文章编号：2095-2163(2020)08-0041-04 中图分类号：TP3;TN91 文献标志码：A

基于 AES 和混沌加密的红外测温图像混合加密系统的研究与设计

吴沐阳[1,2]，姚亚峰[2]，唐 义[3]
(1 国家电网湖南省怀化市分公司，湖南 怀化 418000;2 中国地质大学 机电学院，武汉 430074;3 中南大学 自动化学院，长沙 410013)

摘 要：在泛在电力物联网的迅速发展的时代，如何让物联网变得更安全可靠成为了当代信息安全领域的研究热门。本研究以网络信息安全问题为切入点，利用了 AES(Advanced Encryption Standard)算法混淆密码的功能，以及混沌加密算法在生成序列时的伪随机性，提出了一种将 AES 加密与混沌加密混合的新型加密算法。以电气红外图像为示例，通过 Matlab 完成了对示例图像的混合加密。为了验证混合加密算法的安全性，实验以相邻像素相关性和直方图为评估标准，数据表明混合加密算法比单方面的 AES 加密算法的安全性更高，其应用前景更加广阔。

关键词：AES 加密；混沌加密；安全性分析；图像相关性

The research and design of encryption of electric infrared image based on a mixture of AES and chaotic encryption theory

WU Muyang[1,2], YAO Yafeng[2], TANG Yi[3]
(1 HunanHuaihua Branch, State Grid, Huaihua 418000, Hunan, China; 2 School of Mechatronics, China University of Geosciences, Wuhan 430074, China; 3 School of Automation, Central South University, Changsha 410013, China)

【Abstract】 With the rapid development of ubiquitous power Internet of Things, it has become much more important to improve its reliability and security. Taking the network information security problem as the breakthrough point, based on the feature of the AES (Advanced Encryption Standard) algorithm and the pseudo-randomness of the chaotic encryption algorithm when generating sequences, a hybrid of AES encryption and chaotic encryption algorithm is proposed. Taking electrical infrared image as an example, the hybrid encryption of the sample image is completed through Matlab. In order to verify the security of the hybrid encryption algorithm, the experiment uses adjacent pixel correlation and histogram as evaluation criteria. The result shows that the hybrid encryption algorithm is more secure than the unilateral AES encryption algorithm, and its application prospects are broader.

【Key words】 AES encryption; chaos encryption; security analysis; image correlation

0 引 言

随着科学技术的不断发展，人们之间的联系越来越近。此时，网络的安全保密问题已十分严峻。多年来，各个领域都非常重视的安全储存、传输的机密，以及信息的真实性核查，由此诞生了各种加密算法。

数字图像加密的目的是通过隐藏算法来隐藏目标的图像信息，从而失去图像的原有面目，通过载体信息也无法直接分辨加密后的图像隐藏的内容。本研究采用文献研究法，对 AES(Advanced Encryption Standard)加密算法及混沌加密能否混合进行了预测，其成功率超过 90%。以此为基础设计出一种新的混合加密算法。为验证该混合算法的有效性，使用 MATLAB 为开发工具，对电气红外图像进行混合加密及解密，分别从直方图和相邻像素的相关性方面对混合加密算法进行了安全性分析。

加密算法种类颇多，各有所长。本研究主要以 AES 加密算法为基础进行探讨，见表 1。

表 1 不同算法比较表

Tab. 1 Comparison of different algorithms

算法	类型	密钥长度	说 明
AES	对称密码	长度可变(128 位、192 或 256 位)	替代 DES 的新密码算法
TripleDES	对称密码	168 位(112 位有效)	对 DES 作了一些改进，能满足当前的安全需要
Blowfish	对称密码	长度可变(可以达到 448 位)	长的密钥长度提供了很好的安全性
RC4	对称密码	长度可变(通常从 40 位到 128 位)	快速的流密码。主要用在 SSL 中
DES	对称密码	56 位	常见的加密方法

1 AES 加密原理及实验

AES 加密是一种矩阵操作。该矩阵称为状态(state)阵列。其原始值是明文块[1-3]。当通过加密可以增加矩阵行数时，每轮 AES 加密循环包含 4 个步骤。

(1)轮密钥加。矩阵中的每一个字节都与该次轮秘钥(round key)做 XOR 运算；每个子密钥由密

作者简介：吴沐阳(1992-)，男，硕士，助理工程师，主要研究方向：通信系统研究、网络安全性；姚亚峰(1970-)，男，博士，副教授，主要研究方向：通信系统设计、现代信号处理；唐 义(1984-)，男，硕士，中级工程师，主要研究方向：电气自动化、智能电网。

收稿日期：2020-06-18

钥生成方案产生。

(2)字节替换。通过个非线性的替换函数,用查找表的方式把每个字节替换成对应的字节。

(3)行移位。对矩阵中的每个横列进行循环移位操作。

(4)列混淆。充分混合矩阵中各个直行的操作。

在最后一个加密循环过程中,轮密钥加取代列混合步骤。

本研究以电气红外图像为实验样本,对其进行 AES 加密。在得到加密的乱码图像后,再进行解密,最后可得到原图像。加密过程如图 1 所示。

(a) 加密前 (b) 加密后 (c) 解密后

(a) Before encryption (b) After encryption (c) After decryption

图 1 红外成像仿真图

Fig. 1 Infrared imaging simulation

2 混沌加密原理及仿真实验

混沌理论与相对论、量子力学并列为 20 世纪的三大发现[4]。混沌算法将决定论和随机论紧密联系在一起,改变了人们对随机性和确定性的认识。科研人员从中可知,混沌和加密有天然的联系。Shannon 曾经说过:一个好的混合变换疆场是由两个简单的、不可交换的操作得到。混沌和加密的关系见表 2。

表 2 混沌和加密的对比

Tab. 2 Comparison of chaos and encryption

混沌性质	加密的性质	描述
遍历性	混乱性	输出具有类似的分布状态
对参数敏感	对变换具有扩散性	输入引起输出的改变
混合性	具有扩散性	局部变化引起整个空间的变化
动力系统确定性	伪随机流确定性	系统产生伪随机信号
结构复杂	算法(攻击)复杂	过程简单,结果复杂

本文采用 Logistic 映射作为混沌模型,对图像进行加密,其数学表达公式为:

$$X_{n+1} = X_n \times \mu \times (1 - X_n), \quad (1)$$

其中, X_n 为状态量; μ 为系统控制参数。

研究表明,当 $X \in (0,1)$ 时, Logistic 映射工作处于混沌状态。因此, 初始条件 X_0 在 Logistic 映射作用下产生的序列是非周期的、不收敛的;而在此范围之外,生成的序列必将收敛于某一个特定的值。

当 $1 < \mu \leqslant 3$ 时,定常解为 0 和 $1/\mu$,多次迭代后序列会收敛于这两个值之一。当 $3 < \mu < 4$ 时,系统由倍周期通向混沌。特别是,当 3.569 945 6… $< \mu < 4$ 时,系统进入混沌状态,迭代生成的值处于一种伪随机分布的状态,随着 μ 取值越接近 4,混沌性越强。当 $\mu = 4$ 时,Logistic 映射的 Lyapunov 指数为 $ln2 = 0.693\ 1$。

混沌的加密、解密过程如下。

2.1 加密过程

(1)给定两个 Logistic 系统参数 U_1 和 U_2 及初值 X_{10}、X_{20}。

(2)用原始图像 A 所有像素值之和对 256 做取余运算, 得到整数 d,$d \in [0,255]$,d 除以 256 的结果作为辅助密钥 k,$k \in (0,l)$。

(3)通过辅助密钥 k 对混沌系统初始值进行修改:$X_{10} = (X_{10} + k)/2$,$X_{20} = (X_{20} + k)/2$。修正后的 X_{10}、X_{20} 作为 *logistic* 混沌系统的初始值,构造 2 个长度为 $M * N$ 的实数混沌序列。

(4)转换第(3)步 2 个实数混沌序列, 得到2个改进的混沌序列:$\{y1(i)\}$,$\{y2(i)\}$,$i = 1,2,3,\cdots,M*N$。

(5)顺序取图像中的一点 n(n 为该点序号),n 为奇数时,则由实数混沌序列的 $y_1(n)$ 构造加密密钥:$k(n) = mod(floor(y1(n) * 10 * 15),256)$;若 n 为偶数,则由实数混沌序列的 $y_2(n)$ 构造加密密钥:$k(n) = mod(floor(y2(n) * 10 * 15),256)$。

(6)用原始图像 A 中的第 n 个像素点灰度值 $A(x,y)$ 与步骤(5)产生的 logistic 密钥值进行二进制位异或操作,得到加密后的像素值 $A'(x,y)$。

(7)反复进行步骤(5)、(6)操作,直到所有的像素被加密,即可获得加密图像 A"。

2.2 解密过程

解密处理是上面加密处理的逆过程,经反向操作获得原始图像。对于混沌算法的实验仿真同样采用 MATLAB 进行。实验结果如图 2 所示。

图 2 混沌解密仿真过程图

Fig. 2 Chaotic decryption simulation process diagram

从仿真结果可得,采用混沌算法同样可以达到加密的目的。加密后的图像无明显信息,加密算法是可行的;对加密后的图像解密之后,即得到原图像,从而验证了算法解密的可靠性。

3 混合加密

混合加密即为将原始图像首先进行 AES 加密,然后再进行混沌加密,通过这样级联加密的方式来使图形的安全性得到进一步加强,让破译者在对图像的破译变得更加麻烦、更难破译。

本文以电气工程中常见的红外图像为示例，对混合算法进行有效性进行探讨。首先对红外成像仿真图 1、图 2 分别进行一级 AES 加密，加密后图像立即变得模糊，然后对红外成像仿真进行二级混沌加密，得到的级联加密图像变得更加模糊，相邻像素间的联系性变得越来越小。通过两个加密算法的结合可以看到，原始图像的加密性能变得越来越好，加密图像的安全性也因此得到提高，两种级联加密算法的统一性与完整性也得以验证。此外，仿真结果显示了该算法对于不同图形的普遍适应性。仿真结果见表 3。

表 3　单混加密对比表

Tab. 3　Single mixed encryption comparison

	红外成像仿真图 1	红外成像仿真图 2
原始图像		
AES 加密后		
混沌加密后		
混沌解密后		
AES 解密后		

4　安全性分析

安全性分析是评估加密算法优劣的重要指标之一[8]，安全系数高的加密算法往往能在生活中发挥更稳定的作用。本研究主要讨论图片传输过程中的加密算法。针对图片的组成特性，将从相邻像素相关性和直方图两方面来探讨混合加密算法的安全性。

4.1　相邻像素相关性分析

相邻像素相关性反映图像相邻位置像素值的相关程度[9]。好的图像加密算法应能降低相邻像素的相关性，尽量达到零相关。通常要对图像的水平、垂直、对角像素 3 个方面进行分析。

研究在 matlab7 平台上对图片加密前后的相邻像素相关性进行分析。分别得到原始图像、AES 加密后图像以及混合加密后图像的相关性图。

图像相关性一般可从相关性图和 R 值两方面衡量。图 3 为加密前图像的像素相关性，从中可以看出原始图像的相邻像素相关性比较大，分布不均匀，容易从相关性上获取图片信息。由图 4 可知，经一级加密后使图像的相邻像素相关性大大减少，证明 AES 能很好的防止统计攻击。而从图 5 可得级联加密后，R 值在 AES 一级加密的基础上，又大大减少，证明级联加密比一级 AES 加密效果更优。R 值可由式(2) 而得。

$$R = \frac{\sum (X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum (X_i - \bar{X})^2 (Y_i - \bar{Y}^2}}. \tag{2}$$

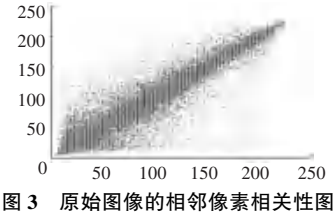


图 3　原始图像的相邻像素相关性图 (R=0.927)

Fig. 3　Adjacent pixel correlation diagram of original image

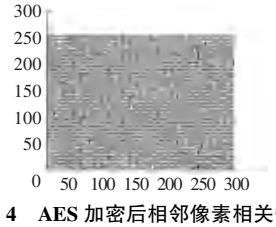


图 4　AES 加密后相邻像素相关性图 (R=0.023)

Fig. 4　Correlation diagram of adjacent pixels after AES encryption

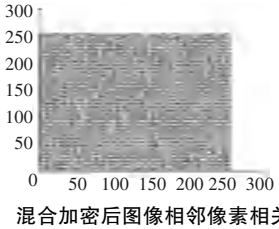


图 5　混合加密后图像相邻像素相关性图 (R=0.002)

Fig. 5　Correlation map of adjacent pixels after concatenated encryption

为了更好更直观的体现不同加密方式在相邻像素不同方向的相关系数，研究列表摆出实验数据。混合加密算法在各方面均比单一的 AES 加密的相关系数更低，安全性更高，见表 4。

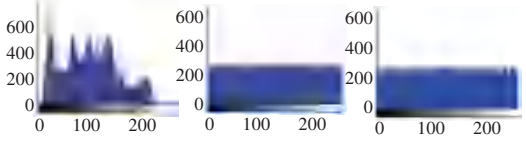
表 4　各方向相关系数

Tab. 4　Correlation coefficient in all directions

相关系数	原图	AES 加密图	混沌加密图
对角线方向	0.924 7	−0.001 2	0.000 4
水平方向	0.985 8	0.003 2	−0.004 6
垂直方向	0.956 6	0.005 6	0.000 502

4.2　直方图分析

直方图(Histogram) 是一种统计报告图，又称质量分布图，由一系列高度不等的纵向条纹或线段表示数据分布的情况。图像的直方图是图像的重要统计特征，它表示了数字图像中每一个灰度级与该灰度级出现的频率间的统计关系[10]。对一幅灰度图像从上到下、从左到右扫描每个像素值，在每个灰度值上计算像素数目，以这些数据为基础即可完成图像直方图的绘制。本研究对图像加密前后直方图对比结果如图 6 所示。



(a) 加密前图像　(b) AES 加密后　(c) 级联加密后

(a) Before encryption (b) After AES encryption (c) After joint encryption

图 6　加密前后直方图对比

Fig. 6　Histogram comparison before and after encryption

由图 5 可知，原始图像的直方图，波形棱角分明，包含丰富的图像信息。而加密后的图像的直方图，波形趋于平均，很难破解出图像的统计特性。混合加密相比单一的 AES 加密的直方图而言，虽用肉眼看不出图像的细微差别，但通过对多幅图像的测

试数据中显示,其直方图信息更难被破译,故混合加密地安全性更好。

5 结束语

加密算法的研究是一个不断更新换代的过程,本研究设计的算法尝试性的将两种完全不同的加密算法级联在一起得到新的混合算法,并通过 matlab 平台对该算法进行了仿真。仿真结果说明,该混合算法能很好的完成图像加密,并且解密后图像还原度很高。研究证明,混合算法的混合理念是可行的,今后可更多的沿用混合思想将不同的算法组合在一起,互相取长补短,从而达到更好的加密效果。

安全性是衡量加密算法的重要指标,本文根据研究对象的载体是图片这一特性,从图片相邻像素相关性和直方图两方面比较了有混沌加密加持的 AES 算法与单一 AES 加密算法的安全性,结果显示混合算法在两方面都优于单一算法,混合算法拥有更高的安全性。

本次研究虽然得到了一个安全性高的混合加密算法,但其各项性能有待进一步提高。后续研究可从改变混合的双方算法入手,提高算法的可靠性和实用性。

参考文献

[1] 闵连权. 一种实用的图像加密算法[J]. 遥感技术与应用, 2005, 20(5): 512-516.

[2] RÖSSLER O E. An equation for continuous chaos[J]. Physics Letters A, 1976, 57(5): 397-398.

[3] CHEN G, UETA T. Yet another chaotic attractor[J]. International Journal of Bifurcation and chaos, 1999, 9(7): 1465-1466.

[4] HALE J K, LUNEL S M V, VERDUYN L S, et al. Introduction to functional differential equations[M]. Springer Science & Business Media, 1993.

[5] 韦鹏程,张伟,杨华千. 一种基于共轭混沌映射的图像加密算法[J]. 计算机科学,2006,11:237-240.

[6] 王永,杨德刚,韦鹏程,等. 一种基于复合离散混沌系统的对称图像加密算法[J]. 计算机科学,2006,33(12):86-90.

[7] 廖晓峰,张伟,韦鹏程,等. 对一种基于混沌映射的对称图像加密算法的改进[J]. 计算机科学,2007,34(12):248-251.

[8] SALOMAA A. Public-key cryptography[M]. Springer Science & Business Media, 2013.

[9] RHEE M Y. Cryptography and secure communications[M]. McGraw-Hill, Inc., 1993.

[10] ZHU J, ZHAP H. Five-dimensional chaotic system and its circuitry implementation[C]//2009 2nd International Congress on Image and Signal Processing. IEEE, 2009: 1-5.

(上接第 40 页)

归到了指定状态;由三相电流局部放大图知负载于 0.5 s 突变后电流值稳定在 220 A 上下,相比无参数变化时电流值有明显变小,但波形始终平稳且无较大纹波。

总体来看,采用曲线拟合 MTPA 控制算法后易于在数字控制器上实现,且电机控制系统不论在参数变化前还是参数变化后系统性能基本保持不变,试验证实了本文所采用的曲线拟合 MTPA 控制算法的有效性。

4 结束语

本文针对电动汽车用内置式永磁同步电机在实际运行工况中会产生参数变化的实际情况,决定采用曲线拟合 MTPA 控制算法对电机的电磁转矩与交、直轴电流曲线进行曲线拟合,该算法简单方便易于实现,同时利于工程实践。

最后仿真验证了该方法可以在参数变化的情况下仍能以最优的电流进行控制,提高了电机的运行效率,增强了系统的鲁棒性,在工程上有很大的应用价值。

参考文献

[1] WU J, WANG J, GAN C, et al. Efficiency Optimization of PMSM Drives Using Field-Circuit Coupled FEM for EV/HEV Applications[J]. IEEE Access, 2018: 15192-15201. 5th order polynomial fitting.

[2] EBRAHIMI B M, FAIZ J, ROSHTKHARI M J. Static-, Dynamic-, and Mixed-Eccentricity Fault Diagnoses in Permanent-Magnet Synchronous Motors[J]. IEEE Transactions on Industrial Electronics, 2009, 56(11):4727-4739.

[3] 王艾萌. 内置式永磁同步电动机的优化设计及弱磁控制研究[D]. 华北电力大学(河北),2010.

[4] 龚锦标,施火泉. 一种改进的永磁同步电机 MTPA 控制算法[J]. 电子测量技术,2018,41(16):52-55.

[5] ZHU D, LIU G, WANG J, et al. A comparison of two MTPA algorithms for an interior permanent magnet synchronous motor drives[C]// International Conference on Electrical Machines & Systems. IEEE, 2017.

[6] JUNG S Y, HONG J, NAM K. Current Minimizing Torque Control of the IPMSM Using Ferrari's Method[J]. IEEE Transactions on Power Electronics, 2013, 28(12):5603-5617.

[7] MALEKPOUR M, AZIZIPANAH-ABARGHOOEE R, TERZIJA V. Maximum torque per ampere control with direct voltage control for IPMSM drive systems[J]. International Journal of Electrical Power & Energy Systems, 2020, 116:105509.

[8] 吴芳. 内置式永磁同步电机最大转矩电流比控制策略研究[D]. 2013.

[9] 李军, 余家俊. 基于分段曲线拟合的 IPMSM 最大转矩电流比控制研究[J]. 工程科学与技术, 2012(S1):307-311.

[10] 陈起旭, 邹忠月, 曹秉刚,等. 纯电动汽车用内置式 PMSM 的 MTPA-FW 控制算法对比研究[J]. 微电机, 2017, 50(6):44-50.

[11] 曹晖, 罗峰, 周盼,等. 永磁同步电机最大转矩电流比控制的仿真研究[J]. 微电机, 2015 (6):55-59.

[12] 田以涛, 王英. 基于最大转矩电流比的永磁同步电动机矢量控制[J]. 电机与控制应用, 2013, 40(5):25-28,58.

[13] 杨强, 冉杰, 范泽宇,等. 考虑参数摄动的永磁同步电机转速跟踪控制器设计[J]. 成都信息工程大学报, 2018, 33(6):612-616.

[14] 叶敏, 郭振宇, 程博,等. 基于参数摄动的电动汽车再生制动鲁棒混合控制研究[J]. 西安交通大学学报, 2007, 41(1):64-68.