新的图像加密方法

唐 聃，王晓京，陈 峥

(中国科学院成都计算机应用研究所 成都 610041)

【摘要】针对数字图像信息数据量大、冗余度高和像素间相关性强等特点，提出了一种基于二元多项式的图像加密新方法。在对图像的加密过程中，该方法使用另一幅图像作为密钥，使得密钥形象直观且伪装性强，而密钥图像的尺寸可以远远小于加密图像，便于保存。因加密的大部分步骤中只用到了有限域的加法运算，因此该算法的加密效率较高。该加密方法不仅有安全性高和便于图像的局部加密等优点，还可以方便地推广到视频的图像加密领域，具有很好的应用前景。

关 键 词 二元多项式； 编码； 有限域； 图像叠加； 图像处理

中图分类号 O438； TN249 **文献标识码** A doi:10.3969/j.issn.1001-0548.2010.01.029

New Class of Image Encryption Method

TANG Dan, WANG Xiao-jing, and CHEN Zheng

(Chengdu Institute of Computer Applications, Chinese Academy of Sciences Chengdu 610041)

Abstract Digital images have many intrinsic features such as large amount of data information, highly redundancy, and strong correlation among pixels and so on. A new method of image encryption based on bivariate polynomials is proposed according to the characters of images. In the process of image encryption, another digital image is used as the key, in this way the size of the image key could be much smaller than the secret image. The majority of steps of encryption and decryption just are add operations over a finite field, so the new method has highly efficiency. In addition, the method can be expanded to the video encryption field easily.

Key words bivariate polynomials; finite fields; encoding; image addition; image processing

随着计算机和网络技术的飞速发展，很多信息都可以迅速方便地在网络上传播和发布。数字图像以其形象、生动的特点被广为利用，成为网络中表达信息的重要手段。一些特殊的应用领域，通过网络等开放的通信手段将场景监控图像发送到指定地点，实行远程集中监控，可以节约大量的人力和物力。但这些场景图像中可能包含大量的涉及安全的敏感信息而不能直接传送，需要对这些信息进行加密处理。因此，数字图像在网络中传播的安全性成为人们关注的焦点，而对于数字图像的加密也成为信息安全中的一个重要研究领域[1-2]。

1 一类新的图像加密方法

与文本加密相同，图像加密也属于密码编码学的范畴。传统的文本加密方法研究已经比较成熟，如DES、AES和IEDA等，这些方法在图像加密中可以借鉴但不能完全照搬，因为与普通文本信息相比，图像信息拥有自己独特的性质，如：

(1) 数据量大；
(2) 相关性强；
(3) 冗余度高。

这些性质使传统加密方法在对图像加密时效果不佳。用DES对图1所示图像进行加密，加密后得到图2，但是仍然可以从加密后的图像中容易辨别出图1中图像内容的轮廓。

图1 原始图像

收稿日期：2008 – 07 – 06； 修回日期：2009 – 05 – 05
基金项目：国家重点基础研究发展计划(2004CB318003)
作者简介：唐 聃(1982 –)，男，博士生，主要从事编码理论方面的研究.

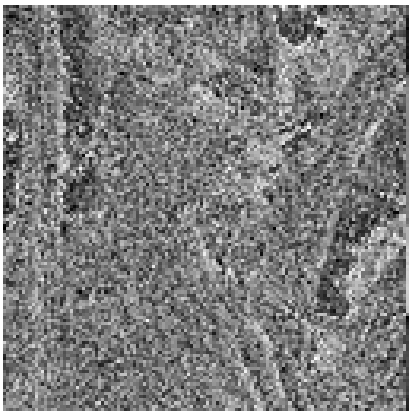

图2　传统加密后图像

目前，图像加密主要采用对称加密体制，而对于图像加密的研究也主要集中在空间域[3-5]、变换域[6-10]和混沌图像加密[11-15]。目前的图像加密技术大都没有考虑图像数据本身的特点[4-12]，如图像数据一般是以二维数组的形式存储的。现在很多针对图像加密的商业系统均是在加密前对图像预处理，将二维的图像数据转换为一维的数据流再进行加密操作，而在解密后又将一维的数据流转换成二维的图像数据，这无疑极大地影响了加解密操作的效率。

本文提出一类新的图像加密方法，该加密方法的所有步骤均基于有限域上的运算[16]。

本文加密方法的步骤如下：

(1) 假设需要加密的图像S宽w高h，其中w和h均为正整数。按照前面的描述，根据像素值将该图像转换为一个矩阵：

$$\boldsymbol{S}=\begin{pmatrix} s(0,0) & s(0,1) & \cdots & s(0,w-1) \\ s(1,0) & s(1,1) & \cdots & s(1,w-1) \\ \vdots & \vdots & \vdots & \vdots \\ s(h-1,0) & s(h-1,1) & \cdots & s(h-1,w-1) \end{pmatrix}$$

(2) 根据图像的类型选定计算的有限域$GF(2^t)$，其中t为正整数。

(3) 选择一幅和图像S同类型且尺寸为$n\times n$的图像K作为密钥的一部分，其中n为正整数。

(4) 根据像素值将密钥图像转换为矩阵：

$$\boldsymbol{K}=\begin{pmatrix} k(0,0) & k(0,1) & \cdots & k(0,n-1) \\ k(1,0) & k(1,1) & \cdots & k(1,n-1) \\ \vdots & \vdots & \vdots & \vdots \\ k(n-1,0) & k(n-1,1) & \cdots & k(n-1,n-1) \end{pmatrix}$$

(5) 确定一个二元$n-1$次多项式$f(x, y) = a(n-1, n-1)x^{n-1}y^{n-1}+a(n-2, n-1)x^{n-2}y^{n-1}+a(n-3, n-1)x^{n-3}y^{n-1}+\cdots+a(1, n-1)xy^{n-1}+a(0, n-1)y^{n-1} + a(n-1, n-2)\times x^{n-1}y^{n-2}+a(n-2, n-2)x^{n-2}y^{n-2}+a(n-3, n-2)x^{n-3}y^{n-2}+\cdots+a(1, n-2)xy^{n-2}+a(0, n-2)y^{n-2}+a(n-1, n-3)x^{n-1}y^{n-3}+a(n-2, n-3)x^{n-2}y^{n-3}+\cdots+a(1, n-3)xy^{n-3}+(0, n-3)y^{n-3}+\cdots+a(n-1, 0)x^{n-1}+a(n-2,0)x^{n-2}+a(n-3,0)x^{n-3}+\cdots+a(1,0)x + a(0,0)$。其中$x, y, i, j, a(i,j)\in GF(2^t)$。二元$n-1$次多项式$f(x,y)$应满足条件$f(i,j)=k(i,j)$，$i,j\in[0, n-1]$。该二元$n-1$次多项式详细的确定方法以及唯一性证明将在后面给出。

(6) 选择两个正整数m_1和m_2，作为密钥的另一部分。其中m_1、$m_2\in[0,\min(2^t-w,2^t-h)]$。

(7) 按如下公式进行计算：$\boldsymbol{K}'=\sum_{i=0}^{w-1}\sum_{j=0}^{h-1} f(i+m_1, j+m_2)$，得到一个$w\times h$的矩阵：

$$\boldsymbol{K}'=\begin{pmatrix} k'(0,0) & k'(0,1) & \cdots & k'(0,w-1) \\ k'(1,0) & k'(1,1) & \cdots & k'(1,w-1) \\ \vdots & \vdots & \vdots & \vdots \\ k'(h-1,0) & k'(h-1,1) & \cdots & k'(h-1,w-1) \end{pmatrix}$$

(8) 按$\boldsymbol{C}=\sum_{i=0}^{w-1}\sum_{j=0}^{h-1}(s(i,j)+k'(i,j))$进行计算，得到一个$w\times h$的矩阵$\boldsymbol{C}$。再将$\boldsymbol{C}$转换成图像，即加密后的图像：

$$\boldsymbol{C}=\begin{pmatrix} c(0,0) & c(0,1) & \cdots & c(0,w-1) \\ c(1,0) & c(1,1) & \cdots & c(1,w-1) \\ \vdots & \vdots & \vdots & \vdots \\ c(h-1,0) & c(h-1,1) & \cdots & c(h-1,w-1) \end{pmatrix}$$

2　二元多项式的确定方法与唯一性证明

前面详细描述了新的图像加密方法的加密步骤，其中最主要的一步是如何根据密钥图像唯一确定一个对应于密钥图像的二元t次多项式。下面将说明二元t次多项式的确定方法以及对一个特定图像确定二元t次多项式的唯一性进行证明。

不失一般性，可以将t次二元多项式记为：

$$\begin{aligned} f(x,y) = {} & a(t,t)x^ty^t + a(t-1,t)x^{t-1}y^t + a(t-2,t)x^{t-2}y^t+\cdots+ \\ & a(1,t)xy^t+a(0,t)y^t+a(t,t-1)x^ty^{t-1}+a(t-1,t-1)x^{t-1}y^{t-1}+ \\ & a(t-2,t-1)x^{t-2}y^{t-1}+\cdots+a(1,t-1)xy^{t-1}+a(0,t-1)y^{t-1}+ \\ & a(t,t-2)x^ty^{t-2}+a(t-1,t-2)x^{t-1}y^{t-2}+\cdots+a(1,t-2)xy^{t-2}+ \\ & (0,t-2)y^{t-2}+\cdots+a(t,0)x^t+a(t-1,0)x^{t-1}+ \\ & a(t-2,0)x^{t-2}+\cdots+a(1,0)x+a(0,0) \end{aligned} \tag{1}$$

将式(1)整理得：

$$\begin{aligned} f(x,y) = {} & (a(t,t)x^t+a(t-1,t)x^{t-1}+a(t-2,t)x^{t-2}+\cdots+a(1,t)x+ \\ & a(0,t))y^t+(a(t,t-1)x^t+a(t-1,t-1)x^{t-1}+a(t-2,t-1)x^{t-2}+\cdots+ \\ & a(1,t-1)x+a(0,t-1))y^{t-1}+(a(t,t-2)x^t+a(t-1,t-2)x^{t-1}+ \end{aligned}$$

$$a(t-2,t-2)x^{t-2}+\cdots+a(1,t-2)x+a(0,t-2))y^{t-2}+\cdots+(a(t,0)\,x^{t}+a(t-1,0)x^{t-1}+a(t-2,0)x^{t-2}+\cdots+a(1,0)x+a(0,0)) \tag{2}$$

将矩阵的每一行作为X轴上的各个坐标，记为集合$X=\{x_0, x_1, x_2, \cdots, x_t\}$，显然其中的各个$x_i$互不相同。将集合$X$中的各个元素代入式(2)得到：

$$\begin{cases} a(t,t)\,x_i^t + a(t-1,t)\,x_i^{t-1}+\cdots+a(1,t)\,x_i + a(0,t) = m(i,t) \\ a(t,t-1)\,x_i^t + a(t-1,t-1)\,x_i^{t-1}+\cdots+a(1,t-1)\,x_i + a(0,t-1) = m(i,t-1) \\ a(t,t-2)\,x_i^t + a(t-1,t-2)\,x_i^{t-1}+\cdots+a(1,t-2)\,x_i + a(0,t-2) = m(i,t-2) \\ \vdots \\ a(t,0)\,x_i^t + a(t-1,0)\,x_i^{t-1}+\cdots+a(1,0)\,x_i + a(0,0) = m(i,0) \end{cases} \tag{3}$$

将矩阵的每一列作为Y轴上的各个坐标，记为集合$Y=\{y_0, y_1, y_2, \cdots, y_t\}$，其中的各个$y_i$也互不相同。将集合$Y$中的每个元素$y_i$分别代入式(3)中的各个等式，并用$y_{i,j}$表示与$x_i$对应的各个$y$值，得到：

$$\begin{cases} m(i,t)\,y_{i,j}^t + m(i,t-1)\,y_{i,j}^{t-1} + m(i,t-2)\,y_{i,j}^{t-2}+\cdots+ m(i,1)\,y_{i,j} + m(i,0) = v(i,j) \\ m(i,t)\,y_{i,j+1}^t + m(i,t-1)\,y_{i,j+1}^{t-1} + m(i,t-2)\,y_{i,j+1}^{t-2}+ \cdots+ m(i,1)\,y_{i,j+1} + m(i,0) = v(i,j+1) \\ m(i,t)\,y_{i,j+2}^t + m(i,t-1)\,y_{i,j+2}^{t-1} + m(i,t-2)\,y_{i,j+2}^{t-2}+\cdots+ m(i,1)\,y_{i,j+2} + m(i,0) = v(i,j+2) \\ \vdots \\ m(i,t)\,y_{i,j+t}^t + m(i,t-1)\,y_{i,j+t}^{t-1} + m(i,t-2)\,y_{i,j+t}^{t-2}+\cdots+ m(i,1)\,y_{i,j+t} + m(i,0) = v(i,j+t) \end{cases} \tag{4}$$

对式(4)作如下变形：

$$\begin{pmatrix} y_{i,j}^t & y_{i,j}^{t-1} & y_{i,j}^{t-2} & \cdots & y_{i,j}^0 \\ y_{i,j+1}^t & y_{i,j+1}^{t-1} & y_{i,j+1}^{t-2} & \cdots & y_{i,j+1}^0 \\ y_{i,j+2}^t & y_{i,j+2}^{t-1} & y_{i,j+2}^{t-2} & \cdots & y_{i,j+2}^0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ y_{i,j+t}^t & y_{i,j+t}^{t-1} & y_{i,j+t}^{t-2} & \cdots & y_{i,j+t}^0 \end{pmatrix} \begin{pmatrix} m(i,t) \\ m(i,t-1) \\ m(i,t-2) \\ \vdots \\ m(i,0) \end{pmatrix} = \begin{pmatrix} v(i,j) \\ v(i,j+1) \\ v(i,j+2) \\ \vdots \\ v(i,j+t) \end{pmatrix} \tag{5}$$

将式(5)简写为$\overline{Y}\,\overline{M}=\overline{V}$，由加密步骤的第2步限定条件，集合$Y$中具有相同$i$值和不同$j$值的各个元素$y_{i,j}$各不相同，由此可以确定$\overline{Y}$是范德蒙行列式，因此式(5)有唯一解。而$\overline{V}$已知，通过对式(5)的求解，可以求出$\overline{M}$。

将所有X的取值代入式(3)得：

$$\begin{cases} a(t,t-i)\,x_0^t + a(t-1,t-i)\,x_0^{t-1}+\cdots+a(1,t-i)\,x_0 + a(0,t-i) = m(0,t-i) \\ a(t,t-i)\,x_1^t + a(t-1,t-i)\,x_1^{t-1}+\cdots+a(1,t-i)\,x_1 + a(0,t-i) = m(1,t-i) \\ a(t,t-i)\,x_2^t + a(t-1,t-i)\,x_2^{t-1}+\cdots+a(1,t-i)\,x_2 + a(0,t-i) = m(2,t-i) \\ \vdots \\ a(t,t-i)\,x_t^t + a(t-1,t-i)\,x_t^{t-1}+\cdots+a(1,t-i)\,x_t + a(0,t-i) = m(t,t-i) \end{cases} \tag{6}$$

其中$0\leqslant i\leqslant t$。

对式(6)作如下变形：

$$\begin{pmatrix} x_0^t & x_0^{t-1} & x_0^{t-2} & \cdots & x_0^0 \\ x_1^t & x_1^{t-1} & x_1^{t-2} & \cdots & x_1^0 \\ x_2^t & x_2^{t-1} & x_2^{t-2} & \cdots & x_2^0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_t^t & x_t^{t-1} & x_t^{t-2} & \cdots & x_t^0 \end{pmatrix} \begin{pmatrix} a(t,t-i) \\ a(t-1,t-i) \\ a(t-2,t-i) \\ \vdots \\ a(0,t-i) \end{pmatrix} = \begin{pmatrix} m(0,t) \\ m(1,t) \\ m(2,t) \\ \vdots \\ m(t,t) \end{pmatrix} \tag{7}$$

将式(7)简写为$\overline{X}\,\overline{A}=\overline{M}$，由加密步骤的第1步限定条件，各个$x_i$的取值互不相同，由此可以确定$\overline{X}$是范德蒙行列式，故式(7)有唯一解。而$\overline{M}$可以通过式(5)计算得出，根据式(7)可计算出$\overline{A}$，由此就可以唯一确定$t$次二元多项式$f(x,y)$。

3 加密方法分析

下面对所提出图像加密方法的一些特点做出分

析，并阐述其用于图像加密的独特优势。

3.1　加密实例及效果分析

选用一个128×128的256级灰度图作为需要加密的秘密图像，如图1所示。因为秘密图像是一个256级的灰度图，因此选择加密计算的有限域为GF(256)= GF(2^8)，使用一个15×15 Pixel的256级灰度图像作为密钥，如图3所示。

图 3　密钥图像

首先按照灰度值将图1和图3转换成矩阵$\boldsymbol{S}$和矩阵$\boldsymbol{K}$。然后按照二元多项式的确定方法为图3唯一确定一个二元14次多项式$f(x,y)$。按照要求选择m_1和m_2，计算矩阵 $\boldsymbol{K}' = \sum_{i=0}^{w-1}\sum_{j=0}^{h-1} f(i+m_1, j+m_2)$。在得出矩阵$\boldsymbol{K}'$后，按照公式$\boldsymbol{C} = \sum_{i=0}^{w-1}\sum_{j=0}^{h-1}(s(i,j)+k'(i,j))$对图像进行的加密效果如图4所示。

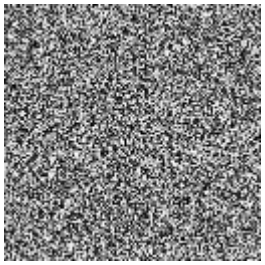

图 4　本文方法加密后图像

图5和图6分别是图1和图4的直方图。从直方图的对比可以看出，经过加密后的图像直方图充满了整个区域，而且分布相当均匀，换句话说加密后的图像非常类似于噪声。

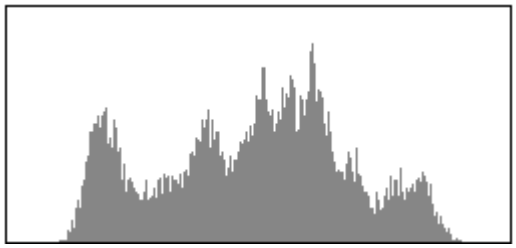

图 5　图 1 的直方图

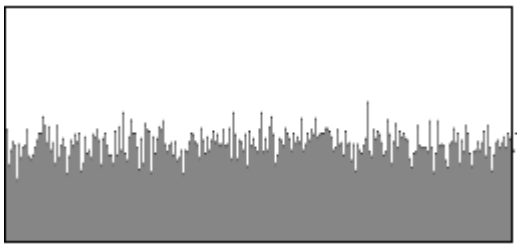

图 6　图 4 的直方图

3.2　其他性能分析

本文加密方法中除了密钥生成阶段(算法复杂度为$O(n^2)$)，加密的其他步骤均只用复杂度为$O(n)$的有限域的加法进行计算，而在密钥生成阶段可以选取尺寸很小的密钥图像进行计算，因此加密的效率应该是较高的，而对于在使用相同密钥加密多幅图像或视频的情况下，该方法比其他图像加密方法的效率优势将更加明显。其次，密钥图像的尺寸在加密计算的有限域中可以是任意的，因此，一般选择尺寸较小的图片作为加密密钥，以便于保存和传输。而只要改变m_1和m_2的值，就可以将密钥图片扩展到整个有限域空间。因此，在加密计算选择的有限域GF(2^t) = GF(q)时，攻击者如果要破译加密图像则需要计算$q\times\sum_{i=1}^{q} q^{i^2}$次才能对整个空间遍历完成。最后，因为在密钥图片确定后的整个加密过程中的计算，均是按照图像存在的二维矩阵特点而基于图像横纵坐标的有限域加法运算，将使对于图像的局部加密更为方便，只需要改变加密图像坐标即可，整个加密的其他步骤都可以不做任何改变。

4　总　结

本文提出的加密方法的密钥为另一幅和加密图像类型相同的图像，形象直观，而密钥图像尺寸可以远远小于加密图像，便于保存。除此之外，与目前大多数图像加密的方法相比，本文所提出的方法更注重于图像本身的特点，具有加密速度快、安全性高和便于图像的局部加密等优点。而该方法也可以非常容易地扩展到视频图像的加密应用中，因此具有很好的发展前景。

参　考　文　献

[1] 韩振海, 刘秋武, 刘　艺, 等. 基于联合变换的旋转不变光学图像加密[J]. 电子科技大学学报, 2004, 33(1): 31-34.
HAN Zhen-hai, LIU Qiu-wu, LIU Yi, et al. Optical image encryption with rotating invariance based on joint transform correlator[J]. Journal of University of Electronic Science and Technology of China, 2004, 33(1): 31-34.

[2] HABUTSU T, ISHIO Y N, SASASE I, et al. A secret cryptosystem by iterating a chaotic map[C]//Advances in Cryptology EU-RCRYPT'91. Berlin: Springer –Verlag, 1991: 127-140.

[3] ZHANG Han, WANG Xiu-feng, LI Zhao-hui, et al. A new image encryption algorithm based on chaos system [C]//International Conference on Robotic, In Telligent Systems and Signals processing. Changsha, China: IEEE Press, 2003: 778-782.

[4] YANG Jun, ZHOU Xian-wei, QIN Bo-ping. On the selection of random numbers in the ElGamal algorithm[J]. Journal of Electronic Science and Technology of China, 2006, 4(1): 25-17.
[5] DANG P P, CHAU P M. Image encryption for secure Internet multimedia applications[J]. IEEE Transactions on Consumer Electronics, 2000, 46(8): 395-403.
[6] JUNG K H, LEE C W. Image compression using projection vector quantization with quadtree decomposition[J]. Signal Processing: Image Communication, 1996, 8(5): 379-368.
[7] LIN T W. Compressed quadtree representations for storing similar images[J]. Image and Vision Computing, 1997, 15(11): 833-843.
[8] WONG W T, SHIH F Y, SU T F. Thinning algorithms based on quadtree and octree representations[J]. Information Sciences, 2006, 176(10): 1379-139.
[9] BOURBAKIS N, ALEXOPOULOS C. Picture data encryption using scan patterns[J]. Pattern Recognition, 1992, 25(6): 567-581.
[10] MUZAFFAR T, CHOI T S. Linked significant tree wavelet-based image compression[J]. Signal Processing. 2008, 88(10): 2554-2563.
[11] MATTHEWS R. On the derivation of a “Chaotic” encryption algorithm[J]. Cryptologia, 1984, 8(1): 29-41.
[12] SHORT K M. Unmasking a modulated chaotic communications Scheme[J]. International Journal of Bifurecation and Chaos,1996, 6(2): 367-375.
[13] DEDIEU H, OGORZALEK M J. Indentifiability and identification of chaotic systems based on adaptive synchronization[J]. IEEE Transactions Circuits and Systems, 1997, 44(10): 948-962.
[14] ZHANG Yong-hong, KANG Bao-sheng, Zhang Xue-feng. Image encryption algorithm based on chaotic sequence [C]//The 16th International Conference on Artificial Reality and Telexistence. Washington, DC, USA: IEEE Computer Society, 2006: 221-223.
[15] WILLIAM S. Cryptography and network security principles and practices[M]. Beijing: Publishing House of Electronics Industry, 2006: 66-67.
[16] PLANK J S. A tutorial on Reed-Solomon coding for fault-tolerance in RAID-like systems[J]. Software−Practice& Experience, 1997, 27(9): 995-1012.

编 辑 张 俊

·我校科研成果介绍·

面向工程应用的复杂目标电磁散射高效数值分析软件A-UEST

该成果直接面向工程需求，针对实际工程中的电大尺寸复杂(复杂形状、复杂材料、复杂结构)目标，应用计算电磁学最新理论成果即多层快速多极子方法(MLFMA)进行电磁散射数值求解，实现了计算的高精度与高效率，其计算复杂度与存储量仅为$C\times O(N\lg N)$(C为常系数，N为未知量数目)。在此基础上进一步提出了转换因子修正内插技术、重复外向波存储技术、多极子模式数修正等技术，同时应用基于树型数据结构的Morton键技术，使MLFMA具有更加优良的性能。该项目提出了一系列创新方法，如修正电场积分方程方法、MLFMA、快速远场近似(FAFFA)与部分耦合模型的结合应用、后期近似迭代技术、局部多层快速多极子方法、均衡混合场积分方程数值解法等，进一步提高了计算效率(系数C降至10^{-4}量级)，减少了内存需求(降至$O(N)$)，使A-UEST软件具备了精确求解复杂结构电大目标电磁散射并适合于各种型号目标应用的实际工程能力。

A-UEST软件经过大量独立来源的理论、实验数据的严格验模，已证明了其可靠性和置信度。对于所计算过的各种验模目标，逐点比较的平均误差小于2 dB。

该软件由电子科技大学独立研发，具有我国自主知识产权；采用模块化结构，图形界面友好；电磁计算模块丰富，后置模块功能较强；除可计算目标电磁散射(RCS)全向方向图之外，还可重建目标几何外形并给出目标表面感应电流分布，大大方便了对目标散射机理分析与RCS控制研究。该软件不仅能用于金属目标，还可用于介质体、介质涂敷金属目标和含腔目标的电磁散射计算；既可计算目标单站RCS，也可计算双、多站RCS；既可计算散射远场分布，也可计算近场分布；通用性和普适性较强。该软件已在多个大型工程项目的目标特性分析中获得成功应用。除上述应用外，A-UEST软件在天线设计、电磁兼容仿真、射频集成电路设计、信号完整性分析等领域也具有广阔的应用前景。