文章编号:1671-4598(2016)06-0164-04 DOI:10.16526/j.cnki.11—4762/tp.2016.06.045 中图分类号:TP309.7 文献标识码:A

基于手指静脉特征图像的加密研究

陈 暄
(浙江工业职业技术学院,浙江 绍兴 312000)

摘要:移动互联下的信息安全是目前研究的热门,提出从手指静脉图像的加密出发,首先对手指静脉图像的特征进行了提取,通过构建图像平滑器来获得静脉图像的大小,明暗区域的选择和特征图像的加强来获得采集后的静脉特征图像,其次对静脉图像采用基于小波基函数,Arnold 映射,二次 Logistic 映射和 Baker 变换的混合加密方式对进行加密;在相关系分析和差分攻击分析等方面实验比较,说明算法具有很好的安全性和低耗时性,能够完全适应在移动互联环境中推广。

关键词:手指静脉特征图像;加密;移动互联

Research on Encryption Based on Finger Vein Feature Image

Chen Xuan
(Zhejiang Industry Polytechnic College, Shaoxing 312000, China)

Abstract: Information security in the mobile Internet is currently a hotspot in researches. Starting from encryption of finger vein image, this paper first extracts characteristics of the finger vein image, and gets the size of vein image through establishing image smoother as well as the collected image of vein features through selecting the darkness area and characteristic features. Then, this paper adopts the function based on wavelet, Android mapping, the quadratic Logistic mapping and Baker transform to encrypt the vein image. Conduct experiment to compare the correlation analysis and differential attack analysis, and the results show that algorithm in this paper is safe and costs less time, so it is suitable to promote it in the mobile Internet.

Keywords: finger vein feature image; encryption; mobile Internet

0 引言

移动互联网相比目前的互联网在信息的获取和传播上会变得更加快捷和方便,越来越受到人们的广泛应用,但由于受到来自网络安全等方面的影响[1],图像加密一直是数据加密研究方向之一[2],其中手指静脉图像加密需要引起重视,因为存在会被劫持并篡改的可能性。国内外学者对此从多个角度对图像加密进行了研究。文献[3-7]提出利用通过 Logistic 映射或者混沌系统产生一组伪随机序列,最终得到加密图像;文献[8-9]提出基于 Chen 映射构造 X、Y、Z 共 3 个方向上的混沌序列。实验证明该算法用于图像快速加密是可行、有效的;文献[10]提出基于稀疏矩阵的 Arnold 数字图像加密算法的安全性,利用图像分层及三层加密结构的思想来加以改进,提出了安全性提升算法 SMA,实验表明,与已有的 Arnold 数字图像加密算法进行对比时,该算法具有更高的安全性。

本文的研究分为 2 个部分,第一个部分首先通过特征获得图像,采用构建图像平滑器,然后针对静脉图像的区域明暗进行特征提取以获得完整的静脉特征图像,第二部分是针对已经获得的图像采用其次对静脉图像采用基于小波基函数,Arnold 映射,二次 Logistic 映射和 Baker 变换的混合加密方式对进行加密。仿真实验证明本文的算法具有很好的安全性。

1 静脉图像的获取和处理

1.1 构建图像平滑器

静脉图像的单一结构无法能够在移动互联网中进行传输,因此需要完全构建图像平滑器来存储静脉的有效信息,本文在 4 个 4×4 的结构单元基础上,构成 1 个 8×8 图像平滑器,如图 1 所示。

0	0	0	0	1	0	0	0
1	1	1	1	0	1	0	0
1	1	1	1	0	0	1	0
0	0	0	0	0	0	0	1
0	0	0	1	0	1	1	0
0	0	1	0	0	1	1	0
0	1	0	0	0	1	1	0
1	0	0	0	0	1	1	0

图 1 8×8 的图像平滑器

通过图像平滑器对静脉图像 f 进行膨胀运算,分别得到 4 个子图像 f_a,f_b,f_c,f_d,然后通过加权重构图像,其中 α,β,κ,ρ 分别代表每一个子图像中的权值值,且大于等于 0 之和为 1,如公式(1)所示:

$$\begin{cases} f = \alpha \times f_1 + \beta \times f_2 + \kappa \times f_3 + \rho \times f_4 \\ st \quad f_1 = f \oplus f_a \\ \quad f_2 = f \oplus f_b \\ \quad f_3 = f \oplus f_c \\ \quad f_4 = f \oplus f_d \end{cases} \tag{1}$$

1.2 静脉图像的明暗区域的提取

静脉图像中存在明暗区域,为了能够获得区域的特征信息,本文设计一种尺寸递增的结构序列 $\{\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_i\}$,对于每一个单位尺寸图像进行自我膨胀,得到 $\varepsilon_i = \overbrace{\varepsilon_1 \oplus \varepsilon_1 \oplus \cdots \oplus \varepsilon_1}^{i}$ $(i \leqslant t)$。将单位尺寸不断地进行变换从而提取不同的图像细节特征,本文通过白变换(White top-hat)和黑变换(Black top-hat)来获得。

收稿日期:2015-11-30; **修回日期**:2016-01-04。
基金项目:浙江省教育厅科研课题(Y201534058)。
作者简介:陈 暄(1979-),男,硕士,讲师,主要从事算法设计和云计算方向的研究。

1）White top-hat 变化公式：

$$White\ top-hat_i = f\times(1-\varepsilon_i) \tag{2}$$

$White\ top-hat_i$ 表示通过 ε_i 对静脉图像 f 在第 i 维上进行白变换。$White\ top-hat_{i(i-1)}$ 表示在静脉图像 f 的尺寸在两个相邻的尺寸上的亮区域的细节，公式如（3）所示，提取静脉图像中的明亮区域的信息如公式（4）所示：

$$White\ top-hat_{i(i-1)} = White\ top-hat_i \cap White\ top-hat_{i-1} \tag{3}$$

$$f_W = \sum_{i=0}^{k} White\ top-hat_i/k + \sum_{i=1}^{k} White\ top-hat_{i-1}/(k-1) + \sum_{i=1}^{k} White\ top-hat_{i(i-1)}/k(k-1) \tag{4}$$

f_W 表示在图像在 0～k 维度上的亮区域特征的白变换的结果。

2）Black top-hat 变换公式：

$$Black\ top-hat_i = f\times(\varepsilon_i-1) \tag{5}$$

$White\ top-hat_i$ 表示通过 ε_i 对静脉图像 f 在第 i 维上进行黑变换。$White\ top-hat_{i(i-1)}$ 表示在静脉图像 f 的尺寸在两个相邻的尺寸上的暗区域的细节，公式如（6）所示，提取静脉图像中的暗区域的信息如公式（7）所示：

$$Black\ top-hat_{i(i-1)} = Black\ top-hat_i \cap Black\ top-hat_{i-1} \tag{6}$$

$$f_B = \left(\sum_{i=0}^{k} Black\ top-hat_i\right)/k + \left(\sum_{i=1}^{k} Black\ top-hat_{i-1}\right)/(k-1) + \left(\sum_{i=1}^{k} Black\ top-hat_{i(i-1)}\right)/k(k-1) \tag{7}$$

式中，f_B 表示在图像在 0～k 维度上的亮区域特征的黑变换的结果。

1.3　静脉图像的增强

为了进一步增强获得静脉图像的效果，本文将静脉原始图像 f、白区域 f_W 和黑区域 f_B 在 [0,1] 区间上进行映射，得到如下。

$$\begin{cases}\overrightarrow{f_L(x,y)} = f(x,y)/L\\ \overrightarrow{f_{WL}(x,y)} = f_W(x,y)/WL\\ \overrightarrow{f_{BL}(x,y)} = f_B(x,y)/BL\end{cases} \tag{8}$$

式（8）中，$\overrightarrow{f_L(x,y)}$，$\overrightarrow{f_{WL}(x,y)}$，$\overrightarrow{f_{BL}(x,y)}$ 分别表示对不同对象的映射后的结果。使用增强算子对静脉原始图像 f_L 进行非线性变换，变换后的结果记为 f'_L，k 为中间临界点，如公式（9）。

$$f'_L(x,y) = G(f_L(x,y)) = \begin{cases}f_L(x,y)^2, & 0\leqslant f_L(x,y)\leqslant k\\ 1-f_L(x,y)^2, & k<f_L(x,y)\leqslant 1\end{cases} \tag{9}$$

利用式（10）得到静脉图像的明暗差值，记为 f_{diff}（x，y）。

$$f_{diff}(x,y) = f_{WL}(x,y) - f_{BL}(x,y) \tag{10}$$

实际中，使用 $f_{diff}(x,y)$ 直接和 f'_L 进行相加效果并不明显。因此需要设置一个系数 s 来弥补差值的影响，f_{en} 表示增强后的图像，如公式（11）所示：

$$f_{en}(x,y) = f'_L(x,y) + s\times f_{diff}(x,y) \tag{11}$$

1.4　小波基函数的选择

针对手指静脉图像的特征，本文选择小波基函数对其进行处理，通过伸缩和平移等运算功能对函数或信号进行多尺度细化分析，非常适合于局部分析。通过小波基函数将静脉图像划分为同等大小的图像，都有一个独立的小波切换块对应相应的图像。小波基函数如下：

$$h_{a,b}(x) = h\left[\frac{x-b}{a}\right]$$

$$s.t\ h(x) = \cos\left(\frac{x}{4}\right)\cdot\exp(-x^2/2) \tag{12}$$

式中，a 为伸缩因子，b 为平移因子。

2　基于混沌的静脉图像的加密

2.1　Arnold 映射

利用混沌系统的初始值来进行迭代对明文的图像进行置换是一种加密手段，本文采用 Arnold 映射方法是混沌图像加密的重要组成部分，其中映射公式如下：

$$\begin{bmatrix}x_{n+1}\\ y_{n+1}\end{bmatrix} = \begin{bmatrix}1 & a\\ b & ab+1\end{bmatrix}\begin{bmatrix}x_n\\ y_n\end{bmatrix}\bmod N,\quad x_0,y_0\in\{0,1,2,\ldots\ldots N-1\} \tag{13}$$

式（13）中，a，b 为正整数，Arnold 映射对二维可逆图像进行了正整数的限制，使得原本静脉图像中相邻的像素点通过变换之后不再相邻。首先将静脉图像中某个点 (x,y) 处的像素值进行随机处理得到一个新位置，然后通过 Arnold 映射变换后的点 (x_{n+1},y_{n+1}) 来取代 (x,y) 作为下一次变换移动的输入值，直到迭代结束完成置换了一副图像。其缺点是静脉图像的有限迭代后容易可能出现恢复图像的情况，因此保密性具有一定的差异。

2.2　二维 Logistic 映射和 Baker 变换

$$\begin{cases}x_{n+1} = x_n + h(x_n + y_n - x_n^2)\\ y_{n+1} = y_n + h(y_n + x_n - y_n^2)\end{cases} \tag{14}$$

当 $h\in[0.653,0.686]$ 的时候，Logistic 处于二维混沌状态。

Baker 映射是数据置乱的方式一种。二维连续的 Baker 变换的表达式如式（15）：

$$\begin{cases}B(x_{n+1},y_{n+1}) = k(2x_n,\frac{y_n}{2}), & x_n\in[0,1/2]\\ B(x_{n+1},y_{n+1}) = k(2x_n-1,\frac{y_n+1}{2}), & x_n\in[1/2,1]\end{cases} \tag{15}$$

其中：(x_n,y_n) 记录着原始数据的位置，(x_{n+1},y_{n+1}) 记录着置乱后的数据位置。

本文将以上两种数据置换的方式进行结合，设计了混合混沌序列构造器，其中，密钥初值通过二维 Logistic 进行置换，原始图像通过 Bakert 置换后与经过处理的密钥通过矩阵进行扩散操作，最后生成加密图像，二者混合加密序列如图 2 所示。

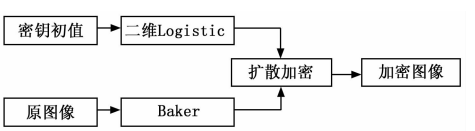


图 2　二者混合加密序列

3　加密算法设计

本文加密算法的设计主要将小波基函数，Arnold 映射，二维 Logistic 映射和 Baker 变换这四者结合起来，通过对静脉图像进行分解，置换，扩散等方面进行处理最后得到加密的图像，其流程如图 3 所示。

本文首先对原始静脉图像进行分解成矩阵（$M/4$）×（$N/4$），然后通过 Baker 序列和经过 Logistic 混沌后的密钥生成混沌序列，小波基函数对图像进行小波分解可以获得分解系

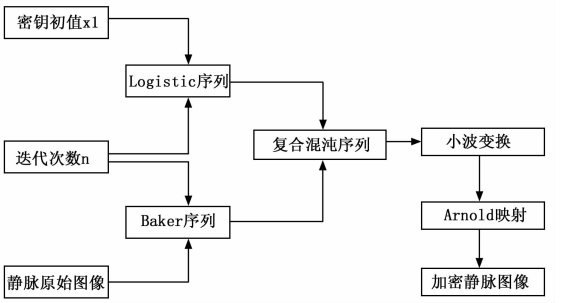


图 3 本文加密流程

数矩阵，对分解后的矩阵采用 Arnold 映射，这样能够有效的在一定程度上可以减少计算量，因此在加密设计上是合理的。

算法步骤如下：

步骤 1：设定一个大小为 $M\times N$ 的静脉图像，将其转换为图像的二维矩阵为 $\boldsymbol{R}$，使用 Baker 对其预处理图像进行 n 次预处理，生成序列 X。

步骤 2：针对密钥，通过（14）迭代映射变换 $M\times N$ 次，生成 $M\times N$ 对混沌序列值，通过对密钥进行异或 B 操作，$B=\bigoplus_{i=1}^{m}\bigoplus_{j=1}^{n} I(M,N)$，从而完成对密钥的混沌加密。

步骤 3：通过 n 次迭代，对步骤 1 中的置换图像 X 和步骤 2 中的 Logistic 密钥生成序列 Y 进行复合混沌序列分解。

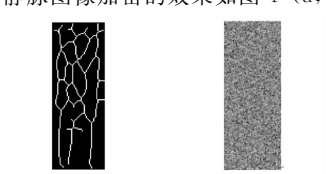
步骤 4：将生成的混合混沌序列进行小波基函数进行变换，生成序列 Z。

步骤 5：使用 Arnold 映射对 Z 产生混沌序列得到 Z'，通过与步骤 4 中的图像序列 Z 进行置换。

将置换后的静脉图像进行小波逆变换，得到最终加密的图像。

4 仿真实验

本文设置硬件环境为酷睿双核，内存为 4 GDDR3，硬盘容量为 240 G，软件仿真环境为 Matlabs2010。选取原始的手指静脉图像，然后对其按照第 1 节描述的静脉特征方法进行提取，如图 4 所示。本文从相关性分析和统计计分析 2 个方面分析来进行验证对手指静脉图像加密的效果如图 4（a，b）中所示。



(a) 采集后的图像 (b) 加密后的图像

图 4

4.1 相关性分析

与其他的图像一样，手指静脉图像中也会包含相关的冗余的信息，虽然通过前述的方法提取图像特征，但相邻的像素点之间无法独立的存在一定的相关性，从采集后的静脉图像和密文图像中随机选择 100 对相邻像素点，按照公式（16）～（19）来计算加密后的图像的水平方向，垂直方向，对角线方向像素相关性，其中 Cov 表示协方差，(x,y) 表示静脉图像中的相邻像素点的灰度值，N 为挑选的像素个数。

$$E(x)=\frac{1}{N}\sum_{k=1}^{N}x_k \tag{16}$$

$$D(x)=\frac{1}{N}\sum_{k=1}^{N}(x_k-E(x)) \tag{17}$$

$$Cov(x,y)=\frac{1}{N}\sum_{k=1}^{N}(x_k-E(x))(y_k-E(y)) \tag{18}$$

$$r(x,y)=\frac{|Cov(x,y)|}{\sqrt{D(x)}\sqrt{D(y)}} \tag{19}$$

表 1 分别列出了加密前后两种图计算所得到的相关系数，从中发现两种之间的相关性比较大，说明采集后的手指静脉的图统计特征已经被扩散到了随机的加密图中。表 2 列出了加密前后的两种图像算法在时间复杂度上的比较，说明本文加密算法后时间复杂度低于未加密算法 31.21%。图 5～7 表示两种图像在 3 个方向上的比较效果，从结果来看，针对采集后的静脉图像加密效果比较好，适合在移动互联的条件下加密。

表 1 采集静脉图与加密图的两相邻像素相关性

方向	采集图	密图
水平方向	0.826 2	0.003 2
垂直方向	0.873 5	0.002 7
对角方向	0.917 3	0.002 4

表 2 采集静脉图与加密图的时间复杂度比较

方向	采集图/%	密图/%
水平方向	75.25	37.25
垂直方向	62.75	33.25
对角方向	89.27	63.14

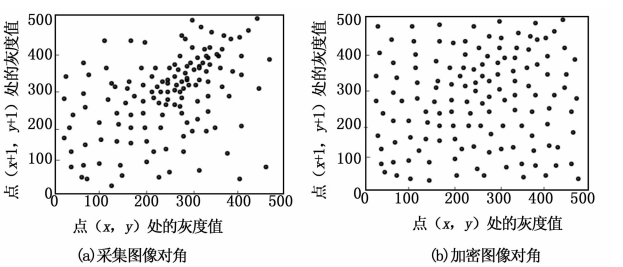


图 5 效果比较图

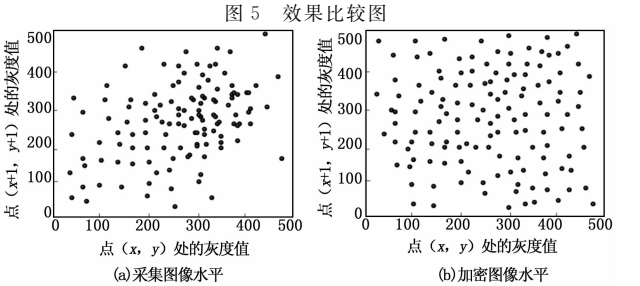


图 6 效果比较图

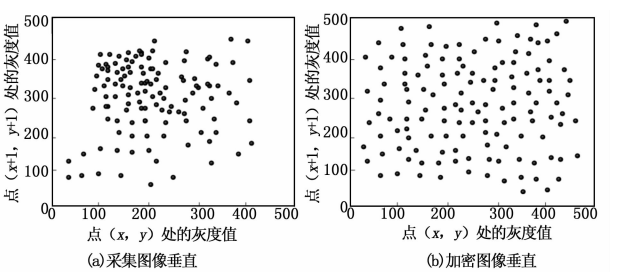
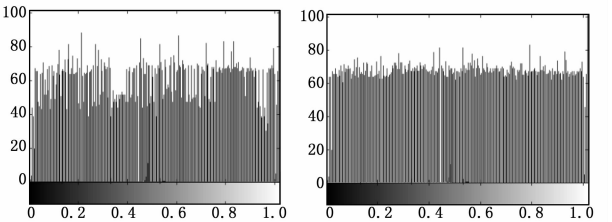


图 7 效果比较图

4.2 统计分析

图 8 显示的文献［9］的效果与本文算法加密的效果比较，

从图中效果来看，本文的算法相比与文献［9］的算法加密之后图像具有很好的稳定性，图像灰度值优于文献［9］的图像灰度直方图，这说明通过在二维 Logistic 的基础上，结合 baker 加密，具有很好的效果。



(a)文献[7]的手指静脉图像灰度图　　(b)本文算法的手指静脉图像灰度图

图 8　效果比较图

5　结束语

本文首先对手指静脉图像的特征进行了提取，其次对静脉图像采用基于小波置换，Arnold 映射，二次 Logistic 映射和 Baker 变换的混合加密方式对进行加密。仿真实验证明本文的加密算法相关系分析和差分攻击分析等方面具有很好的安全性和低耗时性，能够完全适应在移动互联网环境中推广。

参考文献：

[1] 房秉毅，张云勇，吴　俊，等. 云计算应用模式下移动互联网安全问题浅析［J］，电信科学，2013，29（3）：41－46.

[2] 文昌辞，王　沁，苗晓宁，等. 数字图像加密综述［J］. 计算机科学，2012，39（12）：6－8.

[3] 何　冰，牛怀岗，肖令禄. 一种双重变换的二维图像加密算法［J］. 光学技术，2015，41（1）：52－58.

[4] 王　帅，孙　伟，郭一楠. 一种多混沌快速图像加密算法的设计与分析［J］. 计算机应用研究，2015，32（2）：512－515.

[5] 徐　兵，袁　立. 基于改进 Logistic 混沌映射的数字图像加密算法研究［J］. 计算机测量与控制，2014，22（7）：2157－2159.

[6] 丁文珂，张　颖，柴秀丽. 基于自适应和多混沌系统的彩色图像压缩加密算法［J］. 河南大学学报（自然科学版），2015，45（2）：223－228.

[7] 浩　明. 基于多个混沌系统和位运算的图像加密算法［J］. 实验室研究与探索，2015，34（3）：35－39.

[8] 彭　平，孙立新，王铁柱. 基于 Chen 混沌映射的位平面图像加密方法［J］. 数学的实践与认识，2015，45（3）：117－122.

[9] 李巧君，张亚楠. 基于混沌映射的图像快速加密改进算法［J］. 计算机测量与控制，2014，22（10）：3270－3273.

[10] 江　帆，吴小天，孙　伟. 基于稀疏矩阵的 Arnold 数字图像加密算法［J］. 计算机应用研究，2015，35（3）：726－731.

（上接第 163 页）

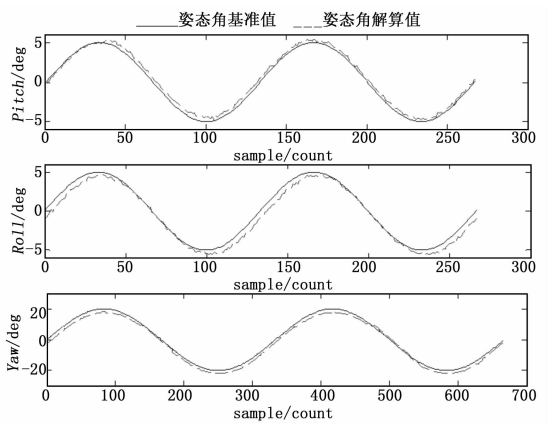


图 3　姿态角动态输出曲线

体的实时位置，满足无人机的飞行要求。与实际飞行时飞机面临的环境有所偏差，实际的误差可能会有所增加。

5　结论

文中介绍了小型四旋翼无人机利用低成本传感器进行解算航姿解算的两种方法，由于单一的姿态解算方法的航姿可信度不高的问题，采用随机加权融合这种自适应滤波方法，对两种不同的解算输出结果进行融合滤波。实验结果统计说明：采用随机加权滤波融合后的姿态信息提高了四旋翼无人机的测量精度，计算量小，能够适应低成本的航姿控制系统。

参考文献：

[1] 聂博文，马宏绪，王　剑，等. 微小型四旋翼飞行器的研究现状与关键技术［J］. 电光与控制，2007，14（6）：113－117.

[2] 赵　勃，鲜　斌，张　鑫，等. 四旋翼飞行器硬件在环仿真平台研究［A］. 第三十一届中国控制会议论文集［C］. 合肥，2012，c 卷：5008－5013.

[3] 吴　勃，徐　欢，乔相伟. 状态切换 UKF 的飞行器姿态确定算法［J］. 电机与控制学报，2012，16（6）：98－104.

[4] 冯智勇，曾　瀚，张　力，等. 基于陀螺仪及加速度计信号融合的姿态角度测量［J］. 西南师范大学学报：自然科学版，2011，36（4）：137－141.

[5] 万晓凤，康利平，余运俊，等. 基于多传感器数据融合的四旋翼飞行器的姿态解算［J］. 科技导报，2014，32（19）：31－35.

[6] 李媛媛，张立峰，多传感器自适应加权融合算法及其应用研究［J］. 自动化与仪器仪表，2008（2）：10－13.

[7] 吴　杰，闫建国. 基于修正的卡尔曼滤波的姿态估计算法研究［J］. 计算机真，2012，29（2）：54－57.

[8] 张荣辉，贾宏光，陈　涛，等. 基于四元数法的捷联式惯性导航系统的姿态解算［J］. 光学精密工程，2008，16（10）：1964－1970.

[9] 葛泉波，李文斌，孙若愚，等. 基于 EKF 的集中式融合估计研究［J］. 自动化学报，2012，39（6）：816－825.

[10] 郭晓鸿，杨　忠，陈　喆，等. EKF 和互补滤波器在飞行姿态确定中的应用［J］. 传感器与微系统，2011，30（11）：149－152.

[11] 辛　琪，史忠科. 基于多源信息的飞行姿态估计方法［J］. 飞行力学，2012，30（6）：527－531.

[12] 梁延德，程　敏，何福本，等. 基于多源信息的飞行姿态估计方法［J］. 飞行力学，2011，30（11）：56－58.

[13] Madgwick S O H，Harrison A J L，Vaidyanathan R H. Estimation of IMU and MARG orientation using a gradient descent algorithm［A］. Proceedings of the 2011 IEEE International Conference on Rehabilitation Robotics（ICORR）［C］. Switzerland：IEEE，2011：1－7.

[14] 张　浩，仁　芊. 四旋翼飞行器航姿测量系统的数据融合方法［J］. 兵工自动化，2013，32（1）：28－31.

[15] 振　江，康健一，张　青，等. 数据融合技术在温室温度检测中的应用［J］. 农业机械学报，2006，37（10）：101－103.

[16] 李　伟，何鹏举，高社生. 多传感器加权信息融合算法研究［J］. 西北工业大学学报，2010，28（5）：674－678.