基于 SHA512 哈希函数和 Rijndael 加密算法 QR 二维码信息安全设计①

肖本海, 郑莹娜, 龙建明, 郭盼盼

(广东工业大学 信息工程学院, 广州 510006)

摘 要: 随着二维码技术广泛应用于电子票务、银行支票、电子保单等多个领域, 二维码的信息泄露和信息篡改等安全问题日益突出. 为提高二维码内部信息的安全性能, 从对二维码内部信息加密和二维码信息防篡改俩个角度来提高. 基于 Visual Studio 2008 C#平台, 设计了一种采用 SHA512 哈希函数和 Rijndael 加密算法混合加密的方法, 该方法利用 Rijndael 加密和 SHA512 数字签名等技术, 对 Rijndael 第一次加密密钥系统随机分配, 并对系统随机分配密钥采用二次 Rijndael 加密防护方法, 并通过 SHA512 对二维码内部信息防篡改校验, 达到对二维码信息及其加密密钥的安全保护. 在生成 QR 二维码之前实现了信息加密, 并从系统构架、算法原理和实现及安全性能等多个方面进行了测试和分析. 分析表明此方法提高了二维码信息的安全性能, 达到对密钥高效管理和对信息的多重保护, 而在加密后密文信息容量较明文信息有所增加.

关键词: 信息加密; Rijndael 算法; SHA512 算法; 二维码; 信息安全

QR Code Design of Information Security Based on Rijndael Encryption Algorithm and SHA512 Encryption Algorithm

XIAO Ben-Hai, ZHENG Ying-Na, LONG Jian-Ming, GUO Pan-Pan

(Guangdong University of Technology, Guangzhou 510006, China)

Abstract: With the QR code technology being widely applied in electronic ticketing, bank checks, E-commerce and other fields, many safety problems have emerged, such as information leakage and data tampering. Based on Visual Studio 2008 c platform, the method with Rijndael random variable and random keys secondary Rijndael encryption protection is proposed using Rijndael encryption and SHA512 digital signature technology. This paper presents a novel design of information security before generating QR code. The encryption principle, algorithm and implementation, safety performance of the proposed method are discussed. Also corresponding testing and analysis are provided to verify the feasibility of the proposed algorithm. Results have proved that the information safety performance of QR code is greatly increased with the encryption algorithm, the efficient management and the multiple- protection to a key. This just causes a smaller increase in the content of the encryption data than those of the raw data.

Key words: information encryptio; Rijndael algorithm; SHA512 algorithm; QR code; information security

随着互联网技术的发展, 二维码在我们日常生活中随处可见, 主要应用于物流、交通、金融、制造业、电子商务、传媒、通讯、旅游、广告等领域. 二维码技术凭借其存储容量大, 信息集成度高, 识别性能好以及能表示字母、符号、汉字和图像等多种信息等优势, 逐渐取代一维码技术, 在商品标签、信息存储、信息传输、信息交换数字验证等方面得到广泛的应用. 因此, 如何保证二维码信息的安全成为其应用中亟待解决的课题. 本文采用二维码信息分组加密技术, 利用 Rijndael 和 SHA512 加密算法相结合, 由 Rijndael

① 收稿时间:2014-11-06;收到修改稿时间:2014-12-22

二次加密保护和 SHA512 身份效验码生成二维码等方法组成一种新的加密方法. 测试分析表明, 该算法进一步提高了 QR 二维码的信息安全性和可靠性.

1　加密算法基本原理

1.1 Rijndael 算法原理

Rijndael 加密算法实质上是 Square 加密算法的变形, 加密算法的分组长度和密钥长度可变, 可以分别指定为 128 位, 192 位和 256 位[1]. Rijndael 算法主要由 S_box 变换替换, 行移位变换, 列混合和轮密钥加等四种运算组成[2]. S-box 变换主要作用是非线性混淆, 行移位变换和列混合变换主要增加算法的扩散程度[1,2], Rijndael 加密算法的主要流程如图 1 所示.

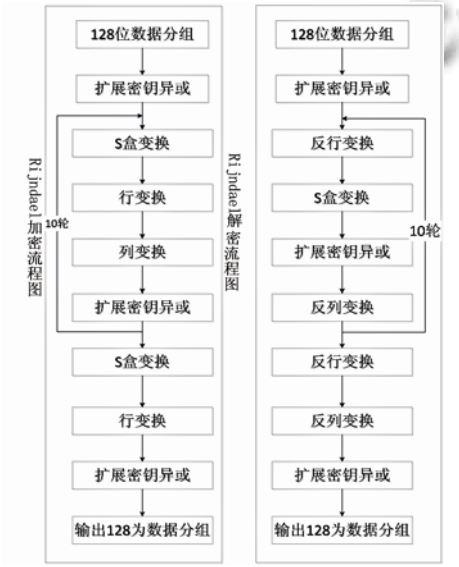

图 1　Rijndael 加密解密算法流程[1]

1.2 SHA512 算法原理

SHA512 是 SHA-2 中安全性能较高的算法, 主要由明文填充、压缩函数变换、消息扩展函数变换和随机数变换等部分组成, 初始值和中间运算结果由 8 个 64 位移位寄存器组成[3,4]. SHA512 输入长度任意位 x, (x 不大于 2128 位), 输出为 512 位哈希算法(Hash), 主要应用于数字签名领域, 相当于信息的“身份证”, 主要用于防止信息在传输过程被篡改和检测信息的完整性. SHA512 加密算法首先进行预处理(明文信息分成 1024 位一组的数据块、消息扩展变换和附加长度值), 然后计算散列值迭代所需要的 Wt, 最后进行散列值计算得到散列值[3,4]. SHA512 内部数据流向如图 2 所示.

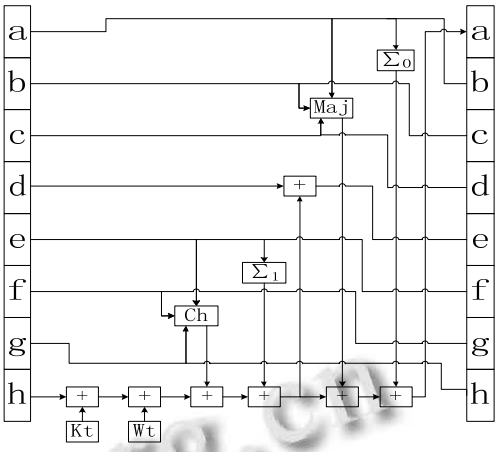

图 2　SHA512 数据流向图[3]

图 2 中, a、b、c、d、e、f、g 和 h 为 8 个 64 位中间结果寄存器[3], 用于存放中间结果和最终散列值; K_t 为定义好的 80 个 64 位迭代常数, W_t 为运算算子, 运算如式(1)和(2)所示, 其中 M_t 为明文信息分组成的 1024 位的数据块. K_t 和 M_t 为常数, 根据(NSA)标准确定. Ch 算子运算函数如式(3)所示, Maj 算子如运算式(4)所示, Σ_0 和 Σ_1 分别如式(5)和(6)所示.

$$W_t = M_t; 0 \le t \le 15 \tag{1}$$

$$W_t = \sigma_1(W_{t-2}) + W_{t-7} + \sigma_0(W_{t-15}) + W_{t-16}; 16 \le t \le 79 \tag{2}$$

$$Ch(x,y,z) = (x \wedge y) \oplus (\neg x \wedge z) \tag{3}$$

$$Maj(x,y,z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z) \tag{4}$$

$$\Sigma_0(x) = ROTR^{28}(x) \oplus ROTR^{61}(x) \oplus ROTR^{39}(x) \tag{5}$$

$$\Sigma_1(x) = ROTR^{14}(x) \oplus ROTR^{18}(x) \oplus ROTR^{41}(x) \tag{6}$$

$$ROTR^n(x) = (x >> n) \vee (x << w - n) \tag{7}$$

式中 $ROTR^n(x)$为 n 位循环右移操作.

2　基于Rijndael和SHA512算法混合加密QR二维码安全设计与实现

二维码应用于电子保单, 某保险公司的需求分析如下: (1)二维码存储的信息分为两个部分, 一部分为明文信息, 客户可以通过二维码查阅的基本信息; 另一部分为密文信息, 客户不可以见, 而保险公司管理层根据权限及密码登陆公司网站才能获取; (2)保证二维码中的密文信息不被泄露; 保证二维码中的信息不被篡改, 当发生篡改之后能及时检测.

为满足上述要求, 本文采用属于对称加密算法的 Rijndael 算法作为主要加密方法, 用随机密钥对密文信息加密, 并对随机密钥进行二次 Rijndael 加密, 加强对随机密钥的保护; 又采用散列加密算法 SHA512 对

二维码中的密文和明文信息进行加密生成校验码; 最后将一次、二次 Rijndael 加密的密文 1 和密文 2、明文信息以及 SHA512 的校验码集成生成二维码, 这种组合加密对密文信息进行了双重保护, 且对随机密钥也实施保护, 从而提高了二维码信息的安全性能.

本算法考虑首先对信息分块、加密, 再生成二维码, 主要强调对密文信息的二次加密和对随机密钥的保护. 采用随机密钥发生器 Rand()类函数随机生成 128 位随机密钥 1, 对需要加密的密文信息进行一次 Rijndael 加密, 形成密文 1; 对随机密钥 1, 结合系统密钥 2 加密之后形成密文 2; 对密文信息和明文信息再进行 SHA512 加密, 生成唯一的 SHA512 校验码 1; 集成密文 1、密文 2、SHA512 校验码 1 及明文信息生成二维码. 当系统读取二维码信息时, 首先提取二维码中保存随机密钥 1 的密文 2, 通过系统密钥 2 对密文 2 进行解密恢复随机密钥 1, 再通过随机密钥 1 对密文 1 进行解密恢复密文信息. 其中明文信息可以直接通过手机二维码扫描器或者微信扫一扫等二维码阅读器直接读出, 但密文信息必须经过本系统的二次解密才能恢复. (二次加密: 密文 1; SHA512 校验码 1)基于 Rijndael 和 SHA512 混合加密算法的 QR 二维码安全设计流程如图 4 所示.

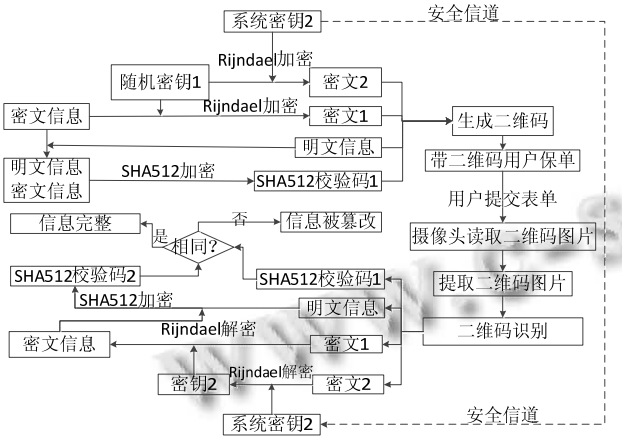

图 4 基于 Rijndael 和 SHA512 混合加密算法的 QR 二维码安全设计流程图

本系统设计实现基于 visual 2008.net 平台, 编程语言为 C#, QR 二维码生成和识别采用 ThoughtWorks 公司设计的标准二维码生成动态链接库 ThoughtWorks.QRCode.dll, Rijndael 加密算法和 SHA512 加密算法采用 visual C# 命名空间 System.Security.Cryptography 下安全类实现, 其内部继承图表如图 5 所示. 密文 1、密文 2、SHA512 校验码 1 及公开信息之间采用标示符分隔开, 二维码内部存储数据结构如图 6 所示.

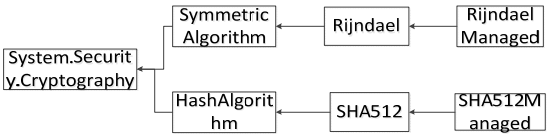

图 5 基于 Rijndael 和 SHA512 算法的内部继承图

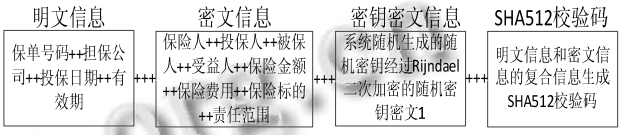

图 6 二维码内部数据存储结构示意图

明文信息、密文信息、随机密钥密文信息和 SHA512 校验码之间采用“+++”分隔符, 明文信息和密文信息内部字段之间均采用“++”作为分隔符.

系统关键代码如表 1 所示.

表 1 基于 C#系统调用关键代码

Rijndael 实现关键代码	Rijndael m_RijndaelProvider = Rijndael.Create();// 创建 Rijndael 实例化对象
	CryptoStream m_csstream =new CryptoStream (m_stream, m_RijndaelProvider.CreateEncryptor (Encoding.Default.GetBytes(EncryptKey), m_btIV), CryptoStreamMode.Write);//创建底层数据流, EncryptKey为加密密钥, m_btIV为初始化向量
	m_csstream.Write(m_btEncryptString, 0, m_btEncryptString.Length);//写入内存流.

SHA512 实现关键代码	SHA512 sha512 = SHA512.Create(); // 创建 SHA512 算法对象
	result1 = sha512.ComputeHash(data); // 调用 SHA512Hash 函数计算 Hash 值

二维码生成识别关键代码	using ThoughtWorks.QRCode; //添加 ThoughtWorks 公司 QR 二维码生成和识别动态链接库
	QRCodeEncoder qrCodeEncoder = new QRCodeEncoder();//创建二维码生成识别实例化对象
	Image image = qrCodeEncoder.Encode(data, Encoding.UTF8);// 创建 image 图像对象, Encoding.UTF8 采用 UTF8 编码格式, data 为 QR 二维码的内部信息
	QRCodeDecoder Decoder = new QRCodeDecoder(); //实现解码 decoder 实例
	String DecoderString=decoder.decode(image); //解码函数 decode(), 输入为 image 图片, 输出为字符串.

基于 Rijndael 和 SHA512 混合加密的 QR 二维码生成和识别算法实现界面如图 7 所示.

图 7　基于 Rijndael 和 SHA512 混合加密的 QR 二维码生成算法实现界面

图 7 所示“经过信息加密后生成的二维码”(上图)中包含了明文信息、以随机密钥 1 加密的密文 1、以系统密钥 2 加密的密文 2 以及 SHA512 校验码, 是执行基于 Rijndael 和 SHA512 混合加密的 QR 二维码生成算法的结果和界面. 其与仅包含信息而没有经过信息加密的二维码(下图)相比是完全不同的.

3　性能测试和分析

3.1 Rijndael 安全性能分析

Rijndael 是对称加密算法中较优秀的加密算法, 其安全性能高, 抗攻击能力强; Rijndael 抗差分攻击能力, 最佳差分特性概率为 2-151, 最差线性逼近偏差为 2-71, 八轮最差差分特征为 2-300, 最差线性逼近偏差为 2-151, 对于 10 轮, 12 轮, 差分特征和最差线性偏差更小[6]; Rijndael 抗纯密钥攻击能力, 对于 128 位密钥破解需要 2128 次, 256 位密钥则要 2256[6]. 假设一台计算机 1 秒钟内能用蛮力攻击破解密钥长度为 56 位的 DES 算法的加密密钥, 那么同样用这台计算机去破解密钥长度为 128 位的 Rijndael 算法的加密密钥, 则需要 1497 亿年 (2128-56/(60*60*24*365)), 由此可见 Rijndael 加密算法的安全性能较高.

3.2 SHA512 安全性能分析

SHA512 是散列算法中较优秀的算法, 散列算法中散列值计算具有不可逆性, 对散列算法攻击最常用的方法是穷举法, 对每次散列值和对应的验证码一一存储起来, 通过验证码对应得出源文件; 由于 SHA512 的散列值具有 512 位, 利用穷举法攻击, 存储的数据量多达 2512 组数据, 根据目前的数据库存储功能和硬件的制约是根本无法实现的.

3.2 二维码安全设计结构性能测试分析

本文基于高可靠性安全设计构架, 采用随机密钥加密、随机密钥 Rijndael 二次密钥保护、和基于复合信息的 SHA512 校验, 以及密钥密文和校验码信息共存于二维码等多项加密技术, 对二维码内部信息提供多重保护, 以进一步提高其安全性能.

为验证此二维码安全设计结构的可靠运行及其安全性能, 本文做了如下四个测试.

测试(1). 对图 8 所示的明文信息和密文信息按照图 4 所示的基于 Rijndael 和 SHA512 混合加密算法的流程进行加密和解密试验, 系统在脱离数据库的条件下能实现完整的信息加密和二维码生成以及二维码识别与解密. 基于 Rijndael 和 SHA512 混合加密算法的信息加密和二维码生成以及识别与解密流程执行结果如图 8 所示.

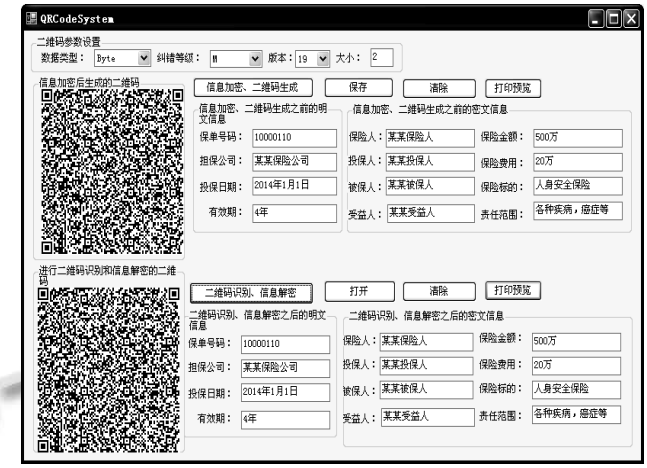

图 8　二维码加密生成和识别解密流程执行结果

由测试(1)和图 8 可见, 对信息分块中的明文信息和密文信息, 按照本文推荐的(如图 4 所示)基于 Rijndael 和 SHA512 混合加密算法的流程, 能够完成一次加密、二次加密、SHA512 校验以及二维码加密生成和二维码识别解密; 对于用上述方法已经生成的二维码经过解码识别和校验解密, 能够准确恢复出原始的明文和密文信息(如图 8 所示).

测试(2). 采用于图 8 所示相同的明文信息和密文信息每次生成二维码, 系统都会自动为此次加密分配一个随机密钥, 所以对相同的信息每次生成二维码其

内部的存储信息都不同, 由此验证随机密钥加密、随机密钥二次保护和密钥密文和校验码信息共存于二维码使得系统可以为其随机分配一个 16 字节的密钥, 此方法便于密钥管理而且安全性能提高, 具有较强的混淆作用. 随机密钥测试结果如图 9 所示.

由测试(2)和图 9 可见, 对相同的密文信息, 第一次加密、生成二维码所形成的的随机密钥 1、随机密钥 1 的密文 2 以及密文信息 Rijndael 加密密文 1 和第二次加密、生成二维码所形成的的随机密钥 1、随机密钥 1 的密文 2 以及密文信息 Rijndael 加密密文 1 是完全不同的. 因此, 此种算法的安全性能更高.

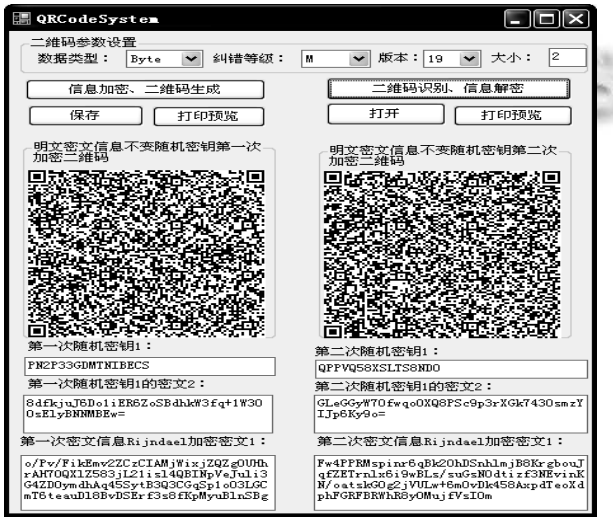

图 9 对相同密文信息二次加密生成二维码测试界面

测试(3). 对明文信息进行攻击篡改, 系统自动校验且检测出信息被篡改并警示, 以保证二维码内部信息的安全性和完整性. 本测试中将图 8 所示“明文信息”中的“担保公司”字段, 由原来“某某保险公司”进行恶意篡改为“某某机械公司”, 系统自动检测并返回检测和校验结果. 明文信息恶意篡改测试结果如图 10 所示. 可见, 明文信息遭到恶意篡改后, 即使二维码解码识别、解密之后, 也无法通过 SHA512 校验, 因为篡改前后的 SHA512 校验码是完全不同的, 因此系统警示“False”.

测试(4). 对密文信息进行篡改攻击, 系统自动校验且检测出信息被篡改并警示, 以保证二维码内部信息的安全性和完整性. 本测试中将“密文信息”中“投保人”字段, 由原来“某某投保人”恶意篡改为“某某责任人”, 系统自动检测并返回篡改和校验结果. 密文信息篡改测试界面如图 11 所示. 可见, 密文信息遭到恶意篡改后, 即使二维码解码识别、解密之后, 仍然无法通过 SHA512 校验, 因为篡改前后的 SHA512 校验码也是完全不同的, 系统因此警示“False”.

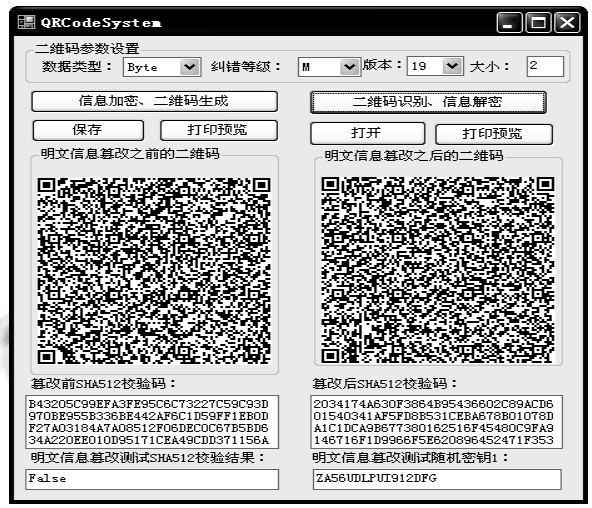

图 10 明文信息攻击篡改测试界面

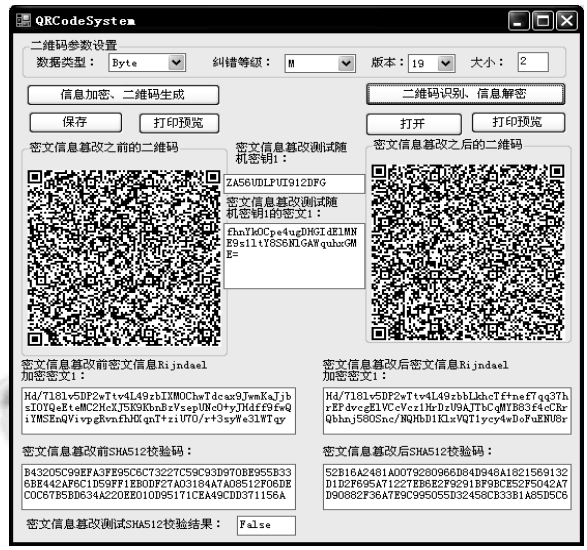

图 11 密文信息篡改测试效果图

上述测试表明, 随机密钥加密、Rijndael 加密算法二次加密和 SHA512 校验结合, 使得二维码的安全性能提高, 保证内部信息不被篡改; 采用随机密钥, 每次 Rijndael 加密的密钥都不同, 并对随机密钥 Rijndael 二次加密, 即使由于管理失误, 导致其中一个密钥被窃取, 也不会导致其他所有信息被破解; SHA512 校验算法主要用于保证信息的完整性, 一旦信息被人篡改, 基于篡改之后信息的 SHA512 校验码就会发生变化, 可以通过 SHA512 校验检测信息是否完整; 密钥密文

和校验码信息二维码内部存储, 使得系统在脱离数据库的条件下正常运行, 减轻了数据库的负担, 解决了由于随机密钥产生大量密钥难以管理的问题. 取得上述优点的前提是以牺牲一定的二维码内部存储空间为代价, 因为信息加密之后的密文信息、随机密钥密文信息和 SHA512 校验码信息在二维码中存储占用了一定量的空间, 对高版本号的二维码信息存储量相对来说较大, 所以此方案是切实可行的.

4 结论

本文采用 Rijndael 二次加密和 SHA512 校验结合的方法, 在生成QR二维码之前实现了信息加密, 并从系统构架、算法原理和实现及安全性能等多个方面进行了分析和测试. 结果表明此方法提高了信息的安全性能, 达到对密钥高效管理和对信息的多重保护, 并将随机密钥和系统密钥均存贮于二维码, 便于密钥管理. 但在加密后密文信息容量较明文信息有所增加.

本文设计算法的特点: 1)Rijndael 加密本身是一种高安全可靠的对称加密算法, 在此基础上引入随机密钥和随机密钥二次保护, 提高了其对密文的安全保护性能; 2)SHA512 是较可靠和较安全的散列加密算法, 将其引入对明文信息和密文信息进行校验, 保证了原始信息的完整性, 即信息的唯一性, 无法被篡改; 3)明文信息、密文信息、密钥密文和校验码信息共存于二维码中, 使得系统能为每一次二维码加密生成提供一个密钥, 无需考虑庞大的数据库来管理复杂的密钥, 加强了密钥的复杂性和安全性能. 此方案的缺点在于加密后密文信息容量较明文信息有所增加.

参考文献

1 弟宇鸣,陈荣桦,左广霞.基于 AES 算法的加密模块设计.电子设计工程,2013,21(2):53–55.
2 陈杰,胡予濮,张跃宇,董晓丽.相关密钥 Square 攻击 AES–92.电子科技大学学报,2013,(2):219–224.
3 李鸿强,苗长云,石博雅,仪鲁男.单向散列函数 SHA-512 的优化设计,2007,33(7):130–132.
4 武金梅.对缩短步数的 HASH 函数算法 SHA-256、SHA-512 的分析[学位论文].济南:山东大学,2008.
5 高彦受.QR 二维码的安全实现与设计分析[学位论文].南京:南京理工大学,2012.
6 张清华,马传龙,赵继德,魏德芳.Rijndael 算法及其性能分析.山东师范大学学报(自然科学版),2002,17(3):23–25.
7 姚峰,何成万,胡宏银.一种采用多种加密算法的文件加密方法.计算机应用与软件,2009,26(11):272–273,285.
8 王哲慧.数据库加密算法及其密钥技术研究[学位论文].长春:长春理工大学,2011.