DOI:10.11721/cqnuj20170319

# 基于非对称密码体制的二维码加密算法*

龙　强[1]，刘小华[2]

(1. 西南科技大学 理学院，四川 绵阳 621010；2. 深圳大学 计算机与软件学院，广东 深圳 518060)

**摘要**:【目的】遵循现有的二维码编码标准，提出了一种基于非对称密码体制的二维码加密算法，使得二维码中的信息能够在不安全的信道中安全地传输。【方法】考虑到二维码的特点，在二维码编码阶段对生成的 0-1 信息明文进行加密。运用 Logistic 混沌模型对 0-1 信息明文进行置换加密，同时对 Logistic 混沌模型的参数明文运用 RSA 加密算法进行加密，然后将加密得到的信息密文和参数密文一同编入二维码图像中进行传输。【结果】实现了二维码非对称加密，整个加密算法命名为 R-L 加密算法。【结论】实例结果表明，R-L 加密算法操作简单易行，算法复杂性不高，安全性能可靠。

**关键词**:RSA 加密算法；Logistic 混沌模型；非对称加密体制；二维码

**中图分类号**:O157.4；TN918.2　　**文献标志码**:A　　**文章编号**:1672-6693(2017)03-0091-05

二维码，又称二维条码，英文名为 2-dimensional bar code 或 QR Code，是一种新型的数据储存和传递技术。它按一定的标准在特定的平面区域内排列黑白相间的图形以储存数据，并通过发送图片将数据传递给接收者。

随着移动互联网技术的快速发展和各类社交网络技术的流行，尤其是智能手机等个人数字设备的普及，二维码作为一种能够储存和传递文字、音像等可数字化信息的全新技术，已经影响到日常生活的方方面面。但是，由于二维码的生成标准是公开的，且没有相应的加密标准，储存和传递的信息很容易被不法分子截获并利用，造成不必要的财产损失。据《2015 年上半年手机安全报告》显示[1]，2015 年上半年新增 Android 病毒包数达到 596.7 万个，同比增长 1 741%，这些手机病毒有 60%以上都是通过二维码传播的。同时，层出不穷的手机诈骗和恶意软件也大都以二维码作为伪装进行[2]。因此，有关二维码安全性的相关理论研究和技术开发成为当今移动互联网领域的一个重要课题。本文在现有的二维码编码标准基础之上，提出了一种基于非对称密码体制的二维码加密算法，使得二维码中的信息能够在不安全的信道中安全地传输。

目前，国内对二维码加密的研究已经取得了一些初步成果。2011 年张定会等人[3]根据 QR 码结构特点，使用 DES 加密算法实现了直接对 QR 二维码图像进行加密和解密。2012 年任勇金[4]提出了一种基于 AES 加密算法和异或计算的二重加密机制。该机制首先利用 AES 加密算法对信息明文进行加密，并绘制出信息密文的二维码 QR1，再根据 QR1 的版本、格式和纠错等级情况，绘制出含有密钥信息的二维码图形 QR2，然后将两个二维码图形 QR1 和 QR2 进行异或运算，最终得到双重加密后的二维码图形。2013 年，高彦受[5]提出使用密钥长度可变的流加密算法 RC4 对二维码进行加密。2013 年，杨海洲等人[6]将与 QR 二维码有相同矩阵形式的 Ising 模型运用到二维码加密中，制定了基于 Ising 模型的二维码加密体制。同年，腾旭[7]将伪指纹特征密钥与二维码结合，提出基于伪指纹特征密钥的二维码加密技术。2014 年，安吉旺等人[8]提出了一种结合 RSA 和 key 口令的改进算法对编码数据信息加密。先对明文信息用 key 口令分组加密，再用 RSA 对 key 密钥加密。同年，于英政等人[9]将 DES 加密算法和 RC4 加密算法结合，制定了一种二维分阶段加密体制。2015 年叶志琼等人[10]对二维码可能的加密位置进行了总结分析。

综上所述，目前对二维码的加密研究主要分为两类：一是直接对二维码要传输的原始数据进行加密，二是对生成的二维码图形加密。但这些方法还存在以下问题：1) 单纯运用 DES，RSA，RC4 的加密算法，加密过程繁琐，对明文直接加密复杂度高，而且密钥的传递得不到有效保障；2) 对生成的二维码图像进行加密的算法加密解密过程计算量大，安全程度相对较低，并且与二维码生成过程结合并不紧密，难以嵌入到二维码生成器中。

本文基于非对称加密体制，将加密算法与二维码的生成过程紧密结合，实现在二维码生成过程中对信息明文进行加密。

* **收稿日期**:2016-06-17　**修回日期**:2017-03-13　**网络出版时间**:2017-05-02 17:24

**资助项目**:国家自然科学青年科学基金(No.11501474)

**第一作者简介**:龙强，男，博士，研究方向为算法设计与分析，最优化理论与算法，E-mail:longqiang@swust.edu.cn

**网络出版地址**:http://kns.cnki.net/kcms/detail/50.1165.N.20170502.1724.012.html

# 1 算法理论基础

R-L算法的核心思想是将RSA加密算法和Logistic混沌映射结合并嵌入到二维码的编码过程中。因此,下面分别简单介绍二维码的编码规则、RSA加密算法以及Logistic混沌映射。

## 1.1 二维码的编码过程[13]

二维码是用某种特定的几何图形按一定规律在平面分布的黑白相间的图形记录数据符号信息的,在代码编制上巧妙地利用构成计算机内部逻辑基础的"0"、"1"比特流的概念,使用若干个与二进制相对应的几何形体来表示文字数值信息,通过图象输入设备或光电扫描设备自动识读以实现信息自动处理。二维码的编码过程分为数据分析、数据编码、纠错编码、布置模块、格式版本信息和掩模等步骤,其流程见图1所示。

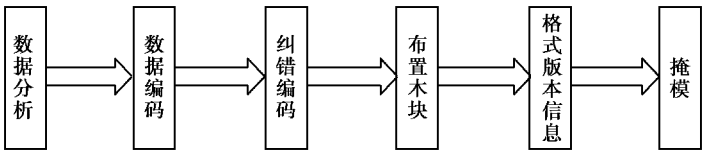



图1　QR二维码编码过程

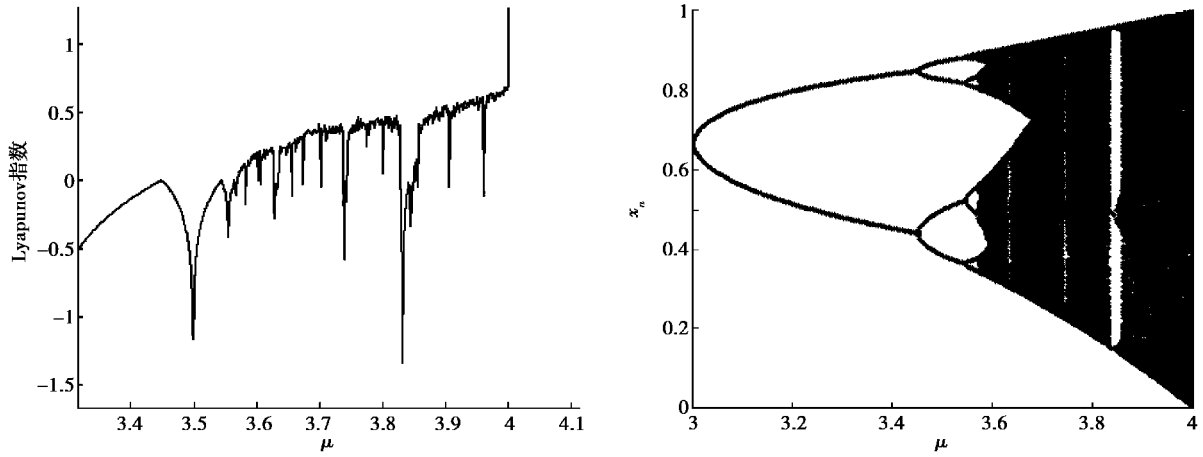
Fig. 1　The process of QR coding

## 1.2 Logistic 映射[11-12,14-15]

Logistic映射是研究动力系统、混沌、分形等复杂系统行为的一个经典模型。Logistic映射是一个时间离散的动力系统,其迭代方程为:

$$x_{k+1}=\mu x_k(1-x_k), \qquad (1)$$

其中,$x_n\in(0,1)$,$\mu\in[3.569\ 945\ 6,4]$。当参数$\mu\in[3.569\ 945\ 6,4]$时,Logistic映射进入混沌状态,并且表现出复杂的动力学特性(图2)。




a　不同$\mu$值下的Lyapnov指数　　b　Logistic映射倍周期分叉特点

图2　Logistic函数的动力学特征

Fig. 2　Dynamic characteristics of Logistic function

## 1.3 RSA 加密算法

RSA加密算法是一种非对称加密算法,其具体加密流程如图3所示。其中,$x$,$y$分别对应于明文和密文,$c$,$n$是公钥,而$d$,$n$是密钥。RSA加密算法的具体步骤如下[14]。

步骤1,不同素数$p$和$q$,注意$p$和$q$需要妥善保管;

步骤2,计算被加密明文二进制下最长位数$L=\log_2 n$,其中$n=p\cdot q$,$n$公开;

步骤3,计算欧拉函数$\varphi(n)=(p-1)\cdot(q-1)$中$\varphi(n)$保密,$p$,$q$秘密销毁;

步骤4,任意选取正整数$e$(公开),使得$\gcd(e,\varphi(n))=1$($e$与$\varphi(n)$互质),且$0<e<\varphi(n)$;

步骤5,求私钥$d$,使得$d\cdot e\equiv 1(\mathrm{mod}(\varphi(n)))$,即$d\cdot e=k\varphi(n)+1(k\in\mathbf{Z})$;

步骤6,公钥$K_u=(e,n)$,私钥$K_r=(d,n)$。

# 2 R-L 加密算法

R-L加密算法是将RSA加密算法和Logistic混沌映射模型相结合并嵌入到二维码编码过程中的一种加密算法。R-L加密算法主要分为3个部分,第一部分是运用Logistic混沌映射实现对0-1信息明文进行位置置换加密。在第二部分中,为了隐藏Logistic混沌映射的参数,运用RSA加密算法对Logistic混沌映射的参数明文进行加密。第三部分将信息密文和参数密文共同编入二维码图形,从而生成加密的二维码。

R-L 算法加密流程见图 4 所示，其中 Alice 是二维码的生成和发送方，Bob 是二维码的接收方。为方便叙述，设 0-1 信息明文为 $M$，Logistic 混沌映射的参数分别为 $x_0$，$\mu_0$。

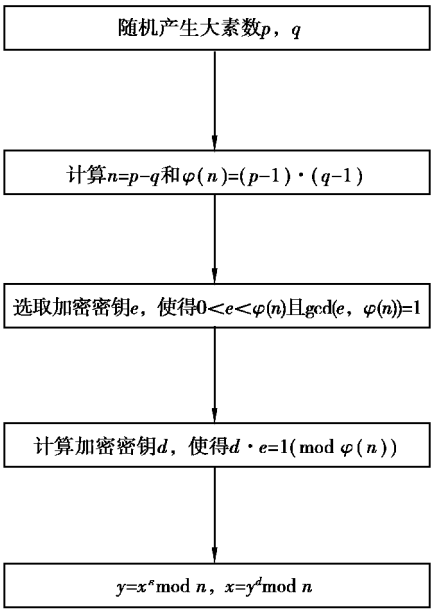



图 3　RSA 加密流程

Fig. 3　The process of RSA algorithm

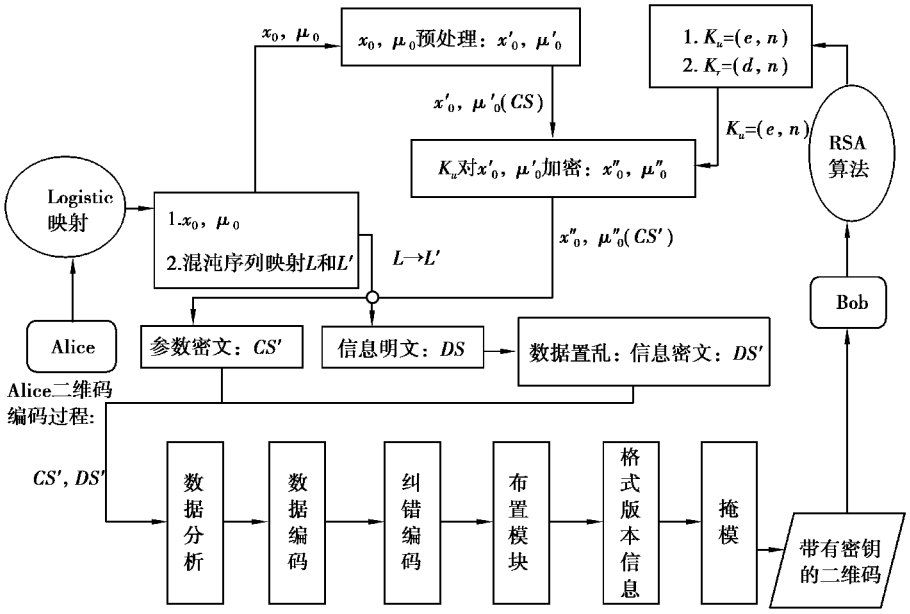



图 4　R-L 算法加密流程图

Fig. 4　The process of R-L algorithm

第一部分：运用 Logistic 混沌映射加密信息明文。

步骤 1，Alice 选取 Logistic 映射的初始参数($x_0$，$\mu_0$)；

步骤 2，Alice 利用初始参数以及 Logistic 混沌模型生成原始混沌序列 $L$；

步骤 3，Alice 对原始混沌序列进行从小到大的排序得到排序后的序列 $L'$；

步骤 4，Alice 将信息明文 $M$ 按照编码规则转换成 0-1 序列 $DS$。并利用 $L\rightarrow L'$ 的映射关系对 $DS$ 进行位置置乱，得到信息密文 $DS'$。

第二部分：运用 RSA 算法加密 Logistic 混沌映射参数。

步骤 1，Bob 利用 RSA 算法生成公钥 $K_u=(e,n)$ 与私钥 $K_r=(d,n)$，将公钥发送给 Alice，私钥自己秘密保存；

步骤 2，Alice 对初始参数($x_0$，$\mu_0$)进行预处理，即将小数扩大倍数成为整数，得到($x'_0$，$\mu'_0$)；

步骤 3，Alice 利用接收到的公钥 $K_u=(e,n)$ 以及 RSA 加密算法对 $x'_0$，$\mu'_0$(CS)加密，得到参数密文($x''_0$，$\mu''_0$)；

步骤 4，Alice 将参数密文($x''_0$，$\mu''_0$)转化为二进制编码 $CS'$。

第三部分：生成加密二维码。

Alice 将参数密文 $CS'$ 和信息密文 $DS'$ 拼接在一起并进行二维码编码的后续操作，即数据分析、数据编码、纠错编码、布置模块、生成格式版本信息和掩模，最终生成加密的二维码图片。发送给 Bob。

## 3 R-L 加密算法实例

为更清晰地表达 R-L 加密算法的操作流程，以 Alice 作为二维码生成以及发送方，以 Bob 为二维码接收方为例，在线秘密传输一串数字即信息明文 $M$：972190，其过程如下。

第一部分：运用 Logistic 混沌映射加密信息明文。

步骤 1，Alice 选取 Logistic 映射的初始参数($x_0$，$\mu_0$)=(0.933 98，4.000 0)，并生成原始混沌序列 $L$，然后对原始混沌序列进行从小到大的排序得到排序后的序列 $L'$。$L$ 和 $L'$ 的对应关系如(2)式：

$$L=\begin{bmatrix}1&2&3&4\\5&6&7&8\\9&10&11&12\\13&14&15&16\\17&18&19&20\end{bmatrix}\rightarrow\begin{bmatrix}17&2&9&13\\15&20&7&11\\18&5&3&4\\10&6&19&14\\12&8&1&16\end{bmatrix}=L'。\tag{2}$$

步骤2,将信息明文 $M$ 按照编码规则转换成0-1序列 $DS$,过程如下。

1) 将数字分为3个一组,并转化为二进制:972→1111001100,190→0010111110;2) 将各组二进制编码拼接起来:972 190→11110011000010111110;3) 在二进制编码前加上符号计数指示符20→00010100和模式指示符:0001。最后得到信息明文为 $DS$:0001 00010100 11110011000010111110;

步骤3,利用 $L\rightarrow L'$(如(2)式)的映射对信息明文的0-1序列 $DS$ 进行位置置乱,得到信息密文 $DS'$:00101010100011101100101011110,其对应于十进制数为:874 807。

第二部分:运用RSA算法加密Logistic混沌映射参数。

步骤1,Bob利用RSA算法生成公钥 $K_u=(e,n)=(11,41\ 217)$ 与私钥 $K_r=(d,n)=(3\ 747,41\ 217)$,并将公钥发送给Alice,私钥自己秘密保存;

步骤2,Alice对初始参数 $x_0,\mu_0$ 进行预处理,得到 $(x_0',\mu_0')=(93\ 398,40\ 000)$;

步骤3,Alice利用接收到的公钥 $K_u=(e,n)$ 以及RSA加密算法对 $(x_0',\mu_0')$ 进行加密,得到参数密文 $(x_0'',\mu_0'')=(7\ 671,21\ 666)$;

步骤4,数据分析与编码:对参数密文 $(x_0'',\mu_0'')$ 分析并编码:1) 每3个数字一组:767 1,216 66;2) 每3个数字分为一组,并将每组数据转化为二进制表示:767→1011111111,1→0001,216→0011011000,66→1000010;3) 将两个数字的二进制表示分别拼接起来:7671→10111111110001,21666→00110110001000010;4) 在两个二进制表示前分别加上符号计数指示符:14→00001110,17→00010001。从而得到参数密文的二进制编码为:

$CS$:00001110 10111111110001 00010001 00110110001000010。

第三部分:生成加密二维码。

Alice对上面得到的 $CS'$,$DS'$ 进行拼接并进行编码的后续步骤,纠错编码、生成版本格式信息、布置模块和掩模,从而得到携带密钥的二维码图片(图5)。

若用手机扫描图5,会得到字符串767121666874807。其中767121666代表的是参数密文,可以用Bob保留的秘钥进行解密得到参数明文;874807代表的是信息密文,可以根据Logistic混沌映射,借助于已经得到的参数明文还原信息密文,从而达到解密的目的。

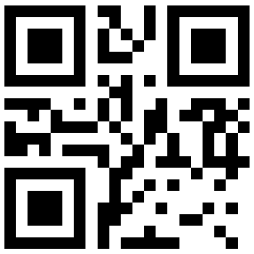


**图5 携带密钥的二维码图片**

Fig. 5 QR code with private key

## 4 结论

R-L加密算法避免了运用RSA加密算法对全部信息明文加密,只需要对Logistic混沌映射的初始参数加密,使得整个算法更加简明、快捷,空间占用率更低。R-L加密算法中用到的Logistic混沌映射对初始条件的敏感性,使得想要尝试使用穷举法攻击成为不可能。将Logistic混沌映射所用到的初始参数运用RSA加密算法加密后放置在二维码中和信息密文一起传送给二维码接收方,相对于直接通过信道发送更方便和安全,同时也实现了非对称加密体制。

未来将从如下两个方面对R-L加密算法做进一步研究:1) 改进已有的二维码生成器和解码器,将R-L加密算法嵌入到其内部程序中,实现带R-L加密算法的二维码在个人电脑端的生成和在手机客户端的读取;2) 在已有算法中加入签名算法,以防止伪装发送方发送信息的情况,例如ElGamal签名方案。

**参考文献:**

[1] 王勇,廖志孟,夏聪颖.智能手机的信息安全问题探讨[J].科技广场,2015(11):50-60.
WANG Y,LIAO M Z,XIA C Y.Discussion on information security of smartphone[J].Science Mosaic,2015(11):50-60.

[2] 张新生.二维码[EB/OL].(2015-11-29)[2016-04-19].http://baike.baidu.com/link?url=YGwlvVCo2TK1IArNnAgiZo0TX6dnm49RZhP6VWKP60BkMbGHScsciz0BLVwgAH5N67T5vQ7jwFVguec3bRa91a.
ZHANG X S.Two demensional code[EB/OL].(2015-11-29)[2016-04-19].http://baike.baidu.com/link?url=YGwlvVCo2TK1IArNnAgiZo0TX6dnm49RZhP6VWKP60BkMbGHScsciz0BLVwgAH5N67T5vQ7jwFVguec3bRa91a.

[3] 张定会,单俊涛,江平,等.QR码DES加密与解密[J].数据通信,2011(3):40-42.
ZHANG D H,CHAN J T,JIANG P,et al.Encryption and decryption of QR codes using DES[J].Data Communications,2011(3):40-42.

[4] 任勇金.基于Rijndae和异或运算的QR二维码双重加密研究[J].华章,2012(29):338-338.
REN Y J.Study on QR two-dimensional code double encryption and XOR operation based on Rijndae[J].Magnificent Writing,2012(29):338-338.

[5] 高彦受.QR 二维码的安全实现与设计分析[D].南京:南京理工大学,2013.
GAO Y S.Safety implementation and design analysis of QR two-dimensional code[D]. Nanjing: Nanjing University of Science and Technology,2013.

[6] 杨海洲,高子坤,王江涛.Ising 模型在 QR 码加密中的优化分析[J].电子技术与软件工程,2014(4):34-34.
YANG H Z,GAO Z K,WANG J T.Optimization analysis of Ising model in OR code encryption[J].Electronic Technology & Software Engineering,2014(4):34-34.

[7] 滕旭.基于伪指纹特征密钥的二维码加密算法研究[J].软件导刊,2013(8):135-137.
TENG X.Research of encryption algorithm of two-dimensional code based on pseudo fingerprint feature[J].Software Guide,2013(8):135-137.

[8] 安吉旺,徐凯宏.基于 RSA 和密钥的二维码加密编码的研究[J].森林工程,2014,30(2):125-129.
AN J W,XU K H.Design of encryption coding of two-dimensional code based on RSA and key[J].Forest Engineering,2014,30(2):125-129.

[9] 于英政,许宏丽.基于 QR 二维码的多级融合加密算法的设计与实现[J].计算机与数字工程,2014,42(12):2362-2364.
YU Y Z,XU H L.Design and development of multilevel fusion encryption algorithm based on QR two-dimensional code[J]. Computer & Digital Engineering,2014,42(12):2362-2364.

[10] 叶志琼,郑维清,郑健,等.疫苗 QR 二维码加密防伪技术[J].齐齐哈尔大学学报(自然科学版),2015(4):41-44.
YE Z Q,ZHENG W Q,ZHENG J,et al.Vaccine of QR code encryption security technology[J].Journal of Qiqihaer University(Natural Science),2015(4):41-44.

[11] 何松柏,周尚波.一类混沌映射扩频序列的研究[J].电子与信息学报,2004(2):23-48.
HE S B,ZHOU S B.Research on spreading sequences with chaotic maps[J].Journal of Electronics & Information Technology,2004(2):23-48.

[12] 张红,周尚波.混沌理论在密码学中的应用[J].重庆大学学报(自然科学版),2004(4):22-30.
ZHANG H,ZHOU S B.Application of chaos theory in cryptography[J].Journal of Chongqing University(Natural Science),2004(4):22-30.

[13] 冯登国.密码学原理与实践[M].北京:电子工业出版社,2009.
FENG D G.Cryptography theory and practice[M]. Beijing: Publishing House of Electronics Industry,2009.

[14] 向宇.一种改进的基于 Arnold 映射的 Hash 加密算法[J].重庆师范大学学报(自然科学版),2013,30(4):103-108.
XIANG Y.Improved Hash encryption algorithm based on Arnold mapping[J].Journal of Chongqing Normal University(Natural Science),2013,30(4):103-108.

[15] 张欣,杨德刚,朱凯.一种基于外部密钥的混沌加密方法[J].重庆师范大学学报(自然科学版),2010,27(2):57-60.
ZHANG X,YANG D G,ZHU K.A new chaotic cryptosystem by using external key[J]. Journal of Chongqing Normal University(Natural Science),2010,27(2):57-60.

## Two Dimensional Code Encryption Algorithm Based on Asymmetric Cryptosystem

LONG Qiang[1], LIU Xiaohua[2]

(1. School of Science, Southwest University of Science and Technology, Mianyang Sichuan 621010;
2. School of Computer and Software, Shenzhen University, Shenzhen Guangdong 518060, China)

**Abstract**: [**Purposes**]Based on the existing two-dimensional codes standard, it provides a two-dimensional code encryption algorithm based on the asymmetric cryptography, which makes the information containing in two-dimensional codes can be transferred in insecure channel. [**Methods**]Given the characteristics of two-dimensional codes, the proposed method encrypts the 0-1 informational plaintext in the process of coding. Firstly, one use Logistic chaotic model to encrypt the 0-1 informational plaintext; and at the same time, use RSA Public Key Cryptography to encrypt the parametric plaintext of the Logistic chaotic model; then code and transfer the informational and parametric cryptographs together in two-dimensional codes, which in return, realizes the asymmetric two-dimensional codes cryptography. [**Findings**]This algorithm is named as R-L Encryption Algorithm in this paper. [**Conclusions**]Experiments show that the R-L Encryption Algorithm is easy to process, with inexpensive computing cost and promising security.

**Keywords**: RSA encryption algorithm; Logistic chaotic model; asymmetric cryptography; two-dimensional code

(责任编辑 黄 颖)