一种基于 Android 平台的图像加密方案

王 伟 金 聪
(华中师范大学计算机学院 武汉 430079)

摘 要 智能手机等移动终端在现实生活中已经被广泛使用,由其引发的图像安全性问题也越来越突出,保护智能手机等移动平台中的图像信息安全迫在眉睫。传统计算机平台下的图像加密技术已经得到了广泛的研究和应用,但移动平台受限于当前的硬件架构,无法直接继承传统平台的安全性技术。针对智能手机等移动平台中的图像信息安全问题,提出了一种基于 Android 移动平台的图像加密方案,该方案创新了灰度变换和图像置乱的结合方法。实验研究表明,所提出的方案在图像加密上具有更高的效率,能有效保护移动平台中图像信息的安全性,具有广泛的应用价值。

关键词 移动平台,Android,图像加密
中图法分类号 TP309.2 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.08.020

Image Encryption Scheme for Android Mobile Platform

WANG Wei JIN Cong
(School of Computer, Central China Normal University, Wuhan 430079, China)

Abstract Mobile platform has been widely used in our real life, such as smart phone, which causes the image security problem is becoming more and more prominent. It is extremely urgent to protect the image information security of smart phone. The image encryption technology by traditional computer platform has been be widely researched and applied, but the mobile platform is limited by the current hardware architecture, so that it can not inherit traditional security technology platform directly. Based on Android mobile platform, an image encryption scheme was put forward in this paper which aims at the image information security problems of smartphones and other mobile platforms. And the scheme is an innovation of the combination between gray level transformation and image method. Experiments show that the proposed scheme has higher efficiency in image encryption, which can effectively protect the security of image information in the mobile platform, and has extensive application value.

Keywords Mobile platform, Android, Image encryption

1 引言

近几年,以智能手机为代表的移动终端发展迅猛。随着其制造成本的不断下降和功能的不断更新,普及率也不断上升,多数人都拥有智能手机等至少一台移动设备。随着人们生活节奏的加快,得益于移动设备的便携性等优点,越来越多的人使用智能手机等移动设备的时间开始多于传统计算机(如台式机、笔机本电脑等)。但是与此不同步的是人们在移动设备上的安全意识却没有多于传统计算机,传统计算机的信息安全技术经过几十年的发展已经日趋成熟,但其受限于移动平台的硬件架框和网络环境,因此照搬传统安全保护技术并不适用。当前,由智能手机等移动设备引发的图像信息安全问题屡见不鲜,保护移动平台的信息特别是图像信息安全迫在眉睫。

目前智能手机等移动设备中应用的移动平台很多,但主要有3个,分别是苹果公司的 ios 平台、谷歌公司的 Android 平台、微软公司的 WinPhone 平台。苹果公司的 ios 平台和微软公司的 WinPhone 平台是其开发的商业化移动操作系统,具有较强的封闭性,安全性较高。而由谷歌公司发布的 Android 平台由于自身的开放性而广受欢迎且占用率高,但是其安全性却较低。因此,本文主要解决 Android 平台的图像信息安全问题,需要考虑的问题有:保证图像在智能手机中的存储安全性、图像在移动环境下的传输安全性和保密算法的高效实用性。

2 相关工作

2.1 传统图像加密技术分析

传统的图像加密技术主要基于现代密码体制。通常将图像像素信息看作一维数据流,在密钥的控制下,利用加密算法(常用加密算法如 EDS、AES、RC6 等)进行加密。但现代密码体制主要是为文本信息设计,而没有考虑到数字图像数据量大、相关性强、空间有序等特点,故对图像信息加密具有较大的计算量,加密效率也不高。随着人们对多媒体信息的安全越来越重视,研究者提出了多种针对图像的加密技术,其主要的思想是将数字图像进行灰度变换和图像置乱[1]。灰度变换是指改变图像像素点的灰度值的大小,使得加密前后,像素

到稿日期:2013-05-31 返修日期:2013-06-20 本文受武汉市科技攻关计划(201210121023)资助。

王 伟(1989-),男,硕士生,主要研究方向为信息安全、移动服务安全,E-mail:wwgzyx@sina.com;金 聪(1960-),女,博士,教授,主要研究方向为信息安全、版权保护。

序列的内容完全改变，N K Pareek 等人利用灰度变换对图像进行加密[2]，得到了较好的加密效果。图像置乱就是将图像的信息次序打乱，将 a 像素移动到 b 像素的位置上，b 像素移动到 c 像素的位置上等，使其变换成杂乱无章难以辨认的图像。Yoon J W 等人首先利用混沌系统构造随机序列，然后将像素矩阵的行或者列按照随机序列重新排列[3]，得到了比较理想的加密效果。但这些方法，一般在灰度变换或者构造随机序列的过程中需要较大的计算量，如果直接移植到移动平台，可能会影响图像加密速度。

2.2 混沌系统

混沌是非线性系统中出现的一种貌似无规则的类随机过程，是普遍存在的复杂运动形式和自然现象。混沌系统一般都具有对初始条件的敏感依赖性、整体稳定而局部不稳定、轨道不稳定及分岔、长期不可预测性等特点。此系统由于具有良好的随机特点，因此经常应用于图像加密算法[3-8]。混沌系统中常见的有 Logistic 系统和 tent 系统。

Logistic 映射源自于对人口统计的动力学系统，是一个典型非线性混沌方程。它具有遍历性、非周期性、长期不可预测性以及非收敛性等良好的混沌性质，其映射定义为(当系数 $3.596\leqslant a\leqslant 4$ 时，系统进入混沌状态)：

$$x_{n+1}=a*x_n*(1-x_n)\quad 0<x_n<1,n=0,1,2,\cdots \tag{1}$$

Tent 系统是一种分段线性的一维映射，具有均匀的概率密度与功率谱密度，以及较理想的自相关性。Tent 映射定义为(其中当 $0<a\leqslant 2$ 时，系统处于混沌状态)：

$$x_{n+1}=\begin{cases}ax_n, & 0\leqslant x_n\leqslant 0.5\\ a(1-x_n), & 0.5<x_n\leqslant 1\end{cases} \tag{2}$$

3 Android 移动平台图像加密

3.1 算法设计思想

本文通过对图像加密技术的研究，提出了一种创新的移动平台图像加密算法。首先将待加密图像矩阵 I 分成若干个小的矩阵块；再利用图像置乱与灰度变换处理每一个小的分块；然后把每个分块内的像素值发散到其他分块内；最后将所有分块合成加密后的图片，加密流程如图 1 所示。本算法在保证加密效果的同时，减少了图像置乱处理所需要的计算量，使之适合在移动平台上加密图像。

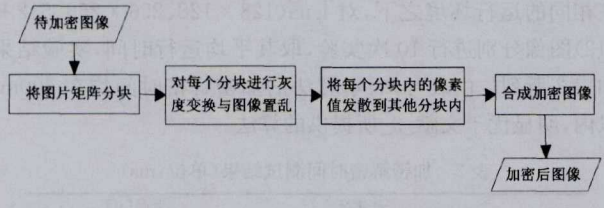


图 1 加密流程图

3.2 加密算法描述

(1)预处理

对于原始图片 I，其像素矩阵大小为 $M\times N$，扩充(用 0 填充)像素矩阵使其大小变为 $M'\times N'$，使得其中 M'、N' 为完全平方数，不妨设 $\sqrt{M'}=m$，$\sqrt{N'}=n$。将 $M'\times N'$ 的像素矩阵按顺序分成 $m\times n$ 个大小为 $m\times n$ 的分块。为了方便起见，用二维数组 $A[i][j]$ 来表示第 (i,j) 个分块。用二维数组 $B_{A[i][j]}[x][y]$ 来表示分块 $A[i][j]$ 中的像素值(其中 $0\leqslant i\leqslant m-1$，$0\leqslant j\leqslant n-1$，$0\leqslant x\leqslant m-1$，$0\leqslant y\leqslant n-1$)。为了增加安全性，先将 Logistic 混沌系统和 Tent 混沌系统分别迭代 $key1$、$key2$ 次。迭代次数 $key1$、$key2$ 作为加密密钥。其中 Logistic 的初值作为密钥 $key3$，参数 a 作为密钥 $key4$。其中 tent 系统的初值作为密钥 $key5$。参数 b 作为密钥 $key6$。

(2) 分块内的处理

利用 Logistic 混沌系统构造序列 $T[m\times n]$，使得 $0\leqslant T[i]\leqslant m\times n-1$，其中 $0\leqslant i\leqslant m\times n-1$，并且有 $T[i]\neq T[j]$，当 $i\neq j$ 时。对每个分块内像素值的处理方法如下，以分块 $A[i][j]$ 为例。

a)构造置换数组

利用 tent 混沌系统产生一个随机数 $temp$。将 $temp$ 分别与每一个 $T[r](r=0,1,2,3,\cdots m\times n-1)$ 相加，再对 $m\times n$ 取余，得到新的序列 $T[m\times n]$。公式表述：

$$T'[r]=(temp+T[r])\bmod(m\times n) \tag{3}$$

b)按照序列 $T'[m\times n]$ 的顺序，置换分块内的像素值。如对于 $B_{A[i][j]}[x][y]$，首先计算置换位置，设

$$k_1=T[x\times n+y]/(m\times n),k_2=T[x\times n+y]\%(m\times n) \tag{4}$$

则 $B'_{[Ai][j]}[k_1][k_2]=B_{A[i][j]}[x][y]$，其中 $0\leqslant x\leqslant m-1$，$0\leqslant y\leqslant n-1$。

c)异或操作。对于分块内的每一个像素值 $B'_{A[i][j]}[x][y]$，利用 tent 混沌系统产生一个伪随机数 e，再将像素值 $B'_{A[i][j]}[x][y]$ 与 e 异或。即：

$$B'_{A[i][j]}[x][y]=B'_{A[i][j]}[x][y]\wedge e \tag{5}$$

d)按照 a)－c)步骤，依次处理每一个分块。

(3)分块间的处理

将每个分块内的像素值发散到其他分块内。将第 (i,j) 个分块像素值 $B'_{A[i][j]}[x][y]$ 发散到第 (i,j) 个分块中的 (i,j) 位置。即：

$$B''_{A'[x][y]}[i][j]=B'_{A[i][j]}[x][y] \tag{6}$$

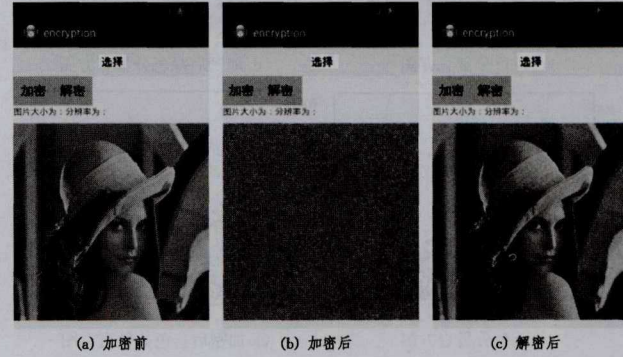
(4)将步骤(3)处置之后的分块按列序优先从小到大的顺序排列，得到加密后的图像 I'。

3.3 解密算法描述：

利用加密时密钥 $key1$、$key2$、$key3$、$key4$、$key5$、$key6$ 的值，按照加密的逆过程解密，然后去掉添加的多余数据(如果存在)，即可得到解密后的图像。

4 实验分析

实验的测试平台为双核 CPU，其型号为 ARM Cortex-A9，频率为 1024MHz，RAM 容量为 1GB，搭载 Android 4.0 操作系统。利用本文的算法对 Lena(256×256)加密的效果如图 2 所示。图 2(a)为加密前的图像，图 2(b)为加密后的图像，图 2(c)为解密后的图像，由图可知，通过本算法，达到了较好的加密效果，通过加密后的图像无法看到原图的信息。



(a) 加密前　(b) 加密后　(c) 解密后

图 2 加密解密效果图

4.1 密钥敏感性分析

通过对密钥做微小的改变来测试密文对密钥的敏感性。为了简单起见，这里只测试对密钥 $key3$ 的敏感性。将 couple(256×256)图像作为用例，不妨令 $key3=0.9000000$。图 3(a)为加密前的图像，图 3(b)为加密后的图像，图 3(c)为输入正确密钥 $key3=0.9000000$ 后得到的解密图像。图 3(d)为输入错误密钥 $key3=0.90000001$ 后得到的解密图像。

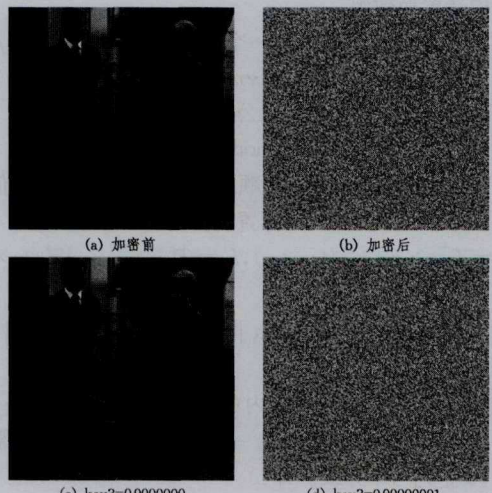


图 3 密钥敏感性分析

4.2 直方图分析

Lena 图像加密前后的直方图对比如图 4 所示，该直方图是一幅图像像素有序分布的图表，反映了图像处理之后像素的分布。由图 4 可知，加密后直方图分布非常均匀，掩盖了图像加密前像素值的分布规律，从而可以有效地抵抗统计分析和已知密文攻击。

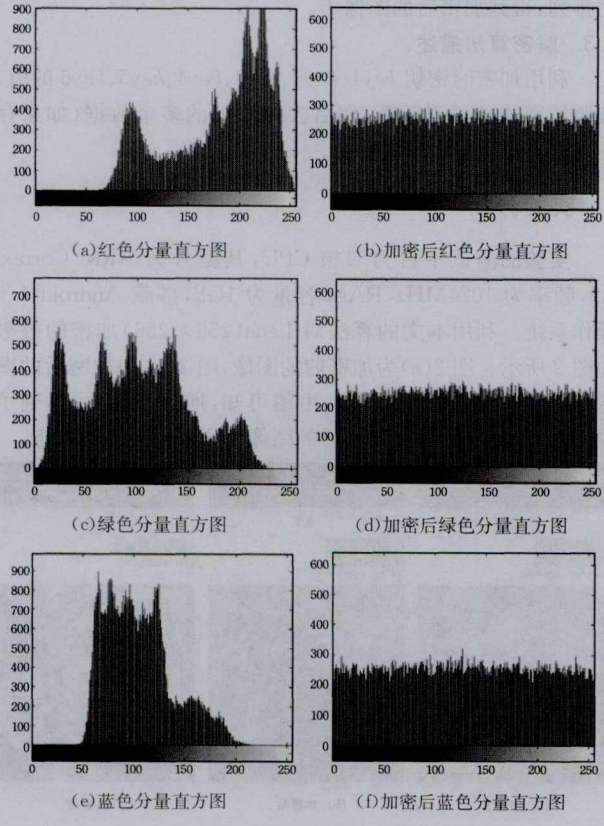


图 4 原图像和加密后图像分量的直方图对比

4.3 相关性分析

加密效果之一是尽可能地降低相邻像素的相关性，用如下离散化式计算相关系数：

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\cdot\sqrt{D(y)}} \tag{7}$$

随机在水平、垂直方向各选取 1000 对相邻像素值，利用上面的公式计算出相关系数，如表 1 所列。通过对比加密前后的相关系数，可以发现本算法有效地减小了相邻像素值之间的相关性。

表 1 平均相关系数比较

	垂直方向			水平方向		
	红色分量	绿色分量	蓝色分量	红色分量	绿色分量	蓝色分量
加密前	0.90958	0.93305	0.95413	0.95413	0.95413	0.95413
加密后	0.05440	−0.0529	−0.0829	−0.0996	−0.0698	0.0543

4.4 信息熵分析

图像信息熵是一种特征的统计形式，它反映了图像中平均信息量的多少。在信息论中，一个系统越是有序，信息熵就越低；反之，一个系统越是混乱，信息熵就越高。所以信息熵也可以说是系统有序化程度的一个度量。

对图像信息熵的计算，可利用如下公式：

$$H=\sum_{0}^{255}p(i)\log p(i) \tag{8}$$

其中，$p(i)$表示图像中灰度值为 i 的像素所占的比例。利用以上公式可计算出加密前后的信息熵，表 2 为加密前后的信息熵的比较，从中看出加密后的各个颜色分量的信息熵均大于加密前的信息熵，说明加密后图像中的信息变得混乱，达到了加密的效果。

表 2 信息熵比较

	信息熵		
	红色分量	绿色分量	蓝色分量
加密前	7.2378	7.5721	6.9260
加密后	7.9966	7.9971	7.9967

4.5 加密解密时间测试

通过本算法与文献[9]中的算法相对比来验证本算法适应于移动设备，且加密解密时间短于文献[9]所提供的算法。在相同的运行环境之下，对 lena(128 * 128、256 * 256、512 * 512)图像分别进行 10 次实验，取其平均运行时间，实验结果如表 3 所列。由表可知，本算法的加密解密时间均在 300ms 以内，明显优于文献[9]所提供的算法。

表 3 加密解密时间测试结果(单位：ms)

图像大小	本算法		文献[9]	
	加密时间	解密时间	加密时间	解密时间
128 * 128	70	68	217	226
256 * 256	261	269	1403	1398
512 * 512	298	287	1685	1576

结束语 本文通过对常用图像加密技术的研究，设计了一种针对智能手机的图像加密算法。为了提高加密速度，先将图像分块，对每个分块进行处理，然后再将每个分块内的像素值分散到其他分块内，最后组合生成加密后的图像。通过实验对加密后图像的效果分析，证实了该算法能有效地应用于移动智能平台，得到了较好的加密结果。该算法与计算机中的图像加密算法相比，在加密效果上还存在一定的差距，在以

(下转第 108 页)

nally 块的最后一条语句连接至 except_exit 节点。

7)对于 throw 节点,生成一个与抛出的异常关联的节点,若该语句在 try 块中,连接异常节点到对应的最近一个 catch 节点,若该语句不在 try 块中,连接异常节点至异常退出点 except_exit;若 throw 节点后存在 finally 节点,应将该节点首先连接到 finally 节点,然后将 finally 块的最后一条语句连接至 except_exit 节点。

8)对于 finally 节点,直接连接其与下一条语句。

相比于文献[10],本算法引入了 finally 节点,并对原有的 try、catch、throw 等节点进行了改进,以符合 Java 语言的异常传播特点。下面是一个函数内异常控制流图的构造实例。

代码 3

```
public static void readFile(String fileName) throws IOException{
1. File file=new File(fileName);
2. Reader reader=null;
3. try{
4. reader=new InputStreamReader(new InputStream(file));}
5. catch(e) {
6. throw new ReadException ();}
7. finally{
8. reader. close;}}
```

按照上述构造方法构造的控制流图如图 2 所示。

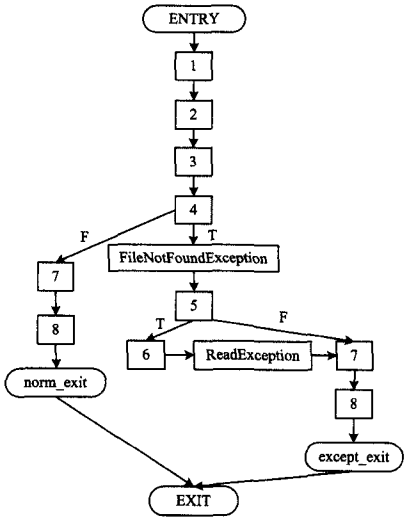


图 2 异常控制流图

插件在程序抽象语法树和中间表示的基础上,分析程序的异常信息,并根据上述构造方法,生成异常控制流图,在此基础上,开发人员进行控制流和数据流分析、程序优化等,进而提高软件健壮性。

结束语 本文提出通过分析异常类型和层次关系,给出代码提示的方法,以解决开发人员注重程序逻辑、忽视异常处理的问题。针对 Java 语言的异常处理特点,本文在已有的异常控制流图基础上引入了 finally 节点来重新定义 try、catch、throw 等异常节点的构造方法,提出了 Java 异常控制流图的构造方法,为程序分析奠定了基础。Eclipse 平台下的异常信息分析插件可以显示 Java 程序异常信息、代码提示,生成异常控制流图,帮助开发人员合理地使用 Java 异常机制和程序分析,提高程序开发效率和软件健壮性。

参 考 文 献

[1] Sawadpong P, Allen E B, Williams B J. Exception Handling Defects: An Empirical Study[C]// 14th International Symposium on High-Assurance Systems Engineering. Omaha, USA, October 2012: 90-97

[2] Rashkovits R, Lavy I. Students' Misconceptions of Java[C]// 7th Mediterranean Conference on Information System. Guimaraes, Portugal, September 2012: 1-21

[3] 姜淑娟,徐宝文. 异常处理——一种提高软件健壮性的方法[J]. 计算机科学,2003,30(9):169-172

[4] 姜淑娟. 异常传播分析技术及其应用研究[D]. 南京:东南大学,2006

[5] 姜淑娟,徐宝文,姜元鹏. 一个异常传播分析工具的设计与实现[J]. 计算机科学,2008,35(7):277-279

[6] Robillard M P. Analyzing exception flow in Java programs [D]. The University of British Columbia, 1999

[7] Robillard M P, Murphy G C. Designing Robust Java Programs with Exception[C]// 8th ACM SIGSOFT international symposium on Foundation of software engineering. 2000: 2-10

[8] Chang B-M, Jo Jang-wu. Visualization of Exception Propagation for Java using Static Analysis[C]// 2nd IEEE International Workshop on Source Code Analysis and Manipulation. Canada, 2002: 173-182

[9] 陈红跃,张宏军,陈刚. Java 异常处理策略研究[J]. 计算机技术与发展,2012,22(7):9-12

[10] Zhang Yan-mei, Jiang Shu-juan, Zhao Xue-feng. Analysis of Object-oriented Programs with Exception-Handling Constructs[J]. International Journal of Advancements in Computing Technology, 2012, 4(1): 505-515

(上接第 96 页)

后的研究中,将会增强加密效果,保护个人手机中图像的隐私。

参 考 文 献

[1] 张云鹏,左飞,翟正军. 基于混沌的数字图像加密综述[J]. 计算机工程与设计,2011,32(2):463-466

[2] Pareek N K, Patidar V, Sud K K. Image encryption using chaotic logistic map [J]. Image and Vision Computing, 2006, 24(9): 926-934

[3] Yoon J W, Kim H. An image encryption scheme with a pseudo-random permutation based on chaotic maps [J]. Commun Nonlinear Sci Numer Simulat, 2010, 15(12): 3998-4006

[4] Wang Yong, Wong K-W, Liao Xiao-feng, et al. A new chaos-based fast image encryption algorithm [J]. Applied Soft Computing, 2010, 11(1): 514-522

[5] Singh N, Sinha A. Chaos based multiple image encryption using multiple canonical transforms [J]. Optics & Laser Technology, 2010, 42(5): 724-731

[6] Lin Qiu-hua, Yin Fu-liang, Mei Tie-min, et al. A blind source separation-based method for multiple images encryption [J]. Image and Vision Computing, 2008, 26(6): 788-798

[7] Liao Xiao-feng, Lai Shi-yue, Zhou Qing. A novel image encryption algorithm based on self-adaptive wave transmission [J]. Signal Processing, 2010, 90(9): 2714-2722

[8] Chen W, Quan C, Tay C J. Optical color image encryption based on Arnold transform and interference method [J]. Optics Communications, 2009, 282(18): 3680-3685

[9] Gao Tie-gang, Chen Zeng-qiang. A new image encryption algorithm based on hyper-chaos [J]. Physics Letters A, 2008, 372(4): 394-400