基于虹膜特征密钥的营房信息加密研究①

王 强, 易良廷

(后勤工程学院 军事工程管理系, 重庆 401331)

摘 要: 在军队后勤信息化建设中, 营房勤务信息化是重要的组成部分. 为解决营房信息化中信息安全面临的严峻形势和传统加密手段的安全隐患, 提出一种基于虹膜特征密钥的信息加密算法. 从人体虹膜中提取 375 位虹膜特征码, 然后从特征码中提取加密密钥用于营房信息加密. 实验结果表明, 加密信息的安全性得到了提高.

关键词: 虹膜特征; 密钥; 营房信息; 加密

Study on the Key Based on Iris Feature for Barracks Information Encryption

WANG Qiang, YI Liang-Ting

(Management Department of Military Engineering, Logistics Engineering University, Chongqing 401331, China)

Abstract: In the military logistics informatization construction, barracks service information is an important part.To solve severe situation of information security in barracks informatization and the safe hidden trouble from traditional encryption methods. a kind of information encryption algorithm based on the iris feature key is put forward, 375 iris codes is extracted from the human iris, then the encryption key used for the barracks information is extracted from iris codes. the experimental results shows that the security of the encrypted information is improved.

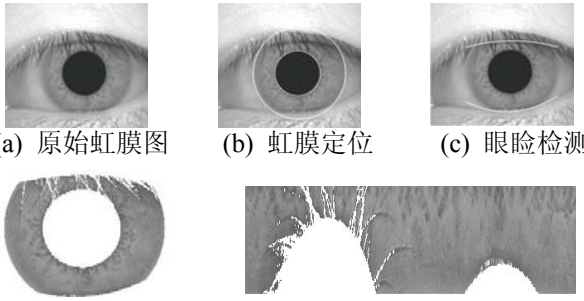
Key words: iris feature;key;barracks information; encryption

在军队营房信息化过程中, 营房保障效能的发挥越来越依赖于信息的获取, 而敌方“黑客”可以利用信息系统或者无线网络的漏洞绕过口令验证而直接窃取营房信息, 为保证营房信息在传输、转换和使用过程中不被敌方获取与使用, 必须采取数据加密算法对营房信息进行加密. 而现有加密算法如 AES 和 DES 等, 其密钥较长(128bit~256bit), 不便于记忆, 密钥通常会被用户存储在某一文件或装置中, 甚至直接存储在计算机硬盘上, 用户通过一个相对容易记忆的口令来释放密钥[1], 这样还是存在安全隐患. 针对这类安全隐患, 提出一种新的基于虹膜特征密钥的营房信息加密算法. 从人体虹膜特征中提取一定长度的 bit, 用于加密算法的密钥, 这样, 密钥来自于人自身, 且随身携带, 不须记忆, 解决了密钥保管问题. 实验结果表明, 基于虹膜特征密钥的加密算法, 在安全性上较经典 Arnold 置乱算法[2]高. 虹膜识别主要包括虹膜预处理、特征提取和模板匹配等步骤[3], 虹膜预处理是虹膜特征提取的基础, 而特征提取是虹膜识别的核心工作, 也是密钥生成的关键. 本文采用二维小波变换提取虹膜特征, 将提取的虹膜特征用于营房信息加密, 取得了满意的效果.

1 虹膜预处理

虹膜预处理包括图像采集、虹膜定位、归一化步骤. 采集的原始人眼图像除虹膜外, 还包括瞳孔、眼睑和睫毛, 所以需要虹膜定位提取虹膜环状纹理, 并且去除睫毛、眼睑和光斑等干扰. 为克服瞳孔缩放等因素引起的差异, 便于比对, 将虹膜图像归一化为固定大小的矩形图像. 虹膜定位采用文献[4]算法, 睫毛、眼睑和光斑干扰检测采用文献[5]算法, 归一化采用文献[6]中的“橡皮板”模型. 图 1 为虹膜预处理过程.

① 收稿时间:2013-01-30;收到修改稿时间:2013-04-01



(a) 原始虹膜图　(b) 虹膜定位　(c) 眼睑检测

(d) 睫毛检测　(e) 归一化

图 1　虹膜预处理

2　图像的二维离散小波变换

二维离散小波变换将图像分解成近似分量和细节分量. 分解的尺度函数 $\varphi_{j,m,n}(x,y)$ 和小波函数 $\psi^i_{j,m,n}(x,y)$ 为:

$$\varphi_{j,m,n}(x,y)=2^{j/2}\varphi\left(2^j x-m,2^j y-n\right) \tag{1}$$

$$\psi^i_{j,m,n}(x,y)=2^{j/2}\varphi^i\left(2^j x-m,2^j y-n\right),i=\{H,V,D\} \tag{2}$$

(2)式中的 i 标识三个方向敏感性小波, 度量不同方向图像强度的变化, H 为水平方向,V 为垂直方向,D 为对角线方向.

尺寸为 M×N 的图像 f(x,y)的二维离散小波变换为:

$$W_\varphi(j_0,m,n)=\frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\varphi_{j,m,n}(x,y) \tag{3}$$

$$W^i_\psi(j,m,n)=\frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\varphi^i_{j,m,n}(x,y),i=\{H,V,D\} \tag{4}$$

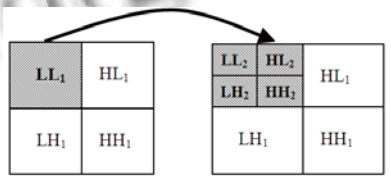
j_0 是任意的起始尺度, 一般选 j_0=0, $W_\varphi(j_0,m,n)$ 定义了在尺度 j_0 的近似系数, $W^i_\psi(j,m,n)$ 对于 $j\ge j_0$ 定义了不同方向的细节系数, 一般选择 N=M=2^J, j=0,1,2, , J-1, m,n=0,1,2, , 2^j-1.

对图像进行二维离散小波变换是从高尺度向低尺度进行的, 如图 2 所示, 每一级小波分解得到近似系数 LL(对应 W_φ), 以及细节系数 HH,HL 和 LH(分别对应 W^D_ψ,W^H_ψ,和 W^V_ψ);而下一级的分解是在上一级的低频系数 LL 上展开的, 类似对 LL 进一步分解可以得到更低尺度下的系数[7].

3　虹膜特征提取

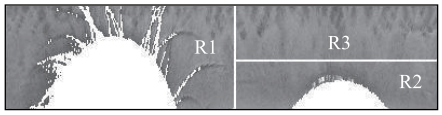
对虹膜归一化图像分析, 如图 3(a)所示, *R*1 区域受上眼睑和睫毛干扰较严重, *R*2 区域受下眼睑干扰, 且虹膜纹理主要集中在靠近瞳孔的区域, 所以选择归一化图像的右上部 *R*3 区域为特征提取区域, 归一化图像大小为 100400, *R*3 区域大小一般不小于归一化图像大小的 1/6[8], 这里取 40×200.

现有大多文献采用 *Gabor* 小波提取虹膜特征, 为了提高编码效率, 本文采用最简单的 *Haar* 小波提取特征, 同时 *Haar* 小波具有正交性、紧致性及广义线性相位[9]特点. 对 *R*3 区域利用图 3(b)所示二维 *Haar* 小波进行三级分解, 得到近似系数 LL_3, 水平细节系数 $LH=\{LH_1,LH_2,LH_3\}$、垂直细节系数 $HL=\{HL_1,HL_2,HL_3\}$ 和对角细节 $HH=\{HH_1,HH_2,HH_3\}$. 如 3(c)所示.

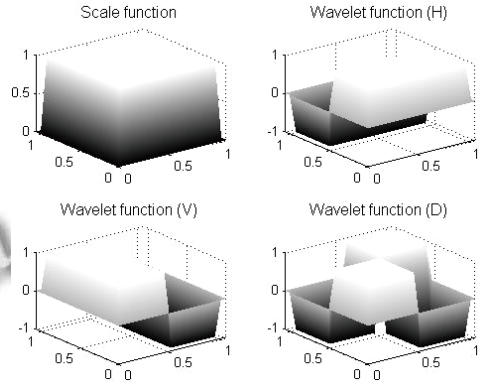


(a) 第一级小波分解　(b) 第二级小波分解

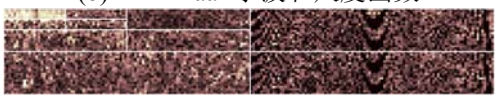
图 2　图像小波分解示意



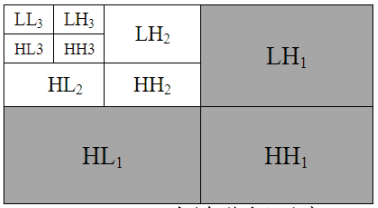
(a)　特征提取区域选取



(b)　2D Haar 小波和尺度函数



(c)　R3 区域 Haar 小波分解序列子图像



(d)　Haar 小波分解示意

图 3　虹膜特征提取

虹膜纹理信息主要集中在细节系数上, 如果把第一或第二层的细节系数作为特征, 导致特征空间过大, 会影响编码效率, 经过大容量样本实验, 发现提取第三层的细节系数 LH_3, HL_3 和 HH_3 作为特征较合适, 每个细节系数大小为$(40\times200)/(2^3\times2^3)=125$, 三个方向的高频分量大小为 $125\times3=375$.

对这 375 个小波系数分析, 有正有负, 而小波系数表示小波与信号的相似程度[10], 正小波系数与负小波系数描述的相似程度截然不同, 故利用该性质对 375 个特征系数进行二进制编码. 设 C={LH_3, HL_3, HH_3}为虹膜特征空间, 特征空间元素 C(i)的编码规则为:

$$\begin{cases} C(i)=0 & if C(i)\le 0 \\ C(i)=1 & if C(i)\ge 0 \end{cases} \quad (5)$$

通过以上编码方式, 共形成 375bits 的虹膜特征码, 与 Daugman 的 2048bits 虹膜特征制码相比, 提高了编码效率, 特征空间比较紧凑, 节省了模板存储空间. 与 Lim 的 87bits 虹膜特征码相比, 更加充分描述了纹理特征.

4 加密密钥提取

采用以下随机函数从所提取的虹膜特征码中生成密钥.

$$f(j)=[(m-j+z_r)\bmod m]+1, z_r\in Z \quad (6)$$

j 为虹膜特征码序列的下标, z_r 定义为伪随机整数且 0<zr<107. m 为虹膜特征码长度, 这里是 375. 选取 AES 密钥长度为 128bit, 即 n=128. 通过(6)式映射得到 128bit 密钥, 如图 4 所示.

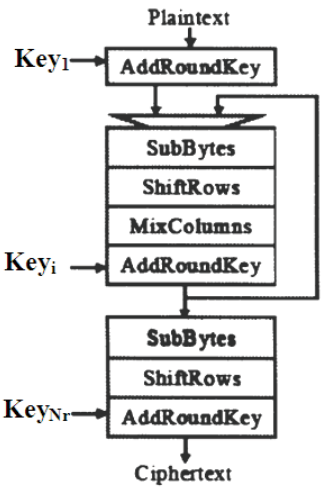
```
P1 =
 Columns 1 through 25
  0  0  0  1  1  0  0  0  0  0  1  0  0  1  0  1  1  0  0  0  0  1  0  1  0
 Columns 26 through 50
  1  1  0  1  0  0  1  1  1  1  0  1  0  0  0  1  1  0  1  1  1  0  0  1  0
 Columns 51 through 75
  1  0  0  1  0  1  1  0  1  0  0  1  0  1  1  1  1  1  0  0  0  1  1  1  1
 Columns 76 through 100
  1  0  1  0  1  1  0  1  0  1  0  1  0  1  0  0  0  0  0  1  0  1  0  0  1
 Columns 101 through 125
  0  0  0  1  1  1  0  1  1  1  1  0  0  0  0  0  0  0  1  0  1  0  0  1  0
 Columns 126 through 128
  0  0  1
```

图 4 从虹膜特征码中提取的 128bit 密钥

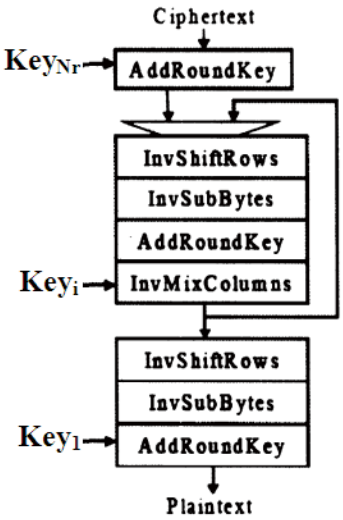
5 基于虹膜特征密钥的信息加密过程

AES 算法是一种明文分组长度和密钥长度均可变的分组加密算法, 同时也是对称加密算法, 其加、解密过程如图 5 所示. 其加密和解密使用的密钥相同, 其分组长度和密钥长度都分别可为 l28 位、l92 位或 256 位[1].

设一幅灰度数字图像可用矩阵 $f(i, j)$表示,图像的大小为 $M\times N$, 其中 $0\leqslant i\leqslant M-1$,$0\leqslant j\leqslant N-1$. $f(i,j)$表示图像在第 i 行第 j 列处像素的灰度值,共有 28=256 个等级,取值范围是[0～255]. 由于 AES 算法中的明文输入是以字节为元素的 16 字节矩阵, 矩阵元素的取值范围也是[0～255],这与灰度图像像素的灰度值范围一致. 因此,本文将 AES 算法中的密钥异或、字节代换、行移位和列混淆应用到数字图像加密中,主要包括三部分内容: (1)利用密钥异或实现图像像素变换; (2)利用字节代换来完成图像像素的替代,起到混乱的作用; (3)采用行移位和列混淆来完成图像像素的置换,起到混乱之上的高度扩散[11].



(a) 加密过程



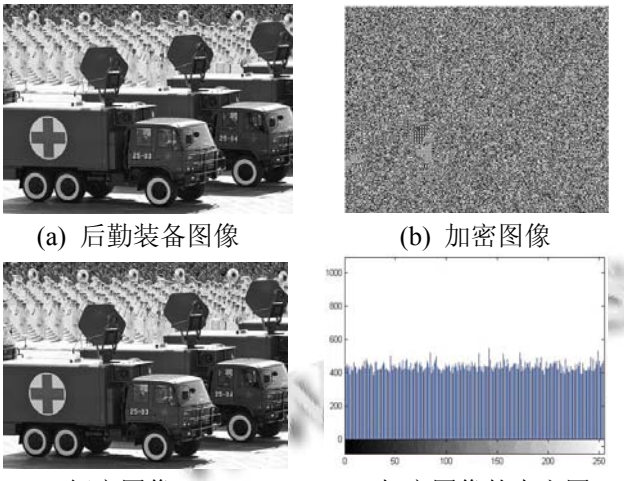
(b) 解密过程

图 5 AES 加解密过程

6 加密效果与分析

6.1 加密效果分析

利用所提取的 128 位密钥充当 AES 密钥对野营装备图像加密, 明文分组为 128 位(16 字节), 对于图像就是以 4×4 像素子块为加密分组. 实验结果如图 5 所示. 野营装备图像大小为 400 像素×280 像素.



(a) 后勤装备图像　(b) 加密图像

(c) 解密图像　(d) 加密图像的直方图

图 6　野营装备图像加密效果

对图 6(d)分析, 加密图像的直方图分布较平坦, 接近均匀分布, 那么可以认为图像信号比较随机, 加密图像的可读性越差, 还原的可能性就更小了, 也就是说加密后图像更安全.

6.2 与 Arnold 变换加密安全性的比较

采用 Arnold 变换[9]对图 6(a)所示野营装备图像进行置乱加密, 由于 Arnold 变换要求输入图像为方阵图像, 所以在图 6(a)中截取带有重要信息的图像方块(280 像素×280 像素).

根据置乱度定义分别计算两种算法加密图像后的置乱度.

$$\mu_{iris}=\frac{\sigma^2_{new}}{\sigma^2_{org}}=\frac{5437.1}{977.4}=5.56 \tag{7}$$

$$\mu_{Arnold}=\frac{\sigma^2_{new}}{\sigma^2_{org}}=\frac{5070.4}{977.4}=5.18 \tag{8}$$

μ_{iris} 为本文提出算法加密图像后的置乱度, μ_{Arnold} 为 Arnold 变换加密图像后的置乱度. 本文算法加密图像后的置乱度 μ_{iris} 大于 Arnold 变换加密图像后的置乱度 μ_{Arnold}, 根据置乱度定义, 置乱度值越大, 表示加密信息越不容易破解, 加密安全性越高[12]. 本文提出的加密算法在加密安全性上较 Arnold 变换高.

7 结语

针对营房信息化中面临的信息安全问题, 提出一种基于虹膜特征密钥的营房信息加密算法, 经过虹膜采集、预处理与特征提取阶段后, 从人体虹膜中提取 375 位虹膜特征码, 然后从特征码中提取加密密钥用于营房信息加密, 实验结果表明, 在加密信息安全性上较经典 Arnold 置乱加密算法高.

参考文献

1 Spillman R. 经典密码学与现代密码学.北京:清华大学出版社,2005.133−145.

2 Abraham DG, Dolan GM, Double GP, Stevens JV. Transaction Security System,IBM Systems J,1991,30(2):206−229.

3 Monrose F, Reiter MK, Li Q, Wetzel S, et al. Cryptographic key generation from voice.IEEE Symposium on Security and Privacy,2001:202−213.

4 周俊,李王辉,罗挺,杨眉.快速准确的虹膜定位算法.计算机工程与设计,2010,31(18):4058−4061.

5 Bowyer K, Hollingsworth K, Flynn P. Image understanding for iris biometrics:a survey. Computer Vision and Image Understanding,2008:281−307.

6 Daugman J. New Methods in Iris Recognition. IEEE Transactions on Systems, Man, and Cybernectics—Part B: Cybernectics,2007,37(5):1167−1174.

7 杨建国.小波分析及其工程应用.北京:机械工业出版社,2007.

8 田启川,潘泉,程咏梅,张洪才.不完全虹膜模式唯一性实验研究.计算机应用研究,2006:237−239.

9 陈珂.基于 Rijndael 的彩色图像加密算法的研究.计算机工程与设计,2007,28(20):4908−4910.

10 L.Ma & T.Tan & Y.Wang,et al.Personal Recognition Based on Iris Texture Analysis,IEEE Transactions on Pattern Analysis and Machine Intelligence,2003,25(12):1519−1533.

11 赵刚,唐真,李建平.基于生物特征的密钥生成和 Rijndael 算法的图像加密方案.计算机工程与科学,2009,31(20):11.

12 柏森,廖晓峰.基于 Walsh 变换的图像置乱程度评价方法.中山大学学报(自然科学版),2004,43(S2):58−61.