一种基于矩阵变换的非对称图像加密算法

韩水华 杨双远

(厦门大学 管理学院, 福建 厦门 361005)

摘要: 为提高图像数据的加解密速度与安全性,提出了一种新的非对称图像加密算法. 算法原理是基于某种矩阵变换,使得原始图像每一分块像素及其频域产生置乱. 具体实现上,首先利用矩阵变换产生密钥对;然后使用私钥对图像在变换域进行加密;最后接收方用公钥解密加密的图像. 由于该算法是基于矩阵变换的,具有实现方便,加解密快速的特点;非对称的加密机制则使得数据加密更具安全性. 同时,为了进一步提高矩阵变换的安全性,引入了第二种加密机制,将伪随机的高斯白噪声加载到变换矩阵上. 分析表明,这种方法对于加密大容量数据尤其是数字图像特别有用.

关 键 词: 图像加密; 非对称加密; 矩阵变换

中图分类号: TP391 文献标识码: A 文章编号: 1671-4512(2006)05-0043-03

An asymmetric encryption algorithm for images based on matrix transformation

Han Shuihua Yang Shuangyuan

Abstract: On the basis of a certain matrix transformation, a novel asymmetric encryption algorithm for image was proposed to scramble all the pixels and frequencies in each block of the original images. The proposed algorithm was especially useful for the encryption of large amounts of data, such as digital images, and had been implemented. A pair of keys was created through the matrix transformation. The image was encrypted by using private key in its transformation domain. The encrypted messages were decrypted by the receiver with the help of the public key. This algorithm was easily implemented and highly efficient to quickly encrypt and decrypt image messages. The asymmetric encryption mechanism made the encrypted data more secure. The second encryption schema was used to produce transformation matrix by pseudo-random Gauss white noise to farther improve the security of matrix transformation.

Key words: image encryption; asymmetric encryption; matrix transformation

Han Shuihua Assoc. Prof.; School of Management, Xiamen University, Xiamen 361005, Fujian China.

采用传统密码学理论开发出来的加解密系统,安全性主要通过密钥控制的复杂替换过程来保证. 对于数据量极为庞大的多媒体数据流而言,难以实现快速的加、解密. 因此必须结合多媒体信息的特点,研究适合多媒体信息的加密技术.

考虑到图像信息的一些特征,近年来发展了几种图像加密系统,如:基于矩阵变换/像素置换[1];基于伪随机序列[2];基于SCAN语言[3];基于"密钥图像"[4];基于四叉树及SCAN语言[5];基于矢量量化压缩编码及其商业密码[6]等. 这些

收稿日期: 2005-07-01.

作者简介: 韩水华(1970-),男,副教授;厦门,厦门大学管理学院(361005).

E-mail: hansh@xmu.edu.cn

基金项目: 国家高技术研究发展计划资助项目(2004AA414050);福建省科技重大专项基金资助项目(2004HZ02).

算法要么加密的速度慢, 要么安全性比较低. 依据现代密码机制, 本文提出了一种基于矩阵变换的非对称图像加密技术.

1 算法原理

为了讨论的便利性, 本文中要加密的图像为灰度图像, 命名为 $\boldsymbol{I}_{M\times N}$ (对于 RGB 图像, 就加密其亮度空间). 具体的加密过程如下:

a 产生一对密钥, 私钥用来加密, 公钥用来解密;

b 将待加密图像分成互不相交的 $P\times P$ 块并做 DCT 变换;

c 对每个 $P\times P$ 块中的前 $K\times K$ 个系数使用私钥加密;

d 合并 $P\times P$ 块并做反 DCT 变换;

e 对反 DCT 后的系数做界定处理, 使之处于 0~ 1 之间.

因为要对每个 $P\times P$ 块中前 $K\times K$ 个系数分别进行加密, 所以使用文献[7]中的方法产生一组空间维度为 $P\times K$ 的标准正交基($K< P$), 定义为 $\{u_i, i= 1, 2, \cdots, K\}$. 同样地, 利用高斯白噪声产生一个 $P\times P$ 的可逆矩阵 $\boldsymbol{A}$. $\{u_i\}$ 组成矩阵 $\boldsymbol{U}$ 的列向量, 具体表示为:

$$\boldsymbol{A}=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1P}\\ a_{21} & a_{22} & \cdots & a_{2P}\\ & \cdots & & \\ a_{P1} & a_{P2} & \cdots & a_{PP}\end{bmatrix};$$

$$\boldsymbol{U}=\{u_i\}=\begin{bmatrix} u_{11} & a_{12} & \cdots & a_{1K}\\ u_{21} & a_{22} & \cdots & a_{2K}\\ & \cdots & & \\ u_{P1} & a_{P2} & \cdots & a_{PK}\end{bmatrix}.$$

假设待加密图像 I 对应的 DCT 变换系数为 $\boldsymbol{X}_{M\times N}$. 对某一个 $\boldsymbol{X}_{P\times P}$ 块的前 $K\times K$ 个系数组成的矩阵 $\boldsymbol{X}_0$, 使用 $\boldsymbol{AU}$ 作为私钥加密, 使用 $\boldsymbol{A}^{-\mathrm{T}}\boldsymbol{U}$ 作为公钥解密. 具体过程如下.

A. 加密过程

a 对图像 I 按 $P\times P$ 分块, 每块分别做 DCT 变换, 对应的 DCT 变换系数定义为 $\boldsymbol{X}_{M\times N}=\mathrm{DCT}(\boldsymbol{I}, [P\quad P])$.

b 每个 $P\times P$ 块都取其前 $K\times K$ 个系数分别加密, 假设某块 $\boldsymbol{X}_0$ 的前 $K\times K$ 个系数组成的矩阵为 $\boldsymbol{X}_1$, 则其使用私钥 $\boldsymbol{AU}$ 加密后的信息为: $\boldsymbol{X}_2=\boldsymbol{AUX}_0$, $\boldsymbol{X}_2\in\mathbf{R}^{P\times K}$.

c 使用 $\boldsymbol{X}_2$ 替换 $\boldsymbol{X}_0$ 的前 $P\times K$ 个系数, 若 K 很接近 P, 则依据 DCT 变换的特性, $\boldsymbol{X}_0$ 剩余的 $(P-K)\times(P-K)$ 个系数均接近于 0, 所以直接替换掉不影响图像的解密效果, $\boldsymbol{X}_0(i,j)=\boldsymbol{X}_2\{1\leqslant i\leqslant P, 1\leqslant j\leqslant K\}$.

d 合并各个 $P\times P$ 块, 做反 DCT 变换并命名为 $\boldsymbol{X}_{2M\times N}$, $\boldsymbol{X}=\mathrm{IDCT}(\boldsymbol{X}_{M\times N})$.

e 为了防止超出, 界定 $\boldsymbol{X}_{2M\times N}$ 所有的值均在 0~ 1 之间.

f 保存 $\boldsymbol{X}_{2M\times N}$ 为灰度图像, 即为加密后的图像文件.

B. 解密过程

总共需要一个五元组: 分块长度 P; 加密矩阵维度 K; 解密公钥 $\boldsymbol{A}^{-t}\boldsymbol{U}$; 系数最小值 $\delta_{\min}$; 系数最大值 $\delta_{\max}$. 假设需要解密的图像为 $\boldsymbol{X}_{3M\times N}$, 则具体的解密过程如下:

a 还原 $\boldsymbol{X}_{3M\times N}$ 系数

$$\boldsymbol{X}_{3M\times N}=\boldsymbol{X}_{3M\times N}\times(\delta_{\max}-\delta_{\min}).$$

b 对 $\boldsymbol{X}_{3M\times N}$ 按 $P\times P$ 分块做 DCT 变换, 命名为 $\boldsymbol{X}_{4M\times N}$,

$$\boldsymbol{X}_{4M\times N}=\mathrm{DCT}(\boldsymbol{X}_{3M\times N}, [P\quad P]).$$

c 每个 $P\times P$ 块都取其前 $P\times K$ 个系数分别解密, 假设某块 D_0 前 $P\times K$ 个系数组成的矩阵为 $\boldsymbol{D}_1$, 其使用公钥 $\boldsymbol{A}^{-\mathrm{T}}\boldsymbol{U}$ 解密后的信息 $\boldsymbol{D}_2\in\mathbf{R}^{K\times K}$ 为: $\boldsymbol{D}_2=(\boldsymbol{A}^{-\mathrm{T}}\boldsymbol{U})^{\mathrm{T}}\boldsymbol{D}_1=(\boldsymbol{U}^{\mathrm{T}}\boldsymbol{A}^{-1})(\boldsymbol{AU})\boldsymbol{X}_0=(\boldsymbol{U}^{\mathrm{T}}\boldsymbol{U})\boldsymbol{X}_0$, 因为 $\boldsymbol{U}$ 的列向量为一组标准正交基, 所以 $\boldsymbol{U}^{\mathrm{T}}\boldsymbol{U}=\boldsymbol{E}$, 即有 $\boldsymbol{D}_2=\boldsymbol{X}_0$.

d 使用 $\boldsymbol{D}_2$ 和 0 替换 $\boldsymbol{D}_0$ 的前 $P\times K$ 个系数

$$\boldsymbol{D}_0(i,j)=\begin{cases}\boldsymbol{D}_2\{1\leqslant i,j\leqslant K\},\\ 0\quad (K< i\leqslant P, 1\leqslant j\leqslant K).\end{cases}$$

e 做反 DCT 变换, 合并各个 $P\times P$ 块并命名为 $\boldsymbol{X}_{5M\times N}=\mathrm{IDCT}(\boldsymbol{X}_{4M\times N})$.

f 保存 $\boldsymbol{X}_{5M\times N}$ 为灰度图像, 即为解密后的图像文件.

2 安全性分析

2.1 噪声分析

图像加密后, 总是可能存在噪声成分, 因此, 可能在有噪声的情况下解密图像. 假设存在的加性高斯白噪声为 n, 即 $\boldsymbol{X}_1'=\boldsymbol{X}_1+n$; 那么解密过程变换为: $\boldsymbol{X}_2=(\boldsymbol{A}^{-\mathrm{T}}\boldsymbol{U})^{\mathrm{T}}\boldsymbol{X}_1'=\boldsymbol{U}^{\mathrm{T}}\boldsymbol{A}^{-1}\boldsymbol{AUX}_0+\boldsymbol{U}^{\mathrm{T}}\cdot\boldsymbol{A}^{-1}n=\boldsymbol{X}_0+\boldsymbol{U}^{\mathrm{T}}\boldsymbol{A}^{-1}n$.

因为变换矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{U}$ 都是通过高斯白噪声转化而来, 大致满足高斯分布, 而噪声 n 本来就满足高斯分布, 所以 $\boldsymbol{U}^{\mathrm{T}}\boldsymbol{A}^{-1}n$ 的值几乎可以肯定会很小. 另一方面, $\boldsymbol{X}_0$ 的幅度要大得多. 因此, $\boldsymbol{U}^{\mathrm{T}}\boldsymbol{A}^{-1}n$ 基本上可以忽略不计, 即有 $\boldsymbol{X}_2\approx\boldsymbol{X}_0$.

2.2　矩阵分析

作为一种公开的图像加密技术, 恶意攻击者总企图从公钥 $\boldsymbol{A}^{-\mathrm{T}}\boldsymbol{U}$ 中计算出私钥 $\boldsymbol{A}\boldsymbol{U}$. 为了防备这种可能性, 对于不同的 $P\times P$ 块, 应该取不同的 $\boldsymbol{U}$. 这样, 除非恶意攻击者获得了全部的 $\boldsymbol{U}$ 矩阵, 否则直接从公钥 $\boldsymbol{A}^{-\mathrm{T}}\boldsymbol{U}$ 中计算出私钥 $\boldsymbol{A}\boldsymbol{U}$ 是不可能的. 同样地, 对于不同的 $P\times P$ 块, 应用不同的变换矩阵 $\boldsymbol{A}$, 也将获得更强的安全性. 为了实验的方便, 每个 $P\times P$ 块都取了相同的 $\boldsymbol{A}$ 和 $\boldsymbol{U}$.

对于矩阵 $\boldsymbol{U}$ 和 $\boldsymbol{A}$ 之间的关系, 假设 $\boldsymbol{A}\in\mathbf{R}^{P\times P}$, 而 $\boldsymbol{U}\in\mathbf{R}^{P\times K}$, 因为 $\boldsymbol{U}$ 是维度为 K 的标准正交基, 所以此时若 P 等于 K, $\boldsymbol{U}$ 成为正交方阵, 容易证明 $\boldsymbol{U}\boldsymbol{U}^{\mathrm{T}}=\boldsymbol{U}^{\mathrm{T}}\boldsymbol{U}=\boldsymbol{E}$, 则有 $(\boldsymbol{A}^{-\mathrm{T}}\boldsymbol{U})(\boldsymbol{A}^{-\mathrm{T}}\boldsymbol{U})^{\mathrm{T}}=(\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}})^{-1}$. 因为存在着矩阵转换关系 $\boldsymbol{A}\boldsymbol{U}=\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}(\boldsymbol{A}^{-\mathrm{T}}\boldsymbol{U})$, 推导出了 $\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}$, 所以实际上等同于从公钥 $\boldsymbol{A}^{-\mathrm{T}}\boldsymbol{U}$ 中计算出私钥 $\boldsymbol{A}\boldsymbol{U}$.

相似地, 若 P 大于 K, $\boldsymbol{U}$ 不是方阵, 则 $\boldsymbol{U}\boldsymbol{U}^{\mathrm{T}}=\boldsymbol{Q}\in\mathbf{R}^{P\times P}$. 因为 $\boldsymbol{U}$ 矩阵的秩为 K, 所以 $\boldsymbol{U}$ 矩阵的行向量不可能是全部两两正交, $\boldsymbol{Q}$ 不是对角矩阵. 从而 $(\boldsymbol{A}^{-\mathrm{T}}\boldsymbol{U})(\boldsymbol{A}^{-\mathrm{T}}\boldsymbol{U})^{\mathrm{T}}=\boldsymbol{A}^{-\mathrm{T}}\boldsymbol{Q}\boldsymbol{A}^{-1}$. 从理论的角度上说, 想从此式推导出 $\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}$, 进而计算出私钥 $\boldsymbol{A}\boldsymbol{U}$ 是肯定不可能的. 所以在生成 $\boldsymbol{U}$ 的时候, 一定要保证 $\boldsymbol{U}$ 不是方阵. P 与 K 之间相差越大, 这类恶意攻击将越艰难.

考察 K 与 P 的取值问题. 如果 P 的取值太大, 就会失去分块的本来意义, 很多图像基本在 256×256 与 512×512 之间. 所以分块长度不能够太大, 否则会失去加密算法的一般性. 但是, 若分块长度 P 太小, 则会导致加密算法运行太慢, 并且加密效果也不佳. 所以本文中 $P=32$. 为了保证取到足够多的系数, K 应该在 $P/2\sim P$ 之间. 本文中 $K=28$. 事实上 P 和 K 也可以作为解密公钥的一部分.

3　实验

对多幅图像进行了实验, 取得了较好的加密效果, 图 1 为对 lena 图像的加解密结果.

图 1　图像加密与解密结果

图 2 为加解密前后图像的灰度直方图. 因为本文在变换域通过矩阵变换进行加密, 所以能够同时改变图像的灰度和频谱. 从图 2 中可以看出加密图像的灰度直方图符合高斯分布, 类似于伪随机噪声, 能够很好地抗统计攻击, 达到较好的隐蔽特性.

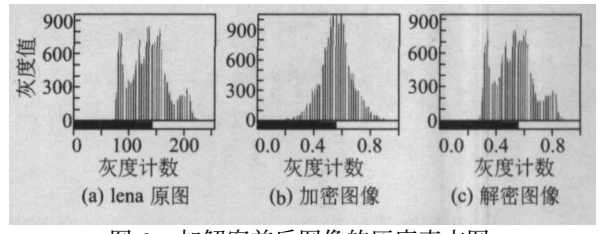

图 2　加解密前后图像的灰度直方图

由于本算法在 DCT 变换域上进行加解密, 因此对于低强度信道噪声、JPEG 有损压缩等方面, 有一定的鲁棒性(见图 3). 可以看出, 单纯的从 bmp 格式转换 JPG 格式, 对于本文解密算法基本上没有影响.

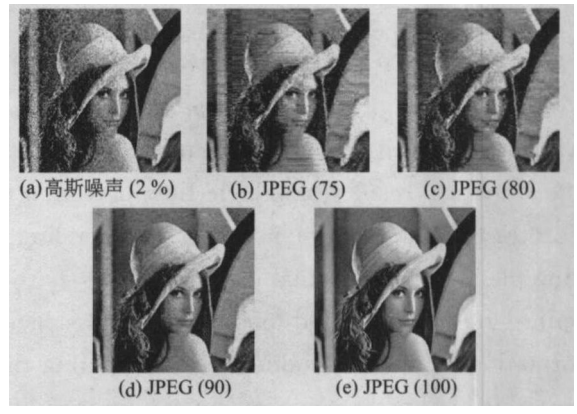

图 3　高斯噪声和 JPEG 压缩对解密图像的影响

本文通过矩阵变换来实现的加密算法, 对于部分图像的水平或者垂直方向操作, 具有一定的抵抗性(如图 4 所示). 图 4 中(a) ~ (d) 分别表示

图 4　水平或垂直方向攻击后的解密结果

在垂直方向放缩为原来的 80 %, 90 %, 110 % 和 120 %. 图 4(e) 和(f) 分别表示在水平方向剪掉加密图像的 1 % 和 5 %. 图 4(g) 为 Frequency Mode Laplacian Removel 攻击简化而来. 图 4(h) 是把原来的加密图像做水平翻转后的解密结果.

(下转第 49 页)

3　实验结果

使用本文方法对实际的四车道交通路口的车辆进行流量统计，得到结果见表 1.

表 1　四车道统计结果

	实际车流/辆	光流法计算结果/辆	误差度百分比/%
车道 1	96	94	2.1
车道 2	88	89	1.1
车道 3	90	88	2.2
车道 4	70	69	1.4

使用背景差法、边缘检测[6]和光流方法对同一车道的车辆进行统计平均比较，结果见表 2.

表 2　三种算法统计结果比较

	实际车流/辆	计算机统计结果/辆	误差度百分比/%
背景差法	85.0	82.5	2.9
边缘检测	85.0	82.8	2.6
光流方法	85.0	84.1	1.1

实验结果表明，该方法检测精度高，同时实现简单、成本较低. 利用本文的基于计算机视觉的光流场检测方法同样可以检测车道占有率、车速等交通参数信息.

参　考　文　献

[1] Boch Erik, Gee Park, Nasu Toshi. New passive traffic detector[J]. IEEE Vehicular Technology Conference, 1997(1): 112-115.

[2] Michalopoulos P G. Vehicle detection through image processing[J]. IEEE Trans on Vehicular Technology, 1991, 40(1): 21-29.

[3] Klein L A, Kelley M R, Mills M K. Evaluation of overhead and in-ground vehicle detector technologies for traffic flow measurement[J]. Journal of Testing and Evaluation, 1997, 25(2): 205-214.

[4] 朱　辉. 视频检测技术在智能交通系统中的应用研究[M]. 西安: 长安大学出版社, 2002.

[5] Horn B K P, Schunck B G. Determining optical flow[J]. Artificial Intelligence, 1981, 17: 185-203.

[6] 郁　梅, 蒋刚毅, 贺赛龙. 基于路面标记的车辆检测和计数[J]. 仪器仪表学报, 2002, 23(4): 386-390.

(上接第 45 页)

基于矩阵变换的非对称加解密算法，既便于实现和提高加解密的速度，又增加了算法的安全性，大量的实验结果证实了本算法的健壮性.

参　考　文　献

[1] 易开祥, 孙　鑫. 一种基于混沌序列的图像加密算法[J]. 计算机辅助设计与图形学学报, 2000, 12(6): 672-676.

[2] Schwartz C. A new graphical method for encryption of computer data[J]. Cryptologia, 1991, 15(1): 43-46.

[3] Bourbakis N, Alexopoulos C. Picture data encryption using SCAN patterns[J]. Pattern Recognition, 1992, 25(6): 567-581.

[4] Kou C J. Novel image encryption technique and its application in progressive transmission[J]. J Electron Imaging, 1993, 2(4): 345-351.

[5] Chang H K, Liou J L. An image encryption scheme based on quadtree compression scheme[C]// Hsieh C H, ed. Proceedings of the International Computer Symposium. New York: IEEE Press, 2001: 230-237.

[6] Chang C C, Hwang M S, Chen T S. A new encryption algorithm for image cryptosystems[J]. The Journal of Systems and Software, 2001, 5(7): 83-91.