色QR二维码中的黑色像素定义为1,白色像素定义为0,将3DES加密后的颜色图像和单色QR二维码按像素进行乘法运算,即可得到颜色/信息混合加密的二维码。

将彩色二维码分解为3种二进制矩阵:红色(R)、绿色(G)、蓝色(B),根据DNA编码规则,得到对应的3个DNA序列P_r,P_g,P_b。使用SHA-256算法生成密钥矩阵$\boldsymbol{M}_{ke}$和Lorenz混沌系统的初始值(x_0,y_0,z_0)进行异或运算并置乱得到3个二进制矩阵$\boldsymbol{R}_e$,$\boldsymbol{G}_e$,$\boldsymbol{B}_e$。最后合并还原得到加密彩色二维码。

2.2　加密算法设计

2.2.1　SM4加密算法

SM4是一种分组密码算法,它的分组长度是16个字节,即128位、四字,对应的密钥的长度也是16个字节、128位、四字。采用迭代机制进行数据加密,总共需要32轮迭代和1次反序变换。由于SM4的分组长度是128位,所以输入的明文是四字,设其为(X_0,X_1,X_2,X_3),对这四字的明文进行32轮迭代。在每次迭代过程中都需要一个轮

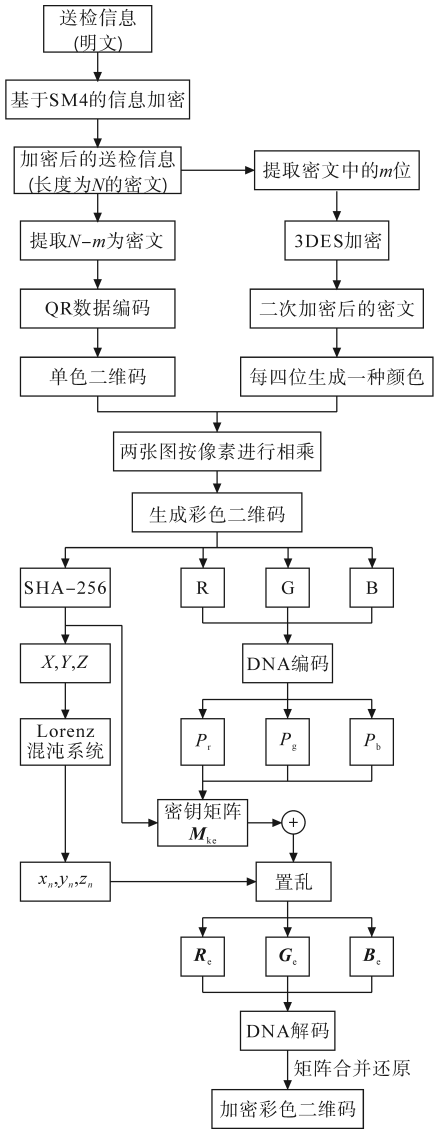


图2　加密流程图

Fig.2　Flowchart of information encryption

密钥。在第1轮迭代时，第5个字按下式计算：

$$X_4 = F(X_0,X_1,X_2,X_3,rk_0) \tag{1}$$

式中：F为轮函数，其通式为$F(X_i,X_{i+1},X_{i+2},X_{i+3},rk_i)$，$(X_i,X_{i+1},X_{i+2},X_{i+3})$为第$i+1$轮迭代的四字明文，$i=0,1,\cdots,31$，$rk_i$为第$i+1$轮密钥。

第6个字按下式计算：

$$X_5 = F(X_1,X_2,X_3,X_4,rk_1) \tag{2}$$

依次类推，可以得到：

$$X_{4+i} = F(X_i,X_{i+1},X_{i+2},X_{i+3},rk_i) \tag{3}$$

迭代执行32轮，即可得到36字$(X_0,X_1,X_2,\cdots,X_{31},X_{32},X_{33},X_{34},X_{35})$。

之后进行一次反序变换，也就是令密文：

$$(Y_0,Y_1,Y_2,Y_3) = (X_{35},X_{34},X_{33},X_{32}) \tag{4}$$

轮函数F的内部运算为

$$\begin{aligned} &F(X_i,X_{i+1},X_{i+2},X_{i+3},rk_i)\\ &= X_i \oplus T(X_{i+1}\oplus X_{i+2}\oplus X_{i+3}\oplus rk_i) \end{aligned} \tag{5}$$

式(5)中T是合成置换，其定义为

$$C = T(A) = L[\tau(A)] \tag{6}$$

式中：A为一字32位输入；C为一字输出；τ为非线性变换，以一个字$J=(j_0,j_1,j_2,j_3)$(其中$j_i(i=0,1,2,3)$是一个字节)作为输入，一个字$\boldsymbol{P}$作为输出；L为线性变换。

其中

$$\begin{aligned} \boldsymbol{P} &= [p_0,p_1,p_2,p_3]\\ &= \tau(J)\\ &= [Sbox(j_0),Sbox(j_1),Sbox(j_2),Sbox(j_3)] \end{aligned} \tag{7}$$

式中：$Sbox$为盒变换。

线性变换L是把输入的一个字循环左移24位得到相应的一个字输出。

2.2.2　3DES加密算法

3DES算法是对原始明文数据或解密数据进行3次DES加密或解密的过程，3DES的算法过程如下式所示：

$$S = E_{k3}\{D_{k2}[E_{k1}(D)]\} \tag{8}$$

式中：D为明文数据；k_1,k_2,k_3为密钥；S为密文。

首先以k_1为密钥对明文数据D进行DES加密，然后以k_2为密钥进行DES解密，最后以k_3为密钥进行DES加密得到最终的密文S。得到密文S后，以4位二进制数为一组把密文分组，把4位二进制数转换为与之对应的颜色，并依次分布在与单色二维码图像宽、高一致的图像里。

2.2.3　SHA-256算法

SHA-256是一种加密哈希函数，旨在将任意大小的数据映射到一个固定大小的哈希值，通常是256位。采用该算法生成彩色二维码的256 bits散列值，并将其作为混沌系统的输入；同时将该散列值定义为加密密钥K，将其分为32块，每块为8 bits，用于对二维码的加密，即

$$K = \{k_i\} \quad i = 1,2,\cdots,32 \tag{9}$$

将K按顺序分为3组，分别为k_1~k_{11}，k_{12}~k_{22}，k_{23}~k_{32}，计算Lorenz混沌系统的初始值：

$$\begin{cases} x_0 = X + (k_1\oplus k_2\oplus\cdots\oplus k_{11})/256\\ y_0 = Y + (k_{12}\oplus k_{13}\oplus\cdots\oplus k_{22})/256\\ z_0 = Z + (k_{23}\oplus k_{24}\oplus\cdots\oplus k_{32})/256 \end{cases} \tag{10}$$

式中：X,Y,Z为输入值K的3组值。

2.2.4　DNA序列

DNA序列中碱基有4种：A(Adenine)，C(Cy-

tosine),G(Guanine),T(Thymine),其中A和T互补,C和G互补,可以用二进制表示为00和11互补,01和10互补。如果用2 bits表示ATGC,则有24种编码规则,但是只有8种满足互补规则,如表1所示。

表1 DNA序列编码规则

Tab.1 DNA sequence encode rules

规则	A	T	G	C
1	00	01	10	11
2	00	10	01	11
3	01	00	11	10
4	01	11	00	10
5	10	00	11	01
6	10	11	00	01
7	11	01	10	00
8	11	10	01	00

在上述8种编码规则中,选择一种进行加密算法设计,本文使用规则1进行异或操作,变换规则如表2所示。

表2 DNA序列编码异或运算规则

Tab.2 DNA sequence encode XOR encode operation rules

异或	A	T	G	C
A	A	T	G	C
C	C	G	T	A
G	G	C	A	T
T	T	A	C	G

像素的灰度值可以被表示为8位二进制,编码成DNA序列。如果某个像素点的像素值为27,其二进制表示为00011011,根据编码规则1可以得到ATGC。DNA序列的加、减和异或操作都基于二进制中的运算规则,由两次异或后可以得到自身的特点,可以将其设计为彩色二维码的加/解密。

2.2.5 Lorenz混沌系统

混沌系统是一种具有高度敏感依赖初始条件的非线性系统,由它产生的序列具有随机特性,在数字图像加密中可以起到有效的保护和加密作用。Lorenz系统是一种经典的混沌系统,它是一组非线性的三维常微分方程,可以表示为

$$\begin{cases} \mathrm{d}x/\mathrm{d}t = a(y-x) \\ \mathrm{d}y/\mathrm{d}t = x(c-z)-y \\ \mathrm{d}z/\mathrm{d}t = xy-bz \end{cases} \tag{11}$$

式中:x,y,z为状态变量;t为时间;a,b,c为系统参数。

当a=10,b=8/3,c=26时,Lorenz吸引子如图3所示,代入系统初始值x_0,y_0,z_0实现对彩色二维码像素值的置乱。

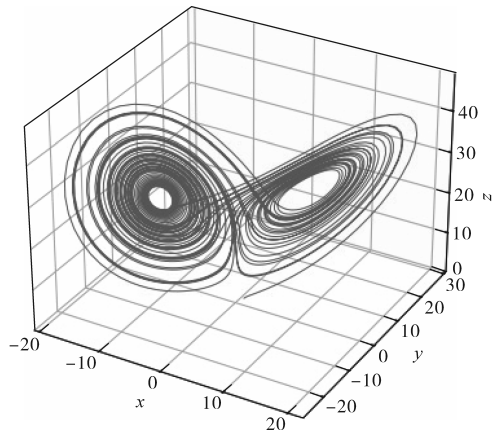


图3 Lorenz吸引子

Fig.3 Lorenz attractor

2.3 解密算法流程

连接在内网的彩色二维码扫描器通过解密获取外网的送检数据信息即明文。其步骤如下:

解密过程为加密过程的逆向操作,将加密彩色二维码进行DNA编码得到置乱的3个二进制矩阵$\boldsymbol{R}_e$,$\boldsymbol{G}_e$,$\boldsymbol{B}_e$,使用密钥矩阵$\boldsymbol{M}_{ke}$进行二次异或得到3个DNA序列P_r,P_g,P_b,再进行DNA解码得到还原后的彩色二维码。

将彩色二维码图像转换为8位bmp图像,由于摄像头不可能完全复原彩色显示器的色彩信息,所以取最接近的颜色所对应的二进制数,例如颜色W对应的8位RGB编码值为$w_7w_6w_5w_4w_3w_2w_1w_0b$,对应的4位二进制数为$v_3v_2v_1v_0b$。颜色Y对应的8位RGB编码值为$y_7y_6y_5y_4y_3y_2y_1y_0b$,对应的4位二进制数为$z_3z_2z_1z_0b$,且满足

$$w_7w_6w_5w_4w_3w_2w_1w_0b < y_7y_6y_5y_4y_3y_2y_1b$$

摄像头捕获的颜色U对应的8位RGB编码为$u_7u_6u_5u_4u_3u_2u_1u_0b$,且满足

$$w_7w_6w_5w_4w_3w_2w_1w_0b < u_7u_6u_5u_4u_3u_2u_1u_0b < y_7y_6y_5y_4y_3y_2y_1b$$

则当

$$\left|u_7u_6u_5u_4u_3u_2u_1u_0b - w_7w_6w_5w_4w_3w_2w_1w_0b\right| \leqslant \left|y_7y_6y_5y_4y_3y_2y_1y_0b - u_7u_6u_5u_4u_3u_2u_1u_0b\right|$$

时,把颜色U对应的4位二进制数设为$v_3v_2v_1v_0b$。当满足

$$\left|u_7u_6u_5u_4u_3u_2u_1u_0b - w_7w_6w_5w_4w_3w_2w_1w_0b\right| > \left|y_7y_6y_5y_4y_3y_2y_1y_0b - u_7u_6u_5u_4u_3u_2u_1u_0b\right|$$

时，把颜色U对应的4位二进制数设为$z_3z_2z_1z_0b$。把所有颜色对应的若干个4位二进数一组的数据拼接为m位的数据后，利用3DES进行解密，如下式所示：

$$D = D_{k1}\{E_{k2}[D_{k3}(S)]\} \tag{12}$$

即以k_1为密钥进行DES解密，然后以k_2为密钥进行DES加密，最后以k_3为密钥进行DES解密。

然后把彩色二维码图像进行二值化，得到单色的QR二维码并对其进行解码得到SM4加密后的密文，对该密文进行SM4解密，SM4的解密过程也需要32轮迭代和1次反序变换。与加密的不同之处在于在轮迭代的时候，逆序使用轮密钥，如第一轮使用rk_{31}，第二轮使用rk_{30}，依次类推，最终得到$N-m$位二进制数。

最后把m位二进制数和$N-m$位二进制数按事先约定的顺序进行组合得到完整的送检信息明文。

3　实验验证

利用如图4所示的实验系统对非电通信方法验证，与外网相连的计算机的CPU为i5-11400，显示采用P24A2G，色数16.7百万色，分辨率1 920×1 080。与内网相连的计算机的CPU为I3-4120U，摄像头采用罗技C270i，MJPG模式下1 280×960分辨率的帧率为30 FPS。编程语言使用Python，单色QR二维码生成和解码采用Zxing。

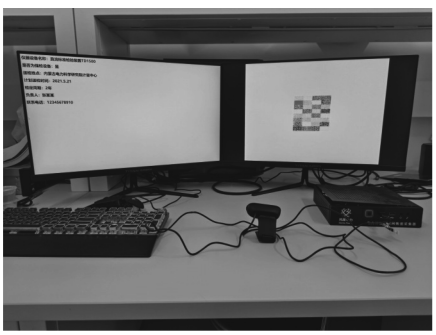


图4　实验系统组成

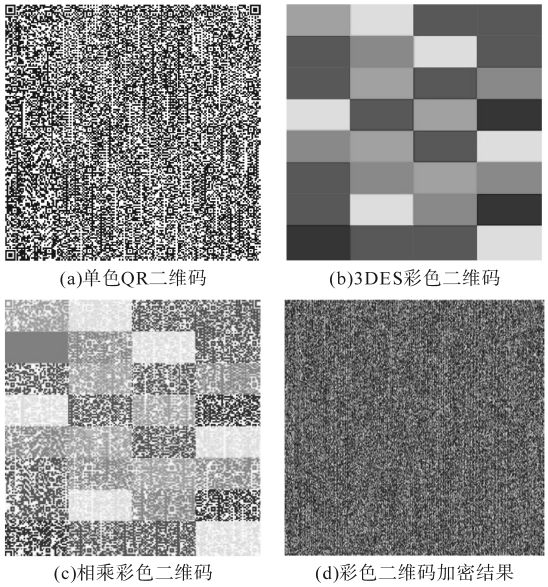
Fig.4　Structure of the experiment system

首先对如表3所示的单个送检信息表格中的文字进行颜色/信息混合加密，明文共540个汉字，用SM4进行加密，加密后的密文是13 056位，取12 928位进行单色QR二维码编码，如图5a所示，取其中128位进行颜色加密，如图5b所示。将图5a和图5b的图像进行像素相乘运算，得到颜色/信息加密的结果如图5c所示。基于SHA-256和DNA序列对图5c进行混沌加密得到的结果如图5d所示。

表3　送检信息示例

Tab.3　Example of testing data

仪器设备名称	是否为强检设备	送检地点	计划送检时间	检定周期	负责人	联系电话
直流标准检测装置TD1500	是	内蒙古电力科学研究院计量中心	2021年5月21日	2 a	张某某	12345678910



(a)单色QR二维码　(b)3DES彩色二维码

(c)相乘彩色二维码　(d)彩色二维码加密结果

图5　单个送检信息实验结果

Fig.5　Experiment on one sample

对图5d中的二维码进行识别和解密，得到的结果与表3一致，说明所提基于加密二维码的电力计量物联网非电通信方法是可行的。

为了验证所提方法的通信性能，把送检信息分为4组，每组送检信息个数分别5个、10个、50个、100个，由于罗技摄像头C270i的帧率为30 FPS，所以把每个送检信息传输时间间隔设为0.5 s，实验数据如表4所示。总耗时指的是每组送检信息以文字形式从外网发送，直至最终内网收到每组全部文字形式送检信息的全部时间。平均加解密时间由一组内每条送检信息加/解密时间累积求和后除以一组内送检信息总条数得到。

表4　通信性能实验数据

Tab.4　Experimental data of communication performance

序号	送检信息个数	总耗时/s	正确率/%	平均加/解密时间/s
1	5	2.87	100	0.058 7
2	10	5.39	100	0.057 4
3	50	25.34	100	0.053 2
4	100	50.36	100	0.057 5

由表4可知,不同分组下本文所提方法的正确率都为100%,说明该方法是可靠的。总耗时与送检信息个数成正比,说明该方法传输速度快且稳定,不存在拥塞的问题。平均加/解密时间都不大于0.060 2 s,说明加/解密算法计算速度较快,不会对数据传输时间产生显著影响。表5为本文与其它加/解密算法加密和解密时间的对比。

表5　不同加密算法效率对比

Tab.5　Comparison of efficiency of different encryption algorithms

算法	数据长度/Byte	加密时间/ms	解密时间/ms
DES	100	13.918	13.987
RSA	100	125.275	127.574
DES&RSA	100	43.451	42.304
本文算法	100	14.645	14.598
DES	200	16.312	16.228
RSA	200	127.786	129.453
DES&RSA	200	48.920	48.051
本文算法	200	17.928	18.002
DES	400	17.854	17.052
RSA	400	130.172	130.354
DES&RSA	400	56.044	61.194
本文算法	400	21.589	20.537

从表5可以看出,随着数据长度的增加,每种算法加/解密时间也随之增加。在加密数据长度相同的条件下,DES算法明显比RSA效率更高,耗时更短,加密耗时最多减少112.32 ms,解密耗时最多减少113.59 ms,但DES算法安全性不高,数据与密钥的安全性都无法得到保证。基于DES与RSA的混合加密算法,结合了两者的优点,但是在此方法中RSA加密算法是对DES的密钥进行加密,并不是对数据本身进行混合加密。本文所提出的方法,在加/解密时间上仅比DES算法稍多,加密时间最多多出21%,解密时间最多多出20.4%,但比其他两种算法耗时都要少,且该方法对彩色二维码进行的混沌加密更进一步提高了安全性,取得了算法耗时与安全性之间的平衡。

4　结论

本文基于颜色/信息混合加密的二维码实现了电力计量物联网中内、外网之间的数据非电通信。在通信形式上,外网送检信息编码为二维码,内网采用摄像头捕获识别二维码,内、外网之间没有任何电气连接,实现了内、外网之间的物理隔离和外网到内网数据信息的单向传输。在安全性上,充分利用彩色显示器色域丰富的特点,把信息加密并生成单色二维码的基础上,将数据二次加密并编码为颜色,从而构造了颜色/信息混合加密的彩色二维码。同时利用SHA-256和DNA序列对彩色二维码进行混沌加密,克服彩色二维码易伪造、抗攻击能力弱的安全缺点,有效防止内、外网数据通信时的信息外泄。实验证明该方法具有100%的加/解密正确率,平均加/解密时间不大于0.058 7 s,可实现准确实时的数据传输,从而满足传输速率、安全性和可靠性等方面的要求。

本文在实际应用中还需要做出更进一步研究,具体待改进的内容为:

1)本文中的送检信息包含了汉字、数字和字母,但不包含诸如送检实物照片等图片类送检信息,后续可以开展送检信息中包含图片的研究工作。

2)本文实验中所生成的二维码是无损的,但在实际应用中显示器显示二维码时可能因为环境光照条件、异物等导致颜色变化、遮挡等问题,如何处理上述问题,后续将做进一步研究。

参考文献

[1] 吴宁,蔡杰,梁公豪,等. 基于SM2的电力广域测量系统安全认证方案[J]. 电气传动,2023,58(3):84-90.
WU Ning, CAI Jie, LIANG Gonghao, et al. Security authentication scheme of power wide area measurement system based on SM2[J]. Electric Drive, 2023, 58(3): 84-90.

[2] 朱海鹏,赵磊,秦昆,等. 基于大数据分析的电力监控网络安全主动防护策略研究[J]. 电测与仪表,2020,57(21):133-139.
ZHU Haipeng, ZHAO Lei, QIN Kun, et al. Active protection strategy of power monitoring network security based on big data analysis[J]. Electrical Measurement & Instrumentation, 2020, 57(21): 133-139.

[3] 邓勇,彭敏放,刘靖雯,等. 电力信息物理系统建模和信息攻击机制分析[J]. 电力系统及其自动化学报,2021,33(10):10-17.
DENG Yong, PENG Minfang, LIU Jingwen, et al. Modeling of cyber power physical system and analysis of information attack mechanism[J]. Proceedings of the CSU-EPSA, 2021, 33(10): 10-17.

[4] 熊海军,张凯. 电力设备监控系统无线网络结构设计策略研究[J]. 电测与仪表,2020,57(21):24-31.
XIONG Haijun, ZHANG Kai. Research on design strategy of wireless network structure in power equipment monitoring systems[J]. Electrical Measurement & Instrumentation, 2020, 57(21): 24-31.

[5] 梅沁，李大伟，虎啸．基于NB-IoT的电力物联网安全技术研究[J]．电力信息与通信技术，2019，17(1)：100-104.
MEI Qin，LI Dawei，HU Xiao．Research on security technology of power internet of things based on NB-IoT[J]. Electric Power Information and Coummunication，2019，17(1)：100-104.

[6] 何张鑫．面向配电网安全的网络隔离组件的研究开发[D]．北京：华北电力大学，2020.
HE Zhangxin. Research and development of network isolation components for distribution of network security[D]. Beijing：North China Electric Power University，2020.

[7] 王静，高昆仑，张波． 基于网络隔离与安全数据交换的发电集团双网体系研究与设计[J]．电信科学，2017，33(2)：163-172.
WANG Jing，GAO Kunlun，ZHANG Bo. Research and design in dual network scheme of power corporation based on network isolation and secure data exchange[J]. Telecommunications Science，2017，33(2)：163-172.

[8] 薛洛良，孟宪胜，胡潇斐，等．基于内外网隔离技术的电力物资结算单据系统研究[J]．电子元器件与信息技术，2020，4(9)：102-103.
XUE Luoliang，MENG Xiansheng，HU Xiaofei，et al．Research on power material settlement document system based on internal and external network isolation technology[J]. Electronic Component and Information Technology，2020，4(9)：102-103.

[9] 韩林，张春海，徐建良．基于二维码的内外网物理隔离环境下的数据交换[J]．计算机科学，2016，43(11)：520-522.
HAN Lin，ZHANG Chunhai，XU Jianliang. Data exchange based on QR code in physically isolated internal and external network environment[J]. Computer Science，2016，43(11)：520-522.

[10] 曹翔．机械产品二维码加密技术研究与应用[D]．兰州：兰州理工大学，2018.
CAO Xiang. Research and application on QR code encryption method of mechanical product[D]. Lanzhou：Lanzhou University of Technology，2018.

[11] 杨丽娟，孙红艳，李瑛．RSA算法在QR码防伪技术中的应用[J]．北华航天工业学院学报，2014，24(2)：24-27.
YANG Lijuan，SUN Hongyan，LI Ying. Application of RSA algorithm in QR code oriented anti-counterfeiting technology[J]. Journal of North China Institute of Aerospace Engineering，2014，24(2)：24-27.

[12] 张定会，郭静波，江平．QR码二值图像混沌加密与解密[J]．移动通信，2011，35(Z1)：131-134.
ZHANG Dinghui，GUO Jingbo，JIANG Ping. Chaos encryption and decryption for QR binary image[J]. Mobile Communications，2011，35(Z1)：131-134.

[13] 张维纳．基于混合加密算法的彩色QR码技术研究与实现[D]．桂林：桂林电子科技大学，2021.
ZHANG Weina. Research and implementation of color QR code based on hybrid encryption algorithm[D]. Guilin：Guilin University of Electronic Technology，2021.

[14] 杨康，袁海东，郭渊博．基于属性加密的二维码分级加密算法[J]．计算机工程，2018，44(6)：136-140.
YANG Kang，YUAN Haidong，GUO Yuanbo. Two-dimensional code hierarchical encryption algorithm based on attribute encryption[J]. Computer Engineering，2018，44(6)：136-140.

[15] XUN Yijing，LI Zhijiang，ZHONG Xiaolu，et al. Dual anti-counterfeiting of QR code based on information encryption and digital watermarking[C]//Advances in Graphic Communication，Printing and Packaging，Singapore：Springer，2019：187-196.

[16] 杨宏宇，王在明．基于SHA-256和DNA序列的彩色二维码混沌加密方法[J]．大连理工大学学报，2017，57(6)：629-637.
YANG Hongyu，WANG Zaiming. Color two-dimensional code chaotic encryption method based on SHA-256 and DNA sequence[J]. Journal of Dalian University of Technology，2017，57(6)：629-637.

[17] CHEREMKHIN P A，KRASNOV V V，RODIN V G，et al. QR code optical encryption using spatially incoherent illumination [J]. Laser Physics Letters，2017，14：026202.

[18] 印曦，黄伟庆．基于混沌理论的彩色QR编码水印技术研究[J]．通信学报，2018，39(7)：50-58.
YIN Xi，HUANG Weiqing. Research on color QR code watermarking technology based on chaos theory[J]. Journal on Communications，2018，39(7)：50-58.

[19] GUANG Yu，SHI Yunbo，CHE Chang. A kind of encryption method of QR code based on ECA state ring[J]. International Journal of Security and Its Applications，2015，9(9)：285-294.

收稿日期：2023-04-24
修改稿日期：2023-06-25