基于 AES 的数字图像置乱方法

陈燕梅 张胜元
(福建师范大学数学与计算机科学学院,福州 350007)

摘 要 以图像信息安全问题为背景,介绍了高级加密标准(AES):Rijndael 算法,并在此对称分组密码算法的基础上,提出了密钥控制下采用 AES 算法进行图像置乱与恢复的方法。该方法既安全又简便。实验结果显示了图像置乱的效果,通过直方图的比较对此进行一定的分析,结果表明,这种方法能达到较好的加密与解密效果,而且易于实现。

关键词 高级加密标准(AES) 数字图像 数字图像置乱 信息安全
中图法分类号: TN911 **文献标识码**: A **文章编号**: 1006-8961(2006)08-1076-05

A Method for Digital Image Scrambling Based on AES

CHEN Yan-mei, ZHANG Sheng-yuan
(*School of Mathematics and Computer Science, Fujian Normal University, Fuzhou* 350007)

Abstract With the security problem of image information as research background, this paper introduces the Advanced Encryption Standard(AES): Rijndael algorithm. Base on the symmetry block cipher algorithm, a method for scrambling and restoring digital images is proposed, which uses the AES algorithm under the control of secret key. This method is safe as well as simple. A simulation shows the effect of image scrambling, and it is analyzed by comparison of histograms. The results show that: this method can reach preferable effect of encryption and decryption, and further more, it's easy to realize.

Keywords advanced encryption standard(AES), digital image, digital image scrambling, information security

1 引 言

数字图像信息安全,是伴随着计算机网络和多媒体技术的迅速发展而产生的新问题。近年来,数字图像技术逐渐克服了往日因存储量巨大而带来的困难,成为信息表达方式的主流,这与人类认知世界的基本方式是相吻合的。然而,问题由之而生,如何保证数字图像信息的安全成为国际上热门的研究课题。

数字图像置乱起源于早期的经典加密学理论和电视图像应用技术,对数字图像的空间域进行类似于经典密码学对 1 维信号的置换,或者修改数字图像的变换域参数,使得图像的视觉效果呈现出各像素随机分布的特点,达到保护原图像内容的目的。

现有几种数字图像置乱方法,主要是基于 Arnold 变换的系列置乱方法;用分形图形学中的方法来对空间曲线进行填充,以及利用其他数学知识和奇特现象进行数字图像置乱[1]。本文提出了一种基于对称分组密码算法 AES 的数字图像置乱方法,并通过实验分析了置乱的效果,验证了此方法的有效性。

2 AES 简介

近年来,DES(data encryption standard)[2]已逐渐显现出许多不足之处,其安全性受到了挑战。一种新的、安全强度高、适合软硬件实现的高效加密标准—高级数据加密标准 AES(advanced encryption standard)[3]应运而生。2000 年 10 月,美国国家标准和技术协会(NIST)宣布从 15 种候选算法中选取出 Rijndael 算法,作为新的对称加密算法标准,称为 AES[4]。

Rijndael 算法[4]是一种分组密码算法,它的分组长度和密钥长度可分别被指定为 128bit、192bit 或

基金项目:国家自然科学基金项目(10226028);福建省泉州市科技重点项目(2004g27)
收稿日期:2005-06-05;**改回日期**:2005-09-13

第一作者简介:陈燕梅(1981~),女。福建师范大学数学与计算机科学学院硕士研究生。主要研究方向为密码学与信息安全。E-mail: happygirlcym@126.com

256bit。本文指定分组长度为 128bit,采用 128bit 的密钥,在这一参数下,算法中轮循环次数为 10 次。

2.1 AES 算法描述

2.1.1 状态矩阵(State)

AES 算法[4~6]将每一个分组的 128bit 视为以 8bit(Byte)为单元的 4×4 矩阵,所有的运算都在该 2 维矩阵上进行,即状态矩阵。矩阵的元素可以用两个十六进制的字符表示,每一列的 4 个 Byte 又被称为一个双字(Word)。

2.1.2 轮操作(Round operation)

AES 算法的核心为对 State 矩阵的 10 次轮操作。除了第 10 轮操作不包含 MixColumns 函数,加密算法中每一次轮操作都由 SubBytes, ShiftRows, MixColumns 和 AddRoundKey4 个函数组成。

(1)位变换(SubBytes)

SubBytes 是非线性运算。由于进行该运算比较复杂,因此在设计过程中先将 0~255 内所有的数进行上述 SubBytes 运算,得到表 SBox,再采用查表法进行运算。对于一个十进制数,将其化为一个 8 位的二进制数:*abcdefgh*,找到 *abcd* 行和 *efgh* 列的位置(行和列都是从 0~15 进行编号),该位置上的值就是它的输出。

(2)行移位(ShiftRows)

ShiftRows 是对 State 矩阵进行行移位操作,第 1 行不移位,第 2 行循环左移一位,第 3 行循环左移 2 位,第 4 行循环左移 3 位。

(3)列混合(MixColumns)

MixColumns 操作是在 State 矩阵内每一列进行如下变换:

$$\begin{pmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{pmatrix}$$

乘积矩阵中的每个元素均是一行和一列中所对应元素的乘积之和。这里的乘法和加法都是定义在有限域 GF(2^8)上的。

(4) 轮密钥加(AddRoundKey)

AddRoundKey 是将 State 矩阵中每个 Byte 与轮密钥组中对应的 Byte 进行异或操作。

2.1.3 密钥扩展(KeyExpansion)

每一次的轮操作都需要一组(4 列)新的轮密钥,所以必须对原来输入的 128bit 进行扩展。详细的密钥扩展方法可见文献[4]。

2.2 AES 算法的加密、解密流程图

AES 算法的加密、解密流程图如图 1,图 2 所示。

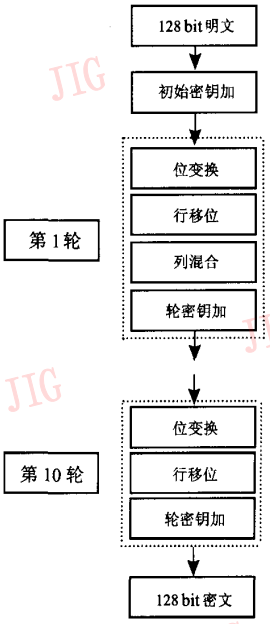


图 1　加密流程

Fig. 1　Encryption flow

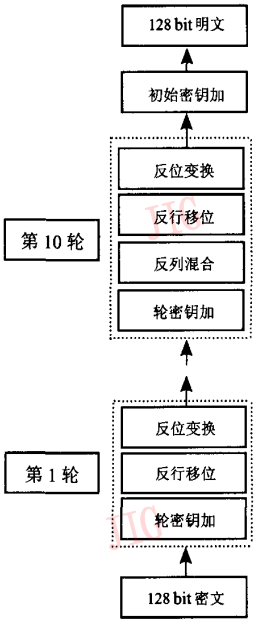


图 2　解密流程

Fig. 2　Decryption flow

可见,在解密时,只需将所有操作的逆变换逆序

进行,并逆序使用密钥编排方案即可。而 AES 算法有其特殊性,即解密本质上和加密有相同的结构,因而存在“等价逆密码”,这个“等价逆密码”能通过原变换的一系列逆变换来实现 AES 算法的解密,这些逆变换按与 AES 算法加密相同的顺序进行。只是密钥扩展有所不同,即先应用原密钥扩展,再将 InvMixColumns 应用到除第 1 轮和最后一轮外的所有轮密钥上。

2.3 AES 算法的特性

(1)对所有已知的攻击具有免疫性。

(2)在各种平台上,其执行速度快而且代码紧凑。

(3)设计简单。

3 基于 AES 算法的数字图像置乱

一幅数字图像 P 可以看作是一个矩阵 $\boldsymbol{P}$,矩阵元素所在的行与列,就是图像显示在计算机屏幕上的诸像素点的坐标,元素的数值就是像素的灰度(通常有 256 个等级,用整数 0 至 255 表示)。彩色图像可以取成混合矩阵,每个像素灰度值与红色(R)、绿色(G)、蓝色(B)有关,可以用 3 个数值矩阵($\boldsymbol{P}^{R}$,$\boldsymbol{P}^{G}$,$\boldsymbol{P}^{B}$)表示。

由于 AES 算法的状态矩阵是以 8bit(Byte)为单元的 4×4 矩阵,矩阵元素的值在 0 至 255 之间,这与通常所用的图像的灰度相吻合。因此,对于一幅图像,将其数字化后得到一个矩阵,对该矩阵采用 AES 算法进行分块处理(不同的图像块在图像中无重叠地排列),即从左上角开始,每 4×4 分块矩阵用 AES 算法加密一次,再将各分块组合,则可以得到与原来不同的矩阵,从而改变了图像像素的灰度值,达到数字图像置乱的目的。显然,图像的恢复过程即是对各分块矩阵的逆运算过程,也就是对置乱后的图像矩阵每 4×4 分块用 AES 算法解密一次。在具体实现的过程中,如果图像矩阵行值或列值不是 4 的倍数,则在底部或右部补 0,使之成为完整分块。

基于以上的分析,程序基本流程如下:

图像加密流程:

(1)给定需要置乱的图像 $\boldsymbol{P}$ 以及口令 X;

(2)由口令生成一个随机的 4×4 矩阵 $\boldsymbol{W}$,并用 $KeyExpansion(\boldsymbol{W})$ 进行密钥扩展,计算 11 轮密钥 key;

(3)读入图像信息,将 R、G、B 值存至矩阵 $\boldsymbol{P}$,$\boldsymbol{P}=(p_{ij})_{n\times m}$,$p_{ij}\in\{0,1,\cdots,255\}$;

(4)置乱:对矩阵 $\boldsymbol{P}$ 的每 4×4 分块 p 采用 AES 算法加密一次,即调用 $Rijndael(p,key)$ 进行运算,将结果存入原分块;

(5)输出置乱图像 $\boldsymbol{P}'$;

(6)将 $\boldsymbol{P}'$在公开通道上进行传输;

(7)将密钥字符串 X 在安全通道上进行传输。

图像解密流程:

(1)从公开渠道得到置乱图像 $\boldsymbol{P}'$;

(2)从安全通道得到密钥字符串 X;

(3)由 X 生成一个随机的 4×4 矩阵 $\boldsymbol{W}$,并计算 11 轮密钥 key';

(4)读入图像信息,将 R、G、B 值存至矩阵 $\boldsymbol{P}'$,$\boldsymbol{P}'=(p'_{ij})_{n\times m}$,$p'_{ij}\in\{0,1,\cdots,255\}$;

(5)复原:对矩阵 $\boldsymbol{P}'$的每 4×4 分块 p'采用 AES 算法解密一次,即调用 $InvRijndael(p',key')$ 进行运算,将结果存入原分块;

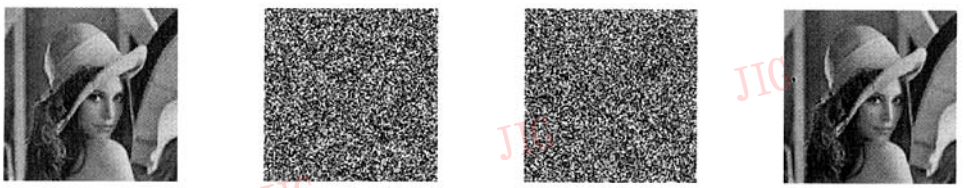
(6)输出复原图像。

以上算法,可在 Matlab7.0 上仿真实现。

4 实验结果与分析

4.1 图像的置乱效果

采用上面介绍的方法进行图像置乱,效果如图 3所示。



(a) 原图 (b) 置乱图(3 轮 AES) (c) 置乱图(11 轮 AES) (d) 复原图(3 轮、11 轮 AES)

图 3 图像置乱效果

Fig. 3 Results of image scrambling

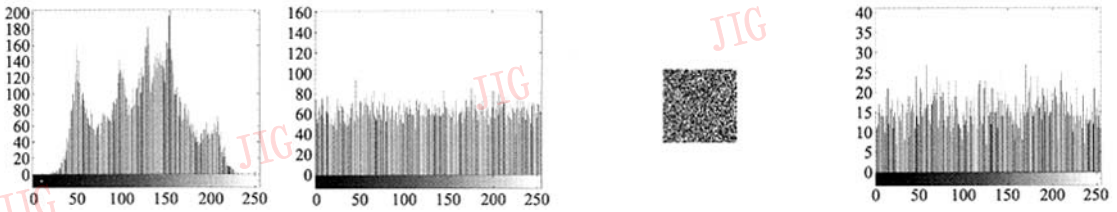
可见,只需应用 3 轮的 AES 算法即可达到很好的置乱效果。AES 算法在设计时已经考虑了差分攻击与线性攻击(例如,S 盒构造中有限域逆操作的使用导致了线性逼近和差分分布表中的各项趋近于平均分布),因此 4 轮以上的 AES 算法对差分攻击和线性攻击基本上是免疫的[7]。因而在图像置乱时,可以根据实际需要采用一定轮数的 AES 算法进行图像加密。

4.2　置乱效果的具体分析

一幅图像的"概貌"可以通过其灰度直方图来描述。例如,如果一幅图像对比度低,则直方图窄而集中于灰度级的中部;如果一幅图像其像素占有全部可能的灰度级并且分布均匀,则这样的图像有高对比度和多变的灰度色调。因而可以通过直方图的比较来分析置乱的效果。

对于一幅类似白噪声的图像,其直方图充满整个区域,而且分布比较均匀。同时,任意截取其中的某个小区域,其直方图的分布具有自相似性。

图 4 就是对置乱前后图像的直方图的一个比较。其中,图 4(a)为图 3(a)的直方图,图 4(b)为图 3(b)的直方图,图 4(c)是从图 3(b)中任意截取一块小区域,图 4(d)是截取出来的小块图像的直方图。从图中可以看出,置乱图像的直方图充满整个区域,而且分布比较均匀。用直方图的相似度来定量地描述置乱的效果。



(a) 原图直方图　(b) 置乱后直方图　(c) 置乱后截取图　(d) 截取图直方图

图 4　直方图比较

Fig. 4　Comparison of histograms

设两图像灰度直方图分别为 $r_1(k)$,$r_2(k)$,$k=0,1,\cdots,G-1$,则定义直方图的相似度[8]为

$$\alpha = 1 - \frac{\sum_{k=0}^{G-1} |r_1(k) - r_2(k)|}{\sum_{k=0}^{G-1} |r_1(k) + r_2(k)|} \qquad (1)$$

对于一幅纯噪声的图像,其直方图分布应该是均匀的,即 $r(i)=r(j)$,$\forall i, j \in \{0,1,\cdots,G-1\}$。用式(1)可计算得置乱后的图像与白噪声图像的直方图相似度为0.948 5,所截取的小图像与白噪声图像的直方图相似度为 0.906 5,而截取部分与整幅置乱图像的直方图相似度为 0.955 7。

这说明经过置乱后图像类似于白噪声,置乱效果良好。

5　结　论

数字图像置乱技术,可以看作数字图像加密的一种途径,也可以用做数字图像隐藏、数字水印图像植入、数值计算恢复方法和数字图像分存的预处理和后处理过程[9]。对于数字图像置乱,人们已做过许多有益的探索,取得了不少成果。但是,寻找一种安全而又简便的置乱方法,一直是数字图像置乱研究的内容。

根据美国国家安全局(National Security Agency,简称 NSA)验证,Rijndael 加/解密算法能有效抵抗目前所有已知攻击算法的攻击。本文提出了密钥控制下采用 AES 算法进行图像置乱与恢复的方法,此方法融合了各种特色,而且设计简单。由于 Matlab 具有强大的数值计算功能尤其是对数组和矩阵的运算,而 AES 算法的基础结构正是以矩阵为基本单位,所以在 Matlab 环境下实现对 AES 算法的仿真简便易行。从上述实验结果与分析来看,这种方法能达到很好的图像置乱效果。而且解密本质上和加密有相同的结构,能够方便地恢复出原始图像。相信这将会有很好的应用前景。

参考文献(References)

1　Yan Wei-qi, Zou Jian-cheng, Qi Dong-xu. A novel digital image scrambling method base on DES [J]. Journal of North China

University of Technology, 2002, **14**(1):1 ~ 7. [闫伟齐,邹建成,齐乐旭. 一种基于 DES 的数字图像置乱新方法[J]. 北方工业大学学报, 2002, **14**(1):1 ~ 7.]

2 Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C(Second Edition)[M]. Brisbane Austr alia: John Wiley and Sons, 1996. [Schneier B 著. 应用密码学: 协议、算法与 C 语言源程序(第 2 版)[M]. 吴世忠等译, 北京:机械工业出版社, 2000.]

3 Daemen J, Rijmen J. AES Proposal: Rijndael[R]. Ventura CA: National Institute of Standards and Technology, 1998:1 ~ 45.

4 Stallings W. Cryptography and Network Security: Principles and Practices(Third Edition)[M]. New Jersey: Prentice Hall, 2003. [Stallings W 著. 密码编码学与网络安全: 原理与实践(第 3 版)[M], 刘玉珍等译, 北京:电子工业出版社, 2004.]

5 Cai Yu-dong, Shen Hai-bin, Yan Xiao-lang. A high-speed implementation of AES[J]. Microelectronics and Computer, 2004, **21**(1):83 ~ 85. [蔡宇东, 沈海斌, 严晓浪. AES 算法的高速实现[J]. 微电子学与计算机, 2004, **21**(1):83 ~ 85.]

6 Trappe W, Washington L C. Introduction to Cryptography with Coding Theory[M]. New Jersey: Prentice Hall, 2002. [Trappe W, Washington L C 著. 密码学概论[M]. 邹红霞等译, 北京:人民邮电出版社, 2004.]

7 Cao Hua-ping, Luo Shou-shan, Wen Qiao-yan, *et al*. On the relationship between the round key and the cipher key of the AES algorithm [J]. Journal of Beijing University of Posts and Telecommunications, 2002, **25**(4): 47 ~ 50. [曹华平, 罗守山, 温巧燕等. AES 算法轮密钥与种子密钥之间的关系研究[J]. 北京邮电大学学报, 2002, **25**(4):47 ~ 50.]

8 Sui Xin-guang, Luo Hui. Digital image scrambling base on S-box [J]. Journal of images and graphics, 2004, **9**(10):1223 ~ 1226. [眭新光,罗慧. 基于 S 盒的数字图像置乱技术[J]. 中国图象图形学报, 2004, **9**(10):1223 ~ 1226.]

9 Zou Jian-cheng, Li Guo-fu, Qi Dong-xu. Generalized gray code and its application in the scrambling technology of digital image [J]. Appl. Math. J. Chinese Univ. (A), 2002, **17**(3):363 ~ 370. [邹建成, 李国富, 齐东旭. 广义 Gray 码及其在数字图像置乱中的应用[J]. 高校应用数学学报(A 辑), 2002, **17**(3):363 ~ 370.]