文章编号:1000－2367(2016)05－0163－06 DOI:10.16366/j.cnki.1000－2367.2016.05.027

基于虹膜特征的密钥生成和 AES 算法的图像加密

解瑞云[1],海本斋[2]

(1.河南工学院 计算机科学与技术系,河南 新乡 453000;
2. 河南师范大学 计算机与信息工程学院,河南 新乡 453007)

摘 要:针对传统加密算法密钥长、记忆困难、不易安全持有等特点,提出虹膜特征密钥提取和 AES 加密算法相结合的图像加密算法.该算法利用 db2 小波分解的虹膜区域,提取第三层的虹膜关键特征高频系数,通过使用随机映射函数生成一个 192 位的密钥.随后将该算法与经典的 Arnold 算法的同时应用于图像加密实验.实验结果表明,利用该算法得到的加密图像的安全性更高.

关键词:虹膜特征;小波变换;AES;图像加密

中图分类号:TP399 **文献标志码**:A

加密算法的安全性是由密钥决定的,然而,密钥过长也会导致记忆和保存困难,同时来自外部的密钥,也会带来加密算法潜在的安全问题.而从人体的生物特征提取出来的密钥,具有唯一性、终身性和可移植性等优点,使得加密信息的安全性可以大大提高.基于生物特征的关键是应用最早在 1989 年出现于 IBM 交易安全系统中利用签字笔和手写信号处理器进行的在线交易过程中[1].MONROSE 等人成功地从声音和按键行为提取密钥[2-3],文献[4]将指纹特征与智能设备的结合提高了加密信息的安全性,文献[5]根据整个特征空间中的生物特征分布映射到加密密钥.然而,这些算法距离实际应用还有一定的距离.此外,基于虹膜特征的密钥生成方法,以及在加密过程中如何使用生成的密钥,这些都是值得进一步研究的问题.

这里提出了一种基于虹膜特征的图像加密算法.该算法首先对虹膜图像进行预处理,随后采用 db2 小波提取虹膜特征,接着利用随机映射函数在将虹膜特征编码的过程中随机生成 192 位密钥,将该密钥与 AES 相结合进行图像加密实验.实验结果表明,与经典的 Arnold 图像加密算法相比,新算法在图像信息保护方面具有更好地安全性.

1 基于小波变换的虹膜特征提取

1.1 小波变换的基本原理

1986 年以来,由于 Y. Meyer,S. Mallat 和 I. Daubechies 的基础工作,小波分析作为傅里叶分析的革命性变革的结果,迅速发展成为一门新兴学科.它的历史可以追溯到 Haar 在 1909 年的工作.从当前小波变换视角看,小波变换许多研究方向出现与 20 世纪 30 年代 Lévy,Littlewood,Paley,Franklin 和 Lusin 的工作相关,由于二战的影响,此后没有新的研究出现.后来由于 Calderón 和 Grossmann 的研究工作,小波变换被称为“原子分解”,目前小波变换在许多科学研究方面得到了广泛应用[6].

小波分析在理论和应用方面具有深刻而广泛的意义,它能通过对时间(空间)频率的局部化分析,有效地从信号中提取信息.它的主要特点是通过变换能够充分突出问题某些方面的特征,通过伸缩平移运算对信号(函数)逐步进行多尺度细化,最终达到从而可聚焦到信号的任意细节,因此小波变换被称为“数学显微镜”.

收稿日期:2016-05-06;**修回日期**:2016-07-11.

基金项目:国家自然科学基金(U1404602);河南省高等学校重点科研项目(15B520006);河南省科技攻关重点项目(162102310442);河南师范大学青年科学基金(2014QK30).

第 1 作者简介(通信作者):解瑞云(1980－),女,河南商丘人,河南工学院讲师,研究方向为计算机网络、网络安全等,E-mail:xieruiyun888@163.com.

它在数学领域本身、信号分析、图像处理、计算机识别、数据压缩、特征提取等领域取得了重要的科学意义和应用价值.

短时傅里叶变换(STFT)窗口函数表示为:

$$\varphi_a(t,\omega) = \varphi(t-a)\mathrm{e}^{-\mathrm{i}t\omega}. \tag{1}$$

短时傅里叶变换(STFT) 其窗口函数通过函数时间轴的平移与频率限制得到,由此得到的时频分析窗口具有固定的大小.对于非平稳信号而言,需要时频窗口具有可调的性质,即要求在高频部分具有较好的时间分辨率特性,而在低频部分具有较好的频率分辨率特性.为此特引入窗口函数,并定义变换:

$$\psi_{a,b}(t) = |a|^{\frac{1}{2}}\psi\left(\frac{t-b}{a}\right). \tag{2}$$

信号 f 的连续小波变换定义为:

$$(W_\psi f)(a,b) = \langle f,\psi_{a,b}\rangle = |a|^{-\frac{1}{2}}\int_{-\infty}^{+\infty} f(t)\bar{\psi}\left(\frac{t-b}{a}\right)\mathrm{d}t. \tag{3}$$

这里$(W_\psi f)(a,b)$ 是小波系数,是关于尺度 a 和位置 b 的函数. "〈 〉"表示内积,$\bar{\psi}$ 是 ψ 的共轭复数. a 是尺度参数; $a \in R$ 并且 $a \neq 0$ 表示与频率相关的伸缩, b 是时间位置参数,通过伸缩尺度和移动参数 b,利用小波的带通特性是来分解不同速率的信号.变换结果可以把这组信号看作是窗口,通过这个窗口可以看到有趣的部分.如图 1 展示不同尺度参数 a 和位置参数 b 下的 Daubechies 小波(db3) 的变化.

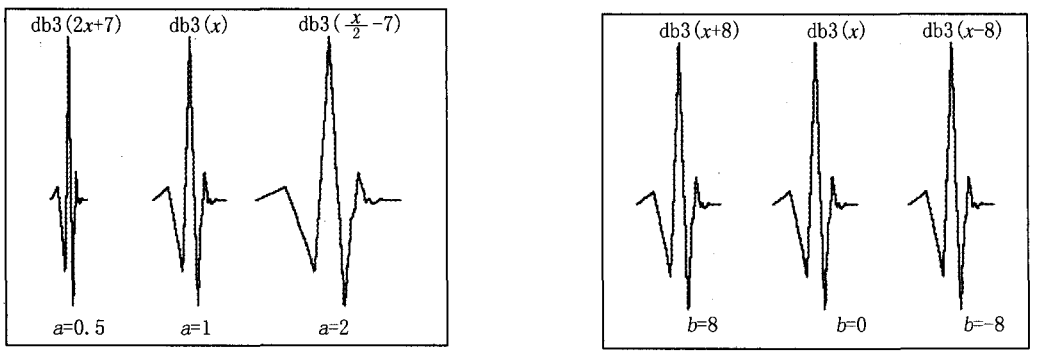


图 1 参数影响小波函数变化的例子

因为小波在函数图中的表达主要存在于有限的范围内的"波",若其傅里叶变换满足条件:

$$C_\psi = \int_R \frac{|\hat{\psi}(\omega)|^2}{|\omega|}\mathrm{d}\omega < +\infty, \tag{4}$$

被称为基本小波或母小波, $\hat{\psi}$ 就 ψ 的傅立叶变换.

对于公式(3),尺度参数 a 发生变化,带宽及带通滤波器中心频率也会发生变化.当 a 变小的时候,中心频率变大,同时带宽变大;反之,当 a 变大时,中心频率变小,同时带宽变窄.小波变换的特性对信号 f 的局部特性分析具有重要的应用价值.小波变换的带通滤波器相当于一个 a 变小情况.当尺度参数由小变大时,滤波器的范围从高到低的变化.因此,小波变换具有缩放功能.小波变换具有以下性质.

(1) 线性变换.小波变换是线性的,线性变换具有重叠的性质;

(2) 时间变换特性.如果 f 的连续小波变换是$(W_\psi f)(a,b)$,那么 $f(x-x_0)$ 的连续小波变换就是$(W_\psi f)(a,b-x_0)$;

(3) 尺度变换.如果 f 的连续小波变换$(W_\psi f)(a,b)$, 那么 $f\left(\frac{x}{\lambda}\right)$的连续小波变换就是$\sqrt{\lambda}(W_\psi f)\left(\frac{a}{\lambda},b\right)$.

除了满足许可条件,小波需要满足以下特性:函数 $\psi(t)$ 具有紧支撑特性,即在一个有限区间外的函数值为零.同时,该函数具有快速衰减特性来获得空间定位.对自然数 N,函数 $\psi(t)$ 具有 N 阶消失矩.

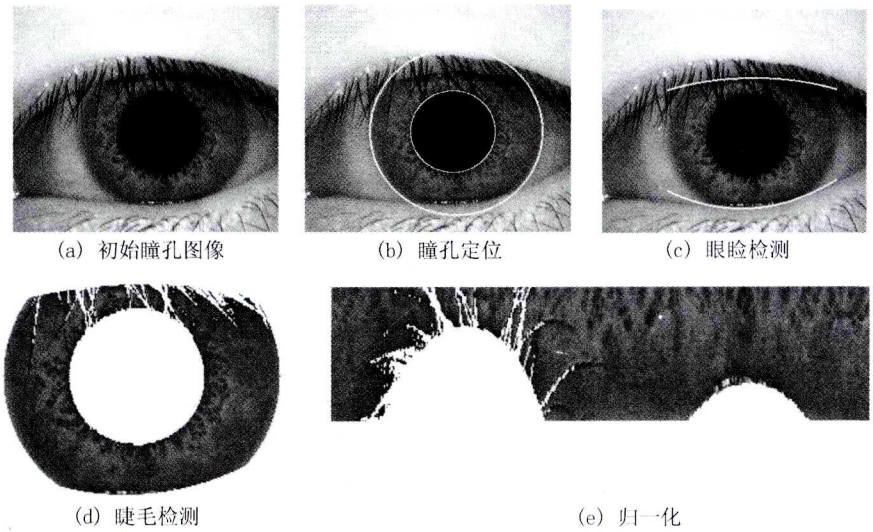
$$\int_{-\infty}^{+\infty} t^k\psi(t)\mathrm{d}t = 0, k = 0,1,\cdots,N-1, \tag{5}$$

随着消失矩 N 的增加,小波函数 $\psi(t)$受到的冲击也会相应增加.

1.2　虹膜特征提取

在提取特征之前，要进行虹膜图像的预处理，包括虹膜图像采集、虹膜定位、虹膜图像归一化[7]. 虹膜图像包括虹膜和眼睑、睫毛以及光点的干扰. 因此，虹膜需要进行归一化，以消除干扰. 将虹膜图像的形状规范化为固定大小的矩形，以比较不同的形状虹膜，如图 2 所示.

虹膜结构如图 3 所示. 虹膜区域内边缘的距离大约是 1.5 mm. 锯齿状的形状称为虹膜睫状区. 基于睫状区，虹膜大致分为两个部分：内部边缘附近的部分称为虹膜瞳孔，外缘附近的部分称为虹膜睫状体[8]. 因为瞳孔部分含有丰富的纹理细节，因此这个区域可以贡献更多的虹膜纹理特征识别.



(a) 初始瞳孔图像　(b) 瞳孔定位　(c) 眼睑检测

(d) 睫毛检测　(e) 归一化

图2 虹膜图像预处理

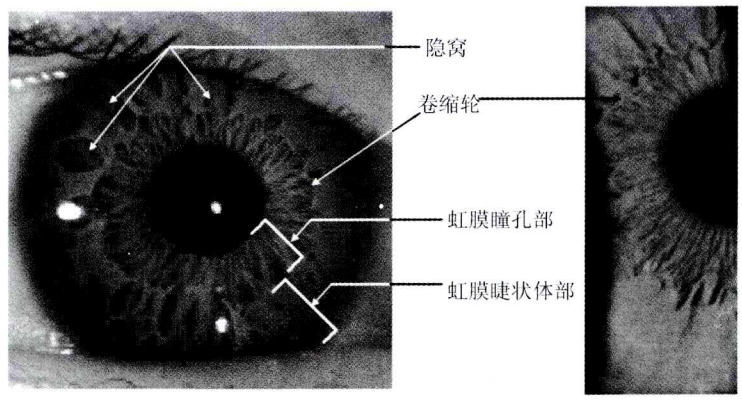


图3　瞳孔文本特征

图4 特征提取区域

通过虹膜图像预处理，得到了虹膜特征的归一化提取区域，如图 4 所示. 将图像分辨率被设置为 100×400，特征提取区域通常不小于归一化图像的 1/6，在这里，设置为 80×200. 目前虹膜特征提取算法大多基于经典的 Gabor 小波变换. 由于 db2 小波具有正交、紧凑和广义线性相位特性[9]，这里使用 db2 小波提取虹膜特征. 然后使用 db2 小波提取区域二维小波变换的三层变换，从而得到低频系数，水平高频系数、垂直高频系数和对角方向的高频系数，如图 5 所示. 由于虹膜纹理特征的细节丰富，主要表现为高频系数，第一、二级的

高频系数的数目较大,导致编码较长,识别效率将受到影响,而第三层的高频系数适中,适合作为虹膜特征.

(a) 垂直高频系数 (b) 水平高频的系数 (c) 对角高频系数

图5 第三层高频系数

第三层的各高频系数的容量为$(80\times200)/(2^3\times2^3)=250$,3 个方向的高频系数的容量为 $250\times3=750$,所提取的 750 个高频系数被随机映射函数生成 192 b 密钥的加密算法.

2 基于 AES 的图像加密算法

2.1 AES 加密算法

随着密码分析技术的发展和计算机运算性能的提高,美国国家标准研究所(NIST)1977 年颁布的 64 位密钥数据加密标准(DES)已经变得不安全. 1997 年,NIST 提出一个高级加密标准的收集行动,从众多加密算法中选择了由 Joan Daemen 和 Vincent Rijment 提出的 Rijndael 加密算法. 而 AES 由于它的独特性,成了 Rijndael 算法的代名词. AES 具有很强的灵活性,对其加密的明文块变量的大小可以是 128 b、192 b 或 256 b,可变密钥长度为 128 位、192 位或 256 位,密钥长度和迭代次数和明文块的大小密切相关,同 DES 相比,具有较高的安全性并且软件和硬件的运行速度更快. AES 以其较强的抗破解能力,没有密码分析攻击的方法可以破解 AES. 2001 年,AES 成了由 NIST 公布高级加密标准[10].

AES 算法是一种具有可变块明文长度和密钥长度的分组加密算法,同时,它是对称的加密算法,其加密和解密使用相同的密钥. 它的分组长度和密钥长度为 128 b,192 b 或 256 b. 让 N_b 代表明文分组长度 (1 word=4 B=32 b). N_k表示密钥的长度,加密轮数 N_r, 与 N_b 和 N_k 的关系如表 1 所示.

表 1 N_r,N_b和 N_k 之间的关系

N_r	N_b	N_k
10	4	4
12	6	4
14	8	4
12	4	6
12	6	6
14	8	6
14	4	8
14	6	8
14	8	8

每轮加密和解密 AES 变换包括替代、行移位、列混合和密钥加解密过程的操作,并由相应的逆运算.

2.2 图像加密原理

彩色图像大多采用 RGB 模式,可以看作是 R,B 叠加形成的. RGB 可以取从 0(黑色)到 255(白)值,与图像灰度值范围一致,因此对于灰度图像的加密方法也可以应用于彩色图像.

矩阵 $f(i,j)$,表示的灰度数字图像,图像大小是 $M\times N$,其中:$0\leq i\leq M-1$,$0\leq j\leq N-1$. $f(i,j)$表示图像 i 行 j 列的灰度值,共有 $2^8=256$ 级,取值范围是 $[0,255]$, 灰度图像的像素灰度值范围是一致的[11]. 因为 AES 算法在明文输入是字节,16 B 为矩阵基体元素,范围也是$[0,255]$. 因此,密钥的异或操作、位移、线性位移和列混合运算应用于灰度数字图像加密. 图像加密后,将具有以下功能:

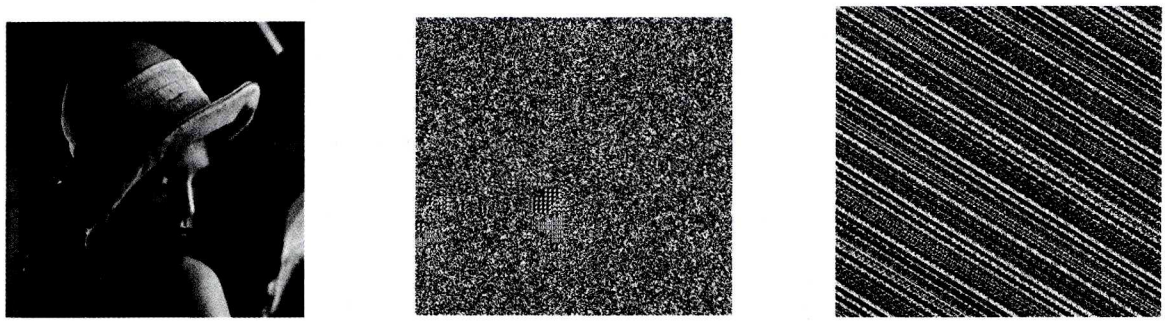
(1) 密钥异或操作实现像素的灰度值变换;

(2) 用替换操作来完成对图像像素灰度值的位移控制,以控制加扰;

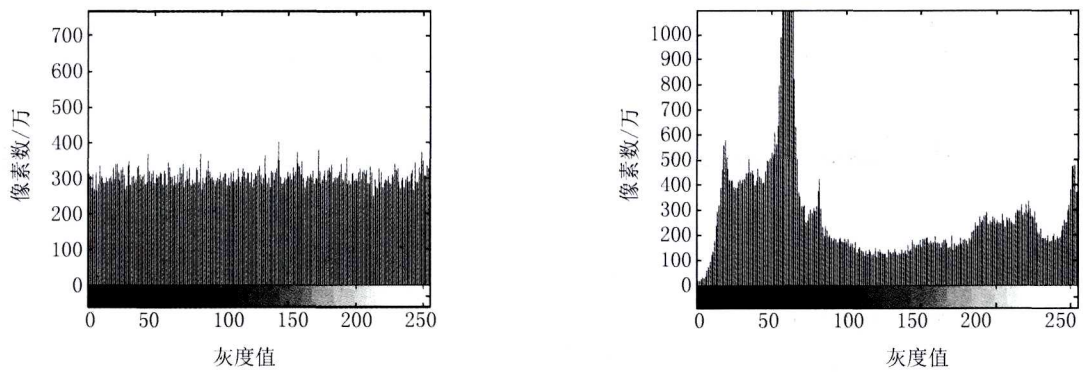
(3) 行移位和列混合被用来完成对高扩散的图像像素位置变换的加扰.

3　图像加密实验分析

使用经典 Arnold 变换对图 6(a)进行加密运算. 图 6(b)显示本文提出的图像加密效果. 图 6(c)显示 Arnold 变换迭代 10 次后的加密效果. 图 6 (d)是图 6 (b)的柱状图. 图 6 (e) 是图 6 (c)的柱状图.



(a)原始图像　　(b) 本文提出算法进行图像加密后的结果　　(c) Arnold变换图像加密后的效果



(d) 本文提出算法进行图像加密后的直方图　　(e) Arnold变换图像加密后的直方图

图6 本文提出算法与Arnold变换图像加密效果对比

按照置乱程度的定义，给出了通过上述两种算法计算图像加密的置乱程度.

$$\mu_i = \frac{\sigma^2_{\text{new}}}{\sigma^2_{\text{org}}} = \frac{5437.1}{977.4} \approx 5.56, \tag{6}$$

$$\mu_A = \frac{\sigma^2_{\text{new}}}{\sigma^2_{\text{org}}} = \frac{5070.4}{977.4} \approx 5.18. \tag{7}$$

μ_i 是本文提出算法的图像加密扰乱程度，μ_A 表示 Arnold 变换图像加密的扰乱程度，μ_i 要明显大于 μ_A. 同时，对加密图像直方图进行了分析，本文提出的图像加密算法的直方图在图像信号随机的情况下比 Arnold 变换更满意，因为加密图像的可读性越差，加密后的图像的还原性越小，图像的安全性越高. 根据上述分析，本文提出的加密算法的图像加密的安全性高于阿诺德变换.

4　结　论

本文提出虹膜特征密钥提取和 AES 加密算法相结合的图像加密算法，利用 db2 小波分解的虹膜区域，提取第三层的虹膜关键特征高频系数，详细分析了使用随机映射函数生成一个 192 b 的密钥的整个过程. 将该算法用于加密测试的图像，通过与经典的阿诺德变换的加密效果进行比较，实验结果表明，该算法的图像加密的安全性更高，保护图像信息效果更好.

参　考　文　献

[1]　Abraham D G, Dolan G M. Transaction Security System[J]. IBM Systems Journal, 2011, 30(2): 206-229.

[2] Monrose F, Reiter M K, Li Q, et al. Cryptographic key generation from voice[J]. IEEE Symposium on Security and Privacy, 2011, 5(11):202-213.

[3] Monrose F, Reiter M K, Wetzel R. Password hardening based on keystroke dynamics[J]. International Journal of Information Security, 2002,1(2):69-83.

[4] Charles C, Negar K, Dermis J. Secure Smartcard-Based Fingerprint Authentication[C]. ACM Workshop on Biometrics Methods and Application. California:Berkeley,1999:45-52.

[5] Davida G, Frankel Y, Matt B. On enabling secure applications through offline biometric identification[C]. Proceedings of IEEE Symposium on Security and Privacy. California:Oakland,2011.

[6] Lim S, Lee K, Byeon D. Efficient iris recognition through improvement of feature vector and classifier[J]. ETRI Journal,2001,23(2): 233-235.

[7] Tian Q C, Pan Q, Cheng Y. The experimental research on incomplete iris patterns and uniqueness[J]. Application Research of computers,2006,20(1):237-239.

[8] Tian Q C, Zhang R S. The overview of biological feature identification technology[J]. Research of computer application,2009,26(12): 4401-4410.

[9] Kee G,Byun Y,Lee K, et al. Improved Techniques for an Iris Recognition System with High Performance[C]. Australian Joint Conference on Artificial Intelligence, Adelaide,2001.

[10] Liu L H, Wen C J. AES differential-algebraic attacks[J]. Computer engineering and application,2010,46(5):111-113.

[11] Zhao Gang, Tang Zhen, Li Jianping. Encryption scheme of image key generation and Rijndael algorithm based on biometric characteristics[J]. Computer engineering and science,2009,31(12):11-12.

[12] Zhang H X, Qiu P L. The applications of scrambling technology in digital watermarking[J]. Journal of circuits and systems,2001,6(3): 33-36.

Image Encryption Research Based on Keys Generated by Iris Feature and AES Algorithm

XIE Ruiyun[1], HAI Benzhai[2]

(1. Computer Science and Technology Department, Henan Institute of Technology, Xinxiang 453000, China;
2. College of Computer and Information Technology, Henan Normal University, Xinxiang 453007, China)

Abstract: The encryption algorithm has disadvantages like the long key making memory difficult and uneasy safekeeping, which causes a potential threat to the information security. Based on the combination of iris feature key extraction and AES encryption algorithm, this paper proposes an image encryption algorithm, The algorithm uses DB2 wavelet decomposition of the iris region, extracting the third layer of the iris key features of high frequency coefficients, through the use of random mapping function to generate a 192 bit key. The algorithm and the classical Arnold algorithm are applied to image encryption experiments at the same time. Experimental results show that the security of the encrypted image is higher by using the algorithm.

Keywords: iris feature; wavelet transform; AES; image encryption