定性映射极化恒等式及其在数字图像加密中的应用*

国红军[1],陈黎黎[1,2],池学东[1]
(1.宿州学院 智能信息处理实验室,安徽 宿州 234000;
2.安徽大学 智能计算与信息处理教育部重点实验室,安徽 合肥 230039)

【摘 要】针对信息安全领域的数据加密问题,结合密码学、属性论方法学等相关学科知识,以静止的灰度图像为研究对象,提出了一种基于Arnold变换和极化恒等式的数字图像加密算法,并利用Matlab工具对算法进行了仿真实验,实验结果验证了该算法对二维数字图像加密的可行性和安全性。

【关键词】定性映射;极化恒等式;Arnold变换;数字图像加密
【中图分类号】TP309.7 【文献标志码】A 【文章编号】1673-1891(2015)03-0035-04
DOI:10.16104/j.cnki.xccxb.2015.03.011

引言

随着计算机技术和网络技术的飞速发展,许多传统的基于纸面的重要信息陆续转化为数字电子媒体的形式出现,并且常常需要通过互联网进行传输和共享。为了保证这些信息在网络传输过程中不被他人窃取或者篡改,应当对某些敏感数据、隐私信息等进行加密处理。

数据加密是指利用加密算法和加密密钥将明文转换为密文,实现对数据信息的隐藏,必要时再通过解密算法和解密密钥将密文恢复为明文的一种数据保密技术[1],如图1所示,它是保证数据信息安全的一种最为可靠的手段。数据加密技术根据密钥的类型可以分为两类:对称密钥加密(DES)和非对称密钥加密(RSA)[2]。对称密钥加密技术在加密和解密时,通信双方使用同一密钥(即$K_E=K_D$),要求双方都必须保持密钥的保密性。非对称密钥技术在加密和解密时,通行双方使用不同的密钥(即$K_E\neq K_D$),加密密钥为公钥,解密密钥为私钥。

随着计算机软硬件技术的不断发展,一些传统的加密算法(如64位DES、512位整数因子分解的RSA等)在不断的试验中被破解。这就要求我们设计出更加先进的加密算法来保证数据信息的安全。

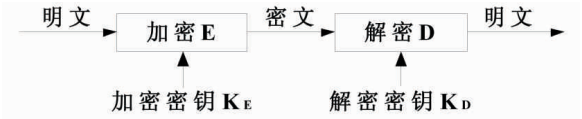

图1 数据加解密过程

2 基于定性映射极化恒等式的数据加密原理

定性映射[3,4]是中国人工智能学会理事—冯嘉礼教授提出的一种基于思维建构和智能模拟的人工智能模型。在定性映射模型的定义中,假设有两个任意的n维向量$\overline{W}$和$\overline{X}$,如图2所示,其内积为$<\overline{W},\overline{X}>=\sum_{i=1}^{n}w_ix_i$,则两向量对应的极化恒等式(polarization identity)[5,6]可表示为式(1)。

$$<\overline{W},\overline{X}>=\sum_{i=1}^{n}w_ix_i=\left(\frac{\overline{W}+\overline{X}}{2}\right)^2-\left(\frac{\overline{W}-\overline{X}}{2}\right)^2=\left(\frac{\overline{W}}{2}+\frac{\overline{X}}{2}\right)^2-\left(\frac{\overline{W}}{2}-\frac{\overline{X}}{2}\right)^2$$
$$=\left(\frac{\overline{W}}{2}+\frac{\overline{W}}{2}\right)\left(\frac{\overline{X}}{2}+\frac{\overline{X}}{2}\right)=OC^2=OB^2-BC^2 \quad (1)$$

由(1)式,在向量$\overline{W}$和向量$\overline{X}$所确定的平面上,分别以$\frac{\overline{W}+\overline{X}}{2}$(即OB)为直径,以$\frac{\overline{W}-\overline{X}}{2}$(即BW)为半径作圆,假设两圆相交于C和D两点,则$BC\perp OC$。此时,记OC为$\overrightarrow{\gamma_1}$,OD为$\overrightarrow{\gamma_2}$,则有:

$$\overrightarrow{\gamma_1}^2=\overrightarrow{\gamma_2}^2=OC^2=OB^2-BC^2=OD^2=OB^2-BD^2=\left(\frac{\overline{W}+\overline{X}}{2}\right)^2-\left(\frac{\overline{W}-\overline{X}}{2}\right)^2=\overline{W}\cdot\overline{X}=\sum_{i=1}^{n}w_ix_i$$

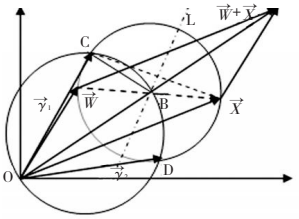

图2 内积的特征向量

当$\overline{W}\perp\overline{X}$时,$\overrightarrow{\gamma_1}$和$\overrightarrow{\gamma_2}$退化为0向量:$\overrightarrow{\gamma_1}=\overrightarrow{\gamma_2}=0$,故$|\overrightarrow{\gamma_1}|^2=|\overrightarrow{\gamma_2}|^2=\sum_{i=1}^{n}w_ix_i=\overline{W}\cdot\overline{X}=0$;当$\overline{W}=\overline{X}$时,$\overrightarrow{\gamma_1}$或$\overrightarrow{\gamma_2}$与向量$\overline{W}$和$\overline{X}$重合,即:$\overrightarrow{\gamma_1}=\overrightarrow{\gamma_2}=\overline{W}=\overline{X}$,故有:$|\overrightarrow{\gamma_1}|^2=|\overrightarrow{\gamma_2}|^2=\sum_{i=1}^{n}w_ix_i=\overline{X}\cdot\overline{X}$。由此可见,向量$\overrightarrow{\gamma_1}$和$\overrightarrow{\gamma_2}$能反映内积$\overline{W}\cdot\overline{X}=\sum_{i=1}^{n}w_ix_i=|\overline{W}||\overline{X}|\cos\alpha$的各种变化规律,它们是内积$\overline{W}\cdot\overline{X}=\sum_{i=1}^{n}w_ix_i$的特征向量。若定义$\wedge$和$\oplus$为向量的极化运算,则极化向量可分别记为$\overrightarrow{\gamma_1}=\overline{W}\wedge\overline{X}$,$\overrightarrow{\gamma_2}=\overline{W}\oplus\overline{X}$,并据此可得以下结论,即,对任一向量$\overline{X}$和模平方等于任一常数的向量$\overrightarrow{\gamma}(|\overrightarrow{\gamma}|^2=\theta)$,存在一个与$\overline{X}$和$\overrightarrow{\gamma_1}$共面的向量$\overline{W}$,使

收稿日期:2015-04-15
*基金项目:宿州学院优秀青年人才基金重点项目(项目编号:2013XQRL01);宿州学院科研平台开放课题(项目编号:2013YKF17);大学生创新创业训练计划(项目编号:201410379002)。
作者简介:国红军(1981-),男,讲师,硕士,研究方向:信息安全、数据挖掘。

得：$\overrightarrow{W}\cdot\overrightarrow{X}=\sum_{i=1}^{n}w_ix_i=|\overrightarrow{\gamma}|^2=\theta$。这时，我们称 $\overrightarrow{W}$ 为 $\overrightarrow{X}$ 相对于 $\overrightarrow{\gamma}$ 的极化向量。相应地，称常数 $\theta(\theta\geq0)$ 相对于 $\overrightarrow{X}$ 和 $\overrightarrow{\gamma}$ 的向量 $\overrightarrow{W}$ 的极化内积分解。

在图2中，过向量 $\overrightarrow{\gamma}$ 的端点 $C(c_1,c_2)$ 作垂线CB，交线段CX的垂直平分线L于点 $B(b_1,b_2)$，则由B满足的下述方程组(2)，可求B的坐标如式(3)所示，再由 $\overrightarrow{W}=2\overrightarrow{B}-\overrightarrow{X}$ 即可得到伴随向量 $\overrightarrow{W}$ 的坐标 (w_1,w_2) 如式(4)所示。

$$\begin{cases} y_b-c_2=-\dfrac{c_1}{c_2}(x_b-c_1) & BC\text{ 的方程} \\ y_b-\dfrac{c_2+x_2}{2}=-\dfrac{c_1-x_1}{c_2-x_2}\left(x_b-\dfrac{c_1+x_1}{2}\right) & L\text{ 的方程} \end{cases} \quad (2)$$

$$\begin{cases} x_b=\dfrac{(2x_2-c_2)(c_1^2+c_2^2)-c_2(x_1^2+x_2^2)}{2(c_1x_2-c_2x_1)} \\ y_b=\dfrac{(2x_1-c_1)(c_1^2+c_2^2)-c_1(x_1^2+x_2^2)}{2(c_2x_1-c_1x_2)} \end{cases} \quad (3)$$

$$\begin{cases} w_1=\dfrac{(2x_2-c_2)(c_1^2+c_2^2)-(c_1x_1+c_2x_2)x_2}{c_1x_2-c_2x_1} \\ w_2=\dfrac{(2x_1-c_1)(c_1^2+c_2^2)-(c_1x_1+c_2x_2)x_1}{c_2x_1-c_1x_2} \end{cases} \quad (4)$$

根据极化恒等式和极化向量运算模型，将向量 $\overrightarrow{X}$ 看作原文，$\overrightarrow{W}$ 为密钥，$\overrightarrow{\gamma}=E(\overrightarrow{X})=\overrightarrow{W}\wedge\overrightarrow{X}$ 或 $\overrightarrow{\gamma}=E(\overrightarrow{X})=\overrightarrow{W}\oplus\overrightarrow{X}$ 当作加密过程，$D(\overrightarrow{\gamma})=\overrightarrow{\gamma}\cdot\overrightarrow{W}^{-1}=\overrightarrow{X}$ 当作解密过程，再将极化运算、向量平移和旋转运算结合起来，便可得到一种基于定性映射极化恒等式的数据加密算法E和解密算法D。

3 数据加密系统设计

如果S为一个加密系统，则可以将它表示为：$S=\{P,C,K,E,D\}$，其中P为明文空间，C为密文空间，K为密钥空间，E为加密算法，D为解密算法。加密系统的设计最重要的是其中的E、D和K。在基于定性映射极化恒等式的数据加密系统中，将密钥集合表示为 $K=\{\overrightarrow{X},\theta,\overrightarrow{W}\}$，其中，密钥 $\overrightarrow{W}$ 和 θ 分别为对原文进行向量平移的坐标大小和旋转角度。具体过程如图3所示。

加密过程：

(1)选择平移和旋转密钥对明文向量 $\overrightarrow{X}$ 进行平移和旋转运算，得到密文 $\overrightarrow{X}'$；

(2)对 $\overrightarrow{X}$ 再进行极化运算 $\overrightarrow{X}'\wedge\overrightarrow{W}$ 或 $\overrightarrow{X}'\oplus\overrightarrow{W}$，得到密文 $\overrightarrow{X}''$。

解密过程：

(1)对密文 $\overrightarrow{X}''$ 进行极化逆运算得到 $\overrightarrow{X}'$，即 $\overrightarrow{X}''\cdot\overrightarrow{W}^{-1}=\overrightarrow{X}'$；

(2)对 $\overrightarrow{X}'$ 进行向量反平移和反旋转运算得到明文 $\overrightarrow{X}$

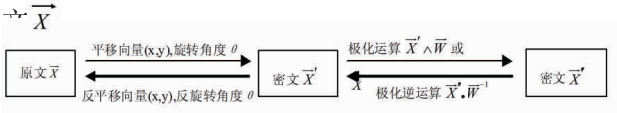

图3 基于极化恒等式的加密系统工作过程

4 二维数字图像加密

4.1 图像置乱

以二维数字图像为例，在对其进行加密处理时，我们首先可以应用Arnold变换[7,8]打乱图像的相关性，将原始图像置乱，得到置乱后的图像矩阵。具体做法如下：假设将正方形的二维数字图像用矩阵M表示，矩阵M中的元素的值为图像的灰度值或RGB颜色分量值。如果图像不是正方形，则通过补0的方式，将其补为正方形。Arnold变换可表示为(5)式。

$$\begin{bmatrix}x'\\y'\end{bmatrix}=\begin{bmatrix}1&1\\1&2\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}\bmod N \quad x,y\in\{0,1,\cdots,N-1\} \quad (5)$$

其中，(x,y) 为像素点在原图像中的坐标，(x',y') 为像素经变换后在新图像中的坐标，N为数字图像的阶数。对一个图像进行Arnold变换，实际上就是把图像的像素点位置按公式进行移动。对于一个2阶的矩阵 $T=\begin{bmatrix}a&b\\c&d\end{bmatrix}$，当满足ad−bc=1时，公式(6)可看作是对二维图像的一种置乱变换。

$$\begin{bmatrix}x'\\y'\end{bmatrix}=\begin{bmatrix}a&b\\c&d\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}\bmod N+1,x,y\in\{1,\cdots,N\} \quad (6)$$

如果我们对一个二维数字图像迭代地使用上述置乱变换，即通过合理的设置参数a,b,c和迭代次数f，将公式(6)左端的 (x',y') 作为下一次的输入，重复迭代f次后，则可得到置乱后的图像矩阵M1。

4.2 图像加密[9]

置乱后的数字图像可根据极化恒等式的内积分解理论来设计对应的加密算法，实现对像素值的加密。具体算法[10]为：设明文向量为 $\overrightarrow{X}=(x_1,x_2)$，密钥向量为 $\overrightarrow{W}=(w_1,w_2)$，密文向量 $\overrightarrow{C}=(m_1,m_2)$，将置乱图像 M_1 按列排成一个一维数组 M_2。先取第一组明文 $x_1=M_2(i)$，$x_2=M_2(i+1)$，i=1，明文向量为 $\overrightarrow{X}=(x_1,x_2)$。取 $w_1=M_2(i+2)$，$w_2=M_2(i+3)$ 作为第一组明文的密钥向量 $\overrightarrow{W}=(w_1,w_2)$，通过极化向量运算进行加密，得到该组的密文向量 $\overrightarrow{C}$，i=i+4，然后依此类推，加密过程如图4所示，其中 (a_1,a_2) 为最后一组明文向量的密钥向量。

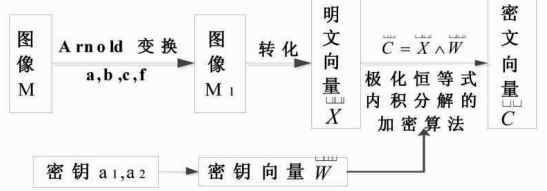

图4 数字图像加密过程

4.3 仿真实验

选取一幅256×256的图像，如图5所示，设置密钥参数为：a=1、b=1、c=2、f=18、a1=125、a2=88，按

上述方法,使用MATLAB语言编程对图像进行置乱和加密处理,如图6和图7所示。图像的解密是上述加密过程的逆过程,解密得到的图像如图8所示。

图5　原始图像

图6　Arnold变换后的图像

图7　极化恒等式原理加密后的图像　图8　解密后的图像

以上的加密过程由于结合了Arnold变换和定性映射极化恒等式加密原理两种数据加密算法,增加了破译难度,因此,即使加密后的图像被非法获取,获取者也无法从其中直接获取有用信息。一方面,以极化恒等式和极化向量运算模型为基础的数据加密算法和解密算法的密钥空间由向量 $K=\{\overline{X},\theta,\overline{W}\}$ 构成,要同时破解向量中的两个分量具有相当的难度。另一方面,从图9和图10中可以看出,经本算法加密后的图像,其相邻的像素点的相关性大大减弱,这使得攻击者想要对图像进行统计分析攻击十分困难,从而保证了信息的安全性。

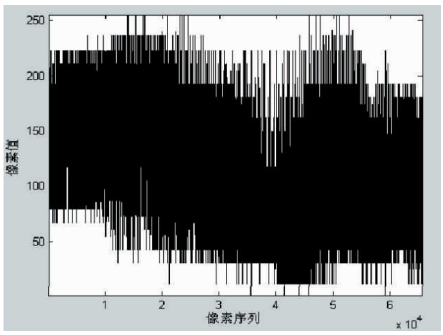

图9　原图像的像素分布

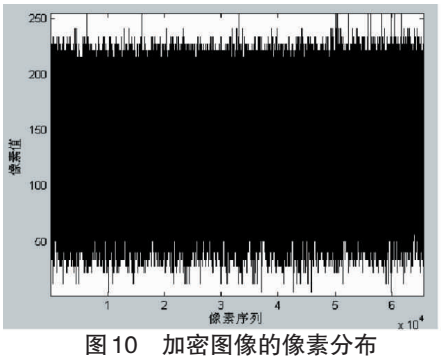

图10　加密图像的像素分布

5 总结

在研究属性论方法的定性映射原理基础上,本文运用定性映射极化恒等式以及极化向量和向量内积分解等相关理论,结合Arnold变换,设计出了一种全新的数据加密算法。通过对二维数字图像的加密和解密仿真实验,验证了该算法的有效性。同时,在安全性方面,该算法相对传统加密算法也有了一定程度的提高。

注释及参考文献:

[1]梁晔,赵彦敏.数据加密算法的分析与研究[J].甘肃高师学报,2011,16(2):14-16.

[2]朱丽娟.数据加密技术的研究与发展[J].中国制造业信息化,2011,40(17):59-62.

[3] Feng Jiali. Attribute network computing based on qualitative mapping and its application in pattern recognition [J]. Journal of Intelligent and Fuzzy System, 2008, (19):243-258.

[4]周炎岩.基于定性映射的数字音频水印算法[D].上海:上海海事大学,2011.

[5]冯嘉礼.内积的极化向量与常数的极化内积分解[J].广西师范大学学报,2001(3):147-152.

[6]冯嘉礼,汪珣,刘永昌.基于定性映射极化恒等式的四钥加密算法[C].海口:第十一届中国人工智能学术年会,2005:429-434.

[7]黄仿元.基于Arnold变换的图像置乱算法及其实现[J].贵州大学学报,2008,25(3):276-279.

[8]吴玲玲,张建伟,葛琪.Arnold变换及其逆变换[J].微计算机信息,2010,26(5-2):206-208.

[9]赵旭.数据加密算法分析与改进[D].哈尔滨:哈尔滨工业大学,2012.

[10]周文杰.极化恒等式和属性网络计算器在图像加密和水印中的应用研究[D].上海:上海海事大学,2009.

Qualitative Mapping Polarized Identity and Application in Digital Image Encryption

GUO Hong-jun[1], CHEN Li-li[1,2], CHI Xue-dong[1]

(1.Laboratory of Intelligent Information Processing, Suzhou University, Suzhou, Anhui 234000;
2.The Key Laboratory of Intelligent Computing & Signal Processing of MOE, Anhui University, Hefei, Anhui 230039)

Abstract: Cryptography, attribute theory and other disciplines of knowledge have been combined, and an image encryption algorithm based on Arnold transform and qualitative mapping polarization identity has been proposed to solve the problem of data encryption in information security. Taking still gray image as the object of study, simulation experiments have been carried out by using Matlab. The experimental results show that the algorithm is feasible and safe.

Key words: qualitative mapping; polarized identity; Arnold transform; digital image encryption

(上接第34页)

energy consumptions and the plug has extended the effective thickness of target.Based on the laws of conservation of energy and the model of Chen and Li,the calculation formula of residual velocity can be put forward after the blunt projectile penetrates the double-layered plate.In the process of armor-piercing, considering about the influence of the plug on the property of terminal ballistic limit,the thesis has compared and analyzed the relevant experimental data about blunt projectile piercing the plates from Weldox 700E series.

Key words: blunt rigid projectile; double-layered plates in contact; perforation; shear plugging; plug