适用于 Android 手机的像素异或图像分块加密算法*

涂正武 金 聪
(华中师范大学计算机学院 武汉 430079)

摘 要：为了克服 Android 手机上图像加密速度慢的缺点，提出了一种适用于 Android 手机的像素异或图像分块加密算法，该算法将密码学中经典的 RC4 算法应用于本文的加密算法中。首先，将原始图像分块，将改进的 RC4 算法运用到相邻的两个子块之间的运算上，从而改变像素值，最后，通过 Logistic 映射对图像置乱。实验结果表明，原始图像加密后的图像类似噪声，加密后的直方图变得更平滑，有足够大的密钥空间，对密钥有很高的敏感性，密文图像的随机性好，密文图像相邻像素之间相关性低，加密算法在 Android 手机上有更快的加密速度。

关键词：像素异或；Android 手机；图像加密；Logistic 映射；图像分块
中图分类号：TP309.2 **文献标识码**：A **国家标准学科分类代码**：520.6040

Image block encryption algorithm based on pixel xor for Android phone

Tu Zhengwu Jin Cong
(School of Computer Science, Central China Normal University, Wuhan 430079, China)

Abstract: In order to overcome the slow speed of image encryption for android phone, an image block encryption algorithm based on pixel xor is proposed for the Android Phones. In this algorithm, the classic RC4 algorithm in cryptography is modified, and then applied to this paper's encryption algorithm. Firstly, the original image is divided into blocks. Then, the improved RC4 algorithm is applied to the operation between the adjacent two sub-blocks, thereby changes the value of pixels. Finally, the image is scrambled by logistic map. Experimental results show that the image has a noise-like characteristic and a flat histogram after the original image is encrypted, and that the algorithm has an enough large key space, a very high sensitivity to the key and a fast speed of image encryption for android phone and the encrypted image has a good randomness and has a low correlation between two adjacent pixels.

Keywords: pixel xor; android phone; image encryption; logistic map; image block

1 引 言

随着移动互联网时代的到来，手机已经成为了人们信息交流中不可或缺的一部分，在手机的信息传输中，图像的传输非常频繁。那么手机上图像传输的安全是人们主要关心的问题，Android 手机操作系统作为主流的手机操作系统，为了满足用户对私密信息进行保护的需求，基于 Android 平台的图像安全的研究和开发显得很有必要。由于 Android 手机内存小、运算能力有限，研究适用于 Android 手机、加密效果好、时间复杂度和空间复杂度小的加密算法成为了一个新的挑战。

混沌具有对初始值与系统参数的敏感性、白噪声的统计特性和序列遍历性等特点，符合密码学要求的扩散、置乱和随机特性。研究者利用混沌对数字图像的加密主要分 3 类：

1)利用混沌映射产生伪随机序列改变明文像素的灰度值，如 Logistic 映射[1]、Lorenz 映射[2]；

2)采用混沌映射置乱图像像素的位置，如 Logistic 映射[3]、Arnold 变换[4]、Tent 映射[5]；

3)两种方法相结合使用。

针对混沌的这些优点，本文中图像加密算法同时采用了混沌映射来置乱像素位置和改变像素值。

无论图像加密还是文本加密，很难做到兼顾安全和速度。图像加密为了追求图像的安全性而设计复杂的加密算法结构，这样导致其加密的速度常常比较慢；而有些图像加密为了追求加密的速度使得设计的算法结构过于简单，这样导致其算法的安全性不好，容易被破解。为了在保证安全性的前提下最大地提高加密速度，将图像分割为固定大小的像素分块，以像素分块为最小的操作单元。最近，有一些基于像素分块的图像加密算法提出，如文献[6-8]。

收稿日期：2015-01
* 基金项目：武汉市科技攻关计划(201210121023)项目

提出了适用于 Android 手机的像素异或图像分块加密算法。该算法对密码学中的经典算法 RC4 算法[9]进行修正,应用于数字图像的加密过程中,使得图像的像素值发生较大的变化,从而满足图像在传输过程中安全性和可靠性的要求。首先,将原始图像划分为 8×8 大小的子块,另外,由 Logistic 映射得到一串伪随机数,将这串伪随机数组成一个 8×8 大小的伪随机块;其次,通过改进的 RC4 算法,在相邻的两个子块之间做运算;最后,由 Logistic 映射对整个图像置乱,得到密文图像。

2 加密算法

本文中的加密算法主要由图像分块、伪随机块生成、块与块的运算、块间像素异或、图像置乱组成。该算法的结构如图 1 所示。

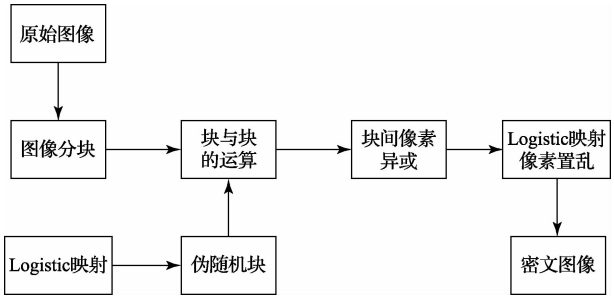


图 1 加密算法的结构

2.1 图像分块

假定原始图像 I 的大小为 $M\times N$,则原始图像 I 的像素值是 $I(i,j)$, $i=0,1,\cdots,M-1$; $j=0,1,\cdots,N-1$。将原始图像 I 分块,每个子块的大小为 8×8,可以分成 $m\times n$ 个子块,则每一个子块可以表示为 $I_{s,t}$, $s=0,1,\cdots,m-1$; $t=0,1,\cdots,n-1$。每一个子块内的每一个像素可以表示为 $I_{s,t}(p,q)$, $p=0,1,\cdots,7$; $q=0,1,\cdots,7$。

$$\begin{cases} m=M/8 \\ n=N/8 \end{cases} \tag{1}$$

原始图像像素与子块像素之间的转换:

$$I_{s,t}(p,q)=I(i,j) \tag{2}$$

式中:$s=i/8$, $t=j/8$, $p=i\%8$, $q=j\%8$。

2.2 伪随机块生成

该伪随机块是由 Logistic 映射生成的伪随机序列组成的。

对于 Logistic 映射:

$$x_{n+1}=4x_n(1-x_n),x_0\in(0,1),x_0\neq 0.5 \tag{3}$$

1)通过给定的密钥 key_1,得到 Logistic 映射的初始值 x_0, key_1 的取值范围为 1~9 999 999;

$$x_0=key_1/10^8 \tag{4}$$

2)由初始值 x_0,Logistic 映射迭代 N_0 次。本文实验中,N_0 取值 100;

3)继续迭代 8×8 次,由式 $l=x_0\times 2^{24}$,得到一组伪随机序列$\{l_i,i=1,2,\cdots,64\}$;

4)由这组伪随机序列组成伪随机块 J,则 $J(i,j)=m_{j+8\times i}$。

2.3 块与块的运算

每一个子块表示为 $I_{s,t}$,也可以表示成一维:

$$I_u,u=0,1,\cdots,m\,n-1,I_u=I_{t+8\times s}=I_{s,t} \tag{5}$$

第 1 个子块 I_0 与伪随机块 J 运算,得到新的第一个子块,仍记为 I_0,之后让 I_0 与 I_1 运算,得到新的 I_1,仍记为 I_1;如此继续下去,直到最后一个子块。计算公式如下:

$$\begin{cases} I_u=I_u\otimes J, & \text{当 } u=0 \text{ 时} \\ I_u=I_u\otimes I_{u-1}, & \text{当 } 0<u<mn \text{ 时} \end{cases} \tag{6}$$

2.4 块间像素异或

本文中,块间像素的异或采用的是一种应用到图像加密中的 RC4 算法,将这种运算记为 $\otimes$。

相邻的两个子块 I_u, I_{u-1} 之间像素的异或 $I_u\otimes I_{u-1}$,如下所示:

1)将两个二维的子块折叠为一维。

$$I_u(k)=I_u(q+8p)=I_u(p,q) \tag{7}$$

$$I_{u-1}(k)=I_{u-1}(q+8p)=I_{u-1}(p,q) \tag{8}$$

2)定义一个大小为 64 的数组 S-box 为 $s[64]$,初始化该 S-box:

$$s[i]=i,i=0,1,\cdots,63 \tag{9}$$

3)通过字符串密钥 key_3 随机交换两个 S-box 的值,来打乱 S-box。由密钥 key_3 转化为大小为 64 的字节数组 $k[i]$,得到另一个 S-box 的序号值 j,交换 $s[i]$和$s[j]$。字符串密钥 key_3 的长度不得小于 8。字符串密钥 key_3 中每个字符的取值范围是 0~255,该字符串密钥 key_3 至少含有 8 个字符,

$$k[i]=key_3[i\%length],j=(j+s[i]+k[i])\%64 \tag{10}$$

式中:length 是字符串密钥 key_3 的长度。

4)交换两个 S-box 的值和,并取这两个的值为序号 r。

$$j=(j+s[i])\%64,r=(s[i]+s[j])\%64 \tag{11}$$

5)由 i 和 j 可以依次得到一组序号 r,依次选取后一个子块的像素 I_u 依次与前一个子块 I_{u-1} 的第 r 个像素 $I_{u-1}(r)$异或。

$$I_u(k)=I_u(k)\oplus I_{u-1}(r) \tag{12}$$

最后将所有异或后的子块合并,得到图像 E_1。

2.5 图像置乱

由异或得到的图像 E_1,通过逻辑映射对图像 E_1 的位置进行置乱,最终得到密文图像 E_2。

由 Logistic 映射得到一组伪随机序列,Logistic 映射公式如下:

$$x_{n+1}=4x_n(1-x_n);x_0\in(0,1),x_0\neq 0.5 \tag{13}$$

本文中的图像置乱就是通过这组伪随机序列进行的。

图像置乱的过程如下:

1)通过给定的密钥 key_2,得到 Logistic 映射的初始值 x_0,key_2 的取值范围为 1～99 999 999

$$x_0 = key_2/10^8 \tag{14}$$

2)将 Logistic 映射迭代 N_0 次,N_0 是常量,本文实验中,N_0 取值 100。

3)依次遍历密文图像 E_1 的每个像素,每遍历一个像素 $E_1(i,j)$就迭代一次 Logistic 映射,得到一个随机数 x_i,由 x_i 可得到序列数 m_i,

$$m_i = \lfloor x_i \times (M \times N) \rfloor \tag{15}$$

式中:$M \times N$ 是密文图像 E_2 的大小,$\lfloor\ \rfloor$ 是向下取整运算。

4) 如果像素 $E_2(p,q)$ 已被占据,继续执行 3);直到有像素 $E_2(p,q)$ 没有被占据,那么将像素 $E_1(i,j)$ 置换到 $E_2(p,q)$。

$$E_2(p,q) = E_1(i,j) \tag{16}$$

式中:$p = m_i/M$,$q = m_i \% M$。最终,得到的 $E_2(p,q)$ 就是对图像 E_1 置乱后得到的密文图像。

3　解密算法

与加密算法比较,解密算法就是加密算法的逆过程,只是块与块的运算和图像置乱有一些不同,其他部分和加密算法一样。首先,将密文图像 E_2 按 Logistic 映射置乱解密,得到图像 E_1,再划分为 8×8 的子块,然后,让子块与子块之间的像素异或,最后将子块合并得到最终解密后的图像 I。

3.1　图像置乱的逆过程

在解密过程中,通过 Logistic 映射对密文图像 E_2 解密,得到图像 E_1。

解密过程中,1)、2)、3)都与加密算法中图像置乱一样,只是 4)有点出入。

4)如果像素 $E_2(p,q)$已被置换,继续执行 3);直到像素 $E_2(p,q)$没有被置换,那么将像素 $E_2(p,q)$置换到 $E_1(i,j)$:

$$E_1(i,j) = E_2(p,q) \tag{17}$$

3.2　块与块运算的逆过程

同加密时一样,将图像 E_1 分块,每一个子块表示为 I_u,$u = 0,1,\cdots,mn-1$。解密时,从最后一个子块 I_{mn-1} 开始解密。最后一个子块 I_{mn-1} 与它前面的一个子块 I_{mn-2} 运算得到解密后的最后一个子块,仍记为 I_{mn-1};依次让子块 I_u 与其前一个子块 I_{u-1} 运算,直到第一个子块 I_0,让第一个子块 I_0 与 Logistic 映射导出的伪随机块 J 运算,这与加密时的顺序正好相反。公式如下:

$$\begin{cases} I_u = I_u \otimes J, & \text{当 } u = 0 \text{ 时} \\ I_u = I_u \otimes I_{u-1}, & \text{当 } 0 < u < mn \text{ 时} \end{cases} \tag{18}$$

4　实验结果

本文的实验是在 Android 手机三星 i699 上进行测试的,CPU 频率为 1 G,RAM 为 512 M。本实验中,原始图像分别取大小为 256×256 的 Lena 图像、大小为 512×512 的 Baboon 图像、大小为 512×512 的 Peppers 图像;加密时选取的密钥组为 key_1 = 88 888 888,key_2 = 88 888 888,key_3 = abcdefgh。经本文方法加密后,加密前后和还原前后图像的对比,如图 2 所示。

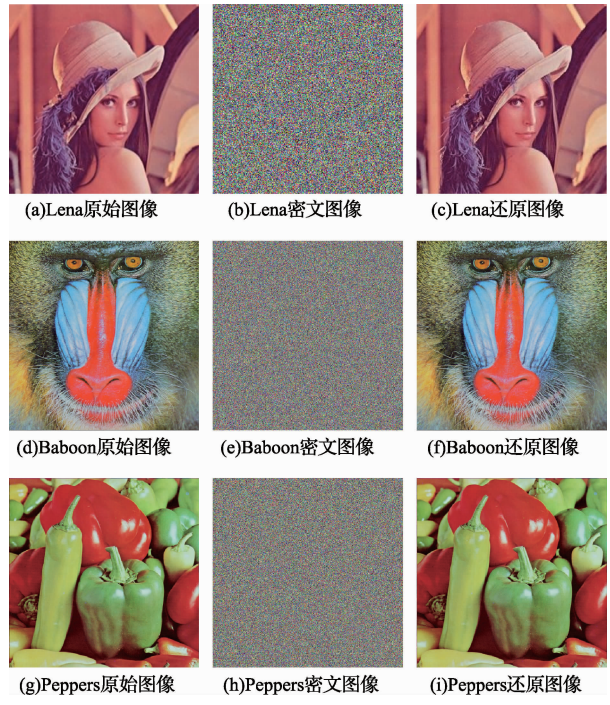


图 2　实验图像加密、还原前后的对比

实验结果中,原始图像经本文中的算法加密后得到的密文图像是一种类噪声图像,这种密文图像不可能用肉眼看出任何原始图像的信息,并且还原后的图像和原始图像完全一致,表明本文中的算法加密和还原的效果都很理想。

5　安全性分析

5.1　密钥空间分析

加密算法的密钥由两个 Logistic 映射的密钥 key_1,key_2 和像素异或时的字符串密钥 key_3。因为 key_1,key_2 被设置成 8 位的十进制整数,而 key_3 至少含有 8 个字符,则本文中加密算法的最小密钥空间是 10^{32}。这个密钥空间已经足够大的抵抗穷举攻击。

5.2　密钥敏感测试

加密算法的密钥敏感测试如图 3 所示,该测试中使用密钥组 K_1(key_1 = 88 888 888,key_2 = 88 888 888,key_3 = abcdefgh)对原始图像(a)加密,得到密文图像(b)。使用相同的密钥组 K_1 对密文图像(b)解密得到正确的还原图像(c)。然后对密钥组 key_1 作一个很小的改变得到密钥组 K_2(key_1 = 88 888 889,key_2 = 88 888 888,key_3 = abcdefgh),使用密钥组 K_2 对密文图像(b)解密,得到错误的还原图像(d),其还是一种类噪声图像。

图 3 密钥敏感性测试

从这个敏感性测试可以看出,密钥只要有一个很小的改变,都使得解密的结果大不相同,这说明本文中的加密算法对密钥有很高的敏感性。

5.3 直方图分析

图像的直方图显示图像中像素的分布密度,一个平滑、均衡的密文图像可以很好的抵制统计攻击。图 4 中显示了 Lena 图像在加密前后 R、G、B 3 个分量直方图的对比。

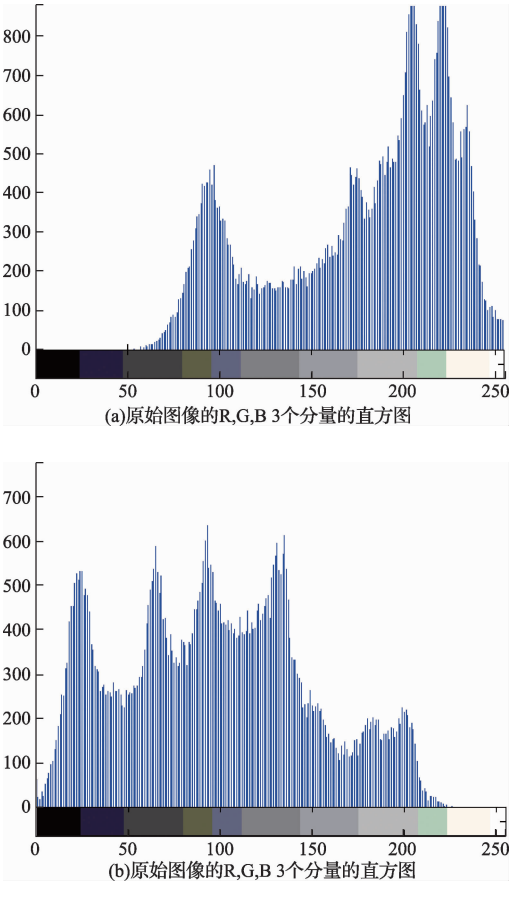


图 4 Lena 图像加密前后直方图的对比

从图 4 中直方图的对比可以看出，密文图像的 R、G、B 3 个分量的直方图与原始图像比较有了很大的改变，其直方图变得平滑和均衡化了，能够有效的抵制统计攻击，很难从密文图像的直方图来破译该密文图像。

5.4　信息熵分析

信息熵是用来衡量随机变量的随机性的，计算信息熵的公式如下：

$$H_L = \sum_{l=0}^{F-1} P(L=l)\log_2 \frac{1}{P(L=l)} \tag{19}$$

式中：F 是灰度级，$P(L=l)$ 是灰度值等于 l 的像素的百分比。

图像的信息熵可以用来衡量图像的随机性，图像信息熵的值越接近信息熵的最大值，那么其随机性就越好。表 1显示了在加密前后图像信息熵的值。

表 1　原始图像和密文图像信息熵对比

图像名	图像大小	原始图像信息熵	本文算法加密后的图像的信息熵
Lena	256×256	7.758 4	7.991 1
Baboon	512×512	7.762 4	7.991 9

从表 1 可知，图像越大信息熵的值越大，原始图像信息熵的偏小，不接近 8；经过本文算法加密后的密文图像信息熵的值非常接近 8。这说明原始图像的随机一般，应用本文的加密算法后，密文图像的随机性非常理想。

5.5　相关性分析

原始图像在水平、垂直、对角方向的相邻像素之间都存在很高的相关性。加密算法的目的就是为了破坏这种相关性，将原始图像加密为类噪声的没有或很少相关性的图像。这样，破译者就很难通过像素之间的相关性对密文图像进行破译。

相邻两个像素之间的相关值可以由如式(20)计算：

$$C_{xy} = \frac{E[(x-\mu_x)(y-\mu_y)]}{\sigma_x \sigma_y} \tag{20}$$

式中：μ 和 σ 分别是像素值的均值和标准差。

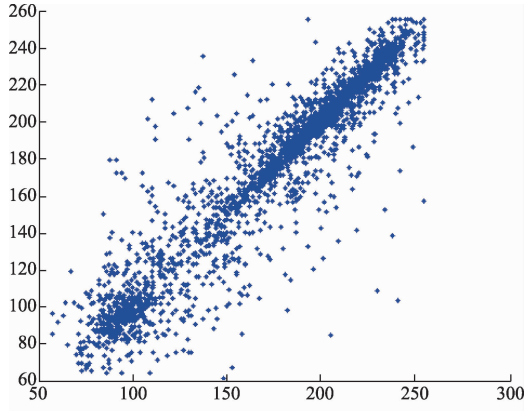
一个良好的密文图像应不能被肉眼识别出原始图像的痕迹，与其相关值应趋近于 0。在实验中，分别从水平、垂直、对角 3 个方向对相关值测试，并和文献[8]的算法进行对比，表 2 中的实验结果是通过从原始图像和密文图像中随机选取 3 000 对相邻像素进行测试得到的。

表 2　原始图像和密文图像的相关值对比

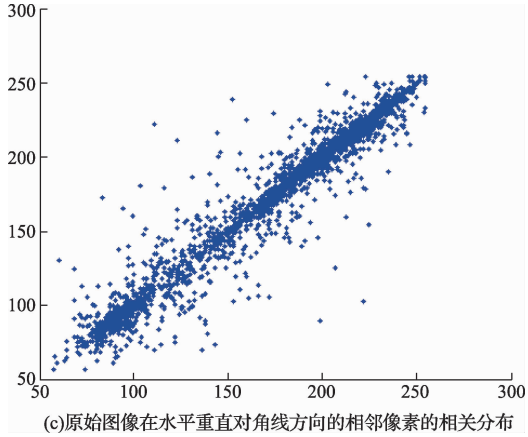
	加密算法	水平方向	垂直方向	对角方向
原始图像		0.971 1	0.938 6	0.921 2
密文图像	本文算法	−0.007 9	−0.007 0	0.004 0
密文图像	文献[8]算法	0.014 1	0.010 7	0.009 7

从表 2 可见，原始图像的相关值非常大，接近 1，说明原始图像的相邻像素之间有很高的相关性。对比本文算法和文献[8]算法的结果可以看出，本文算法的相关值更接近 0，这说明本文算法的加密效果更好。

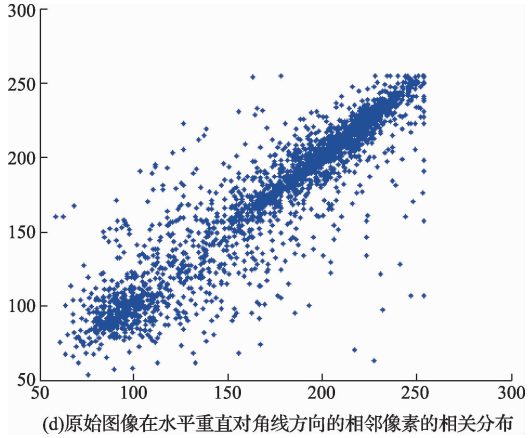
(a)原始图像和密文图像



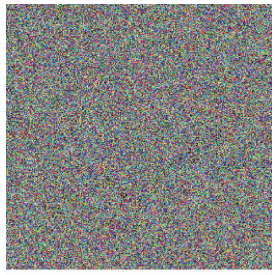
(b)原始图像在水平重直对角线方向的相邻像素的相关分布



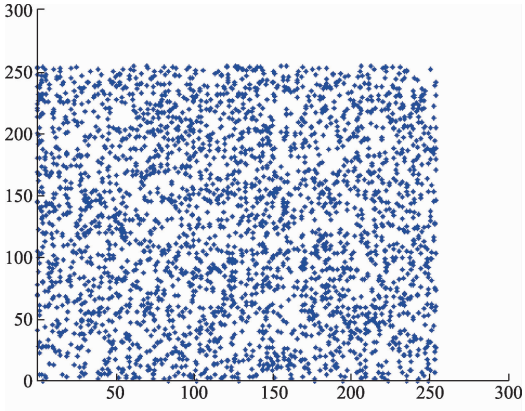
(c)原始图像在水平重直对角线方向的相邻像素的相关分布



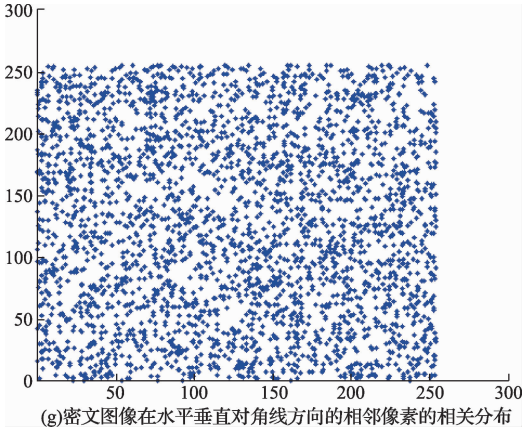
(d)原始图像在水平重直对角线方向的相邻像素的相关分布



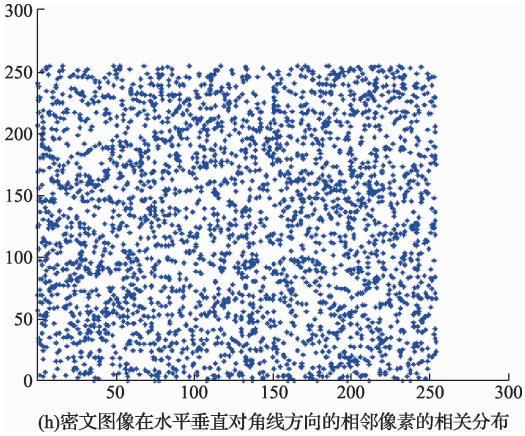
(e)原始图像和密文图像



(f)密文图像在水平垂直对角线方向的相邻像素的相关分布



(g)密文图像在水平垂直对角线方向的相邻像素的相关分布



(h)密文图像在水平垂直对角线方向的相邻像素的相关分布

图 5 原始图像和密文图像的相关性

图 5 中显示了原始图像和密文图像的相邻两个像素之间的相关性,从原始图像的相关性可以看出,其分布近似线性分布,这说明原始图像相邻像素之间有很高的相关性;而从密文图像的相关性可以看出,其分布近似均匀分布,这说明密文图像相邻像素之间有很低的相关性。

5.6 速度分析

加密算法主要是基于像素之间的异或的加密算法,其主要操作是异或,异或这种操作相对于其他的操作其耗时是很少的。对于 Android 智能手机这种运算能力有限,能很好的提高加密的速度。

速度分析实验的测试对象是 256×256 的 Lena 图像和 512×512 的 Baboon 图像,将本文算法和文献[10]作对比进行测试,测试的结果见表 3 所示。

表 3 不同算法加密时间对比

图像名	图像大小	本文算法/s	文献[10]/s
Lena	256×256	0.267	0.569
Baboon	512×512	1.370	2.251

从表 3 中可以看出,本文中所提出的加密算法在运行速度上要优于文献[10],这说明本文的算法速度和效率很高,适合应用于 Android 手机中。

6 结 论

提出了一种适用于 Android 手机的像素异或图像分块加密算法,在相邻两个子块之间运算时,相邻两个子块内像素的异或方式,采用了经典加密算法中的 RC4 算法,从实验数据可以看出,其加密后的图像近似噪声图像,直方图的分布更平滑、均衡,相邻像素几乎不相关,也有很好的随机性;又由于其主要操作是异或操作,加密速度快,很适用于 Android 手机。

参考文献

[1] ZHANG Z, SUN S L. Image encryption algorithm based on logistic chaotic system and S-box scrambling [J]. Image and Signal Processing, 2011, 1(4): 177-181.

[2] 卢辉斌,郑恒娜,韩秀峰. 基于 Lorenz 三维混沌序列的彩色图像加密算法[J]. 电子测量技术,2008, 31(11):34-36.

[3] 李小艳,李韧,沈民奋. 一种新的基于混沌序列的双随机置乱算法[J]. 电子测量与仪器学报,2008, 22(6):59-64.

[4] SHANG Z W, REN H E, ZHANG J. A block location scrambling algorithm of digital image based on Arnold transformation[C]//The 9th International Conference for Young Computer Scientists, 2008. ICYCS 2008. IEEE, 2008: 2942-2947.

[5] KADIR A, HAMDULLA A, GUO W Q. Color

image encryption using skew tent map and hyper chaotic system of 6th-order CNN [J]. Optik-International Journal for Light and Electron Optics, 2014, 125(5):1671-1675.

[6] LIU H J, ABDURAHMAN K, NIU Y J. Chaos-based color image block encryption scheme using S-box[J]. AEUvInternational Journal of Electronics and Communications, 2014, 68(7):676-686.

[7] MOHAMED F K. A parallel block-based encryption schema for digital images using reversible cellular automata[J]. Engineering Science and Technology, an International Journal, 2014, 17(2):85-94.

[8] WANG X Y, CHEN F, WANG T. A new compound mode of confusion and diffusion for block encryption of image based on chaos[J]. Communications in Nonlinear Science and Numerical Simulation, 2010, 15(9): 2479-2485.

[9] GINTING R U, DILLAK R Y. Digital color image encryption using RC4 stream cipher and chaotic logistic map [C]//2013 International Conference on Information Technology and Electrical Engineering (ICITEE2013), Yogyakarta, Indonesia, 7-8 October 2013, 101-105.

[10] LIAO X, LAI S, ZHOU Q. A novel image encryption algorithm based on self-adaptive wave transmission [J]. Signal Processing, 2010, 90(9): 2714-2722.

作者简介

涂正武,1989 年出生,在读硕士研究生。主要研究方向为图像加密。

E-mail:776918019@qq.com

金聪,1960 年出生,教授。主要研究方向为图像加密、图像水印、图像语义等。

E-mail:jinc26@aliyun.com

(上接第 45 页)

[2] 钟水和, 王建, 潘尧成, 等. 单通道单脉冲跟踪系统自动校相的设计与实现[J]. 四川兵工学报, 2015(7):97-99.

[3] 张书仙, 李瑭, 潘点飞. 基于数字波束形成的多目标测控[J]. 国外电子测量技术, 2014,33(8):73-77.

[4] 张振庄, 耿大孝. 船载天线动态校相技术研究与实现[J]. 无线电通信技术, 2015(1):52-55.

[5] 张小清, 郭星明, 李金喜,等. 一种无人机天线跟踪系统的数字校相方法[C]//2014(第五届)中国无人机大会论文集,2014.

[6] 汤恩生, 赵鸿, 周军. 角跟踪接收机中的自动校相技术[J]. 红外与激光工程, 2014(1):328-331.

[7] 罗小巧, 姜龙, 秦亚萍, 等. 基于 FPGA 的数字基带相关接收系统的设计[J]. 电子测量技术, 2012, 35(2):130-134.

[8] 陈怀艳, 王宝龙, 郝莉娜. 航天测控系统测试资源优化配置策略[J]. 电子测量与仪器学报, 2013,27(4):281-288.

[9] 瞿元新, 毛南平. 船载 X 频段微波统一测控系统快速校相方法[J]. 遥测遥控, 2014(2):69-72.

[10] 江建军, 黄云雪, 孙彪, 等. 基于随机解调器的宽带雷达信号探测[J]. 仪器仪表学报, 2014,35(3):709-713.

[11] 张维宁. 提高雷达测角性能的方法研究[D]. 哈尔滨:哈尔滨工业大学, 2013.

[12] 仇三山. 双通道单脉冲跟踪快速校相改进算法[J]. 四川兵工学报, 2013(5):96-98.

[13] 印金国. 单脉冲雷达跟踪系统跟踪过程自动校相方法研究[D]. 昆明:云南大学, 2012.

[14] GUPTA P K, VAGHELA R, BHATT K A, et al. Two-channel monopulse tracking receiver for onboard antenna tracking system [C]//2012 International Conference on Communication, Information & Computing Technology (ICCICT). IEEE, 2012: 1-6.

[15] 郑建荣. 单脉冲雷达测角幅相不一致影响及校正[J]. 现代电子技术, 2012,35(9):1-3.

作者简介

宋晓瑞,1990 年出生,在读硕士研究生。主要研究方向为航天测控技术、数字信号处理。

E-mail:sxrjmx@163.com