基于多普勒波和小波变换的图像置乱算法

卢曾新,曲大鹏,范铁生
(辽宁大学 信息学院,辽宁 沈阳 110036)

摘 要:由于图像信息在网络存储和传输的过程中易受到非法攻击者的截取,人们对图像信息的安全性和有效性提出了较高的要求,因此,对图像进行加密置乱就显得特别重要。文中提出了一种新的图像置乱算法,其基本思想是根据多普勒波和小波变换的特点,先对图像进行分块,然后对分块进行多尺度小波变换,对所有小波系数运用多普勒波进行像素值置乱,再对低频系数运用多普勒波生成多项式进行像素位置置乱。通过仿真实验表明,该算法能达到良好的置乱效果,充分改变了图像的统计特征,且不存在周期性恢复的问题,能抵抗一定的剪切、滤波和加噪等攻击,因此可以有效地用于图像加密。

关键词:图像置乱;多普勒波;小波变换;像素值置乱;像素位置置乱
中图分类号:TP301.6 **文献标识码**:A **文章编号**:1673-629X(2015)07-0138-04
doi:10.3969/j.issn.1673-629X.2015.07.030

Image Scrambling Algorithm Based on Doppler and Wavelet Transform

LU Zeng-xin, QU Da-peng, FAN Tie-sheng
(Information Institute of Liaoning University, Shenyang 110036, China)

Abstract: Since the image information is vulnerable to the illegal attack interception in the network storage and transmission process, leading to more demanding for the safety and effectiveness of the image information, therefore, the chaotic image encryption device is particularly of great importance. A new image scrambling algorithm, based on Doppler wave and wavelet transform, is proposed in this paper. Firstly, divide the image into small blocks, then the block is processed by multiscale wavelet transform, its wavelet coefficients of pixel values scrambling by Doppler, then use Doppler generator polynomial to carry out pixel position scrambling on low-frequency coefficients. Experimental results show that the algorithm can achieve better scrambling effect, changing the statistical property of the image, without problem of cyclical recovery, resistant to attacks of shearing, filtering and adding noise, which can be applied to image encryption efficiently.

Key words: image scrambling; Doppler wave; wavelet transform; pixel values scrambling; pixel position scrambling

0 引 言

由于图像文件具有直观、形象的特点,越来越受到网络用户的青睐。但当它们在网络中传输时,就有可能遭到破坏,因此,对这些图像进行加密就显得非常重要。

图像置乱是加密预处理的重要技术,以增加信息的隐藏和抗攻击能力[1]。已经有很多对图像进行置乱的算法,并取得了良好的效果,如 Arnold[2]、幻方[3]、Gray 码[4]、骑士巡游[5]、Fibonacci 变换[6]等。文献[7]通过混沌序列对 Arnold cat 变换进行改进,提出了一种图像位置均匀置乱算法,尽管密钥量大,但具有周期性;文献[8]利用混沌映射,对单一像素的高四位与低四位进行置乱,尽管能改变灰度分布规律,但对攻击的分散能力不好;文献[9]通过分析扩散算法,提出了局域单点扩散的概念,并将其和图像置乱相结合,但它是在空间域中进行的,降低了像素之间的相关性,给网络传输带来了安全隐患;文献[10]提出了一种基于生命游戏的置乱算法,虽然没有周期性,但是置乱不彻底,效果不理想;文献[11]对传统的骑士巡游算法进行改进,提出了一种分块分层、和 Arnold 相结合的置乱算法,密钥空间较大,但它只改变了像素的位置,像素分布规律没有变化,容易受到攻击。

收稿日期:2014-07-16 **修回日期**:2014-10-22 **网络出版时间**:2015-05-06
基金项目:辽宁省教育科学研究项目(L2013001);辽宁大学优秀青年教师资助项目
作者简介:卢曾新(1987-),男,硕士,研究方向为数字图像处理、信息隐藏;范铁生,教授,研究方向为信息隐藏、声纹识别、数字图像处理等。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20150506.1627.021.html

基于上面的分析,文中提出了一种基于多普勒波和小波变换的图像置乱算法。多普勒波具有频散特点,随着距离的增加,高频向低频移动;小波分析是一种时频分析,是对图像进行多尺度分解的强有力工具,因而能有效地从信号中提取信息[12]。文中借助多普勒波和小波的上述特点,生成不同周期的多普勒波,并将其周期作为密钥,利用多普勒波对小波分解后的高、低频系数进行像素值置乱,并运用多普勒波多项式对低频系数进行位置置乱,实现了对图像变换域上的双重置乱,提高了置乱的效率,增强了图像抗攻击的能力,较好地满足了置乱的要求。对置乱后的图像利用正确的密钥可以得到恢复。

1　基本原理

1.1　多普勒效应

多普勒效应是一种常见的自然现象,存在于声波、光波、电滋波等几乎所有类型的波中。它是指在波源与观察者之间存在相对运动时,观察者所接收到的频率与波源的频率不相等的现象。在运动的波源前面,波被压缩,波长变短,频率变高;在运动的波源后面,波长变长,频率变低。当波源的速度越大时,效应也就越明显。例如:当一列火车开来时,能感觉到它的汽笛声越来越尖锐,当它远离而去时,又感到它的汽笛声越来越低沉,这就是一种典型的多普勒效应。设波源的频率为 f_0,波源的运动速度为 v,声音在空气中传播的速度为 u,静止的观察者 P 与波源的运动方向距离为 l,则观察者所接收到的频率为

$$f = \frac{u}{u - \dfrac{v^2(t - t_0)}{\sqrt{l^2 + v^2 (t - t_0)^2}}} f_0 \tag{1}$$

其中,t_0 为与观察者的位置相对应的时间中心,当 $t < t_0$ 时,$f > f_0$,表示波源接近观察者;当 $t > t_0$ 时,$f < f_0$,表示波源远离观察者[13]。

1.2　小波变换

当对数字图像进行多分辨率分析时,小波变换是首选工具。它将信号分解为多个尺度,不同的尺度表现出不同的频域特性,这种直观形象的描述框架以及多分辨率分析的优点,都非常有助于深入了解图像的空域和频域特性,因此,它在图像压缩、分割、去噪、加密等方面得到了较好的利用。它的基本实现方法是:对图像的行和列先进行一维小波变换,再对其进行水平和垂直滤波,将原图像分解成了 4 个子图像,分别是:水平和垂直方向上低频生成的 LL_1,水平方向上的低频和垂直方向上的高频生成的 LH_1,水平方向上的高频和垂直方向上的低频生成的 HL_1,以及水平和垂直方向上高频生成的 HH_1。对 LL_1 继续进行分解,将得到 4 个更低分辨率的分量 LL_2、HL_2、HL_2 和 HH_1。依此类推,对图像进行 i 尺度的二维小波变换后,将形成一个简单的多层次框架,即低频近似信号 LL 和高频细节分量,其中高频分量有 LH_i,HL_i 及 HH_i,它们分别是 i 尺度上的水平、垂直和对角线方向上的高频分量。

2　算法实现

2.1　多普勒波分析

借助多普勒波的频移特点,可以用它来改变图像的像素值和像素位置,达到对图像进行置乱的目的。根据图像大小选择合适的多普勒波多项式,利用随机数模拟多普勒波频率数组,根据不同的周期,经过多次循环迭代,生成所需的多普勒波。

2.2　图像分块

当对图像用多普勒波进行置乱时,由于生成多普勒波的长度与图像的大小相关,因此,当图像较大时,生成多普勒波将耗费较多的时间,从而严重影响了置乱的时间效率。所以本算法中采取对原始图像进行分块的思想,在分块的基础上再进行置乱,这样可以大大提高效率。

2.3　小波分析

由于小波系数中有一个值发生变化时,其变化会影响到它所对应的空间邻域内的每个像素上,因此,对小波系数置乱比对像素本身置乱的效果更好。随着小波分解层数的增加,小波系数的范围和能量逐渐增大,因此,如果进行相同程度的置乱,大尺度低频子带的变化对原图像的影响,比小尺度低频子带的变化对原图像的影响更大[14],文中采用多尺度来提高置乱程度。另外,由于低频子带集中了被分解图像的绝大部分信息,是对原图的最大逼近,高频子带分别体现了水平、垂直、对角三个方向的边缘和轮廓,能量相对低频要小得多。因此,低频系数的变化对图像的置乱效果影响最大,所以,本算法中先对低频系数进行多普勒像素值置乱,然后再运用多普勒波生成多项式进行位置置乱;虽然高频系数对置乱度的影响较小,但为了不泄漏图像的边缘细节信息,也需要对各尺度的高频系数进行像素值置乱。

2.4　实现过程

步骤 1 预处理:假定原始图像为 $f(x,y)$,其中 $[r, c] = \text{size}(f)$。如果原图像是彩色图像,则提取每个分量图像,转换成灰度图像。

步骤 2 对图像 f 进行分块:假定每块大小为 $b \times d$,则把图像分成 $p \times q$ 个不相交的子图像,其中,$p = \text{floor}(r/b)$,$q = \text{floor}(c/d)$。如果 $\text{mod}(r/b) \neq 0$,则第 p 行的分块的行大小都为 $b + \text{mod}(r/b)$;如果

$\mathrm{mod}(c/d) \neq 0$,则第 q 列的分块的列大小都为 $d + \mathrm{mod}(c/d)$。

步骤 3 对子图像进行多尺度小波变换:使用小波工具箱中的任一个小波对子图像做 n 尺度二维小波分解,将其低频系数记为 LL_n,各尺度高频系数依次为 $\mathrm{HL}_k, \mathrm{LH}_k, \mathrm{HH}_k$,其中 $k = 1,2,\cdots,n$。

步骤 4 低频系数置乱:利用多普勒波公式生成多普勒波信息 D_n。记 LL_n 的最大值为 amax,中值为 amid,$[s,t] = \mathrm{size}(\mathrm{LL}_n)$。如果 $\mathrm{LL}_n(i,j) \leqslant \mathrm{amid}$,则 $\mathrm{LL}_n'(i,j) = \mathrm{mod}(\mathrm{LL}_n(i,j) + \mathrm{ua} * D_n, \mathrm{amid})$,并使记录矩阵 $\mathrm{jl}(i,j) = 0$;否则 $\mathrm{LL}_n'(i,j) = \mathrm{mod}(\mathrm{LL}_n(i,j) + \mathrm{ua} * D_n, \mathrm{amax})$,并使记录矩阵 $\mathrm{jl}(i,j) = 1$,ua 为多普勒嵌入低频系数的强度。最后从多普勒波生成多项式中随机取出 $s + t$ 个数,对 LL_n 进行行列交换,完成位置置乱。

步骤 5 高频系数置乱:利用多普勒波公式生成周期不同的多普勒波信息 $D_k(k = 1,2,\cdots,n-1)$,其中同一尺度的多普勒波周期相同。依次利用下式对各尺度高频系数进行置乱,$\mathrm{HL}_k = \mathrm{HL}_k + \mathrm{uk} * D_k$;$\mathrm{LH}_k = \mathrm{LH}_k + \mathrm{uk} * D_k$;$\mathrm{HH}_k = \mathrm{HH}_k + \mathrm{uk} * D_k$。其中,uk 为多普勒置乱的强度。

步骤 6 小波逆变换:将步骤 4 和 5 中已经置乱的低频系数和高频系数进行二维小波逆变换,将生成的各块拼接成完整的置乱图 F。

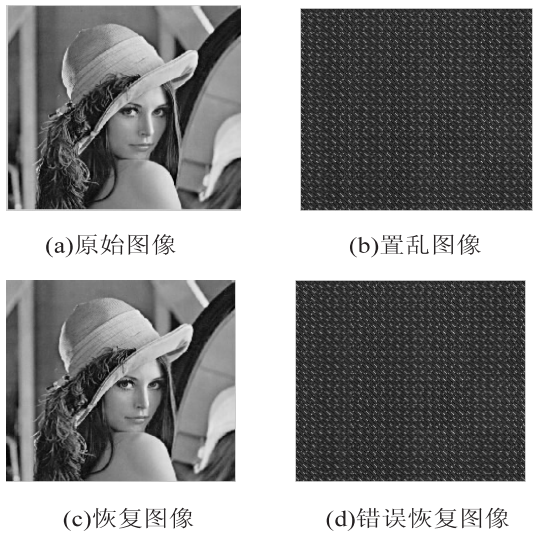
图像的恢复过程是置乱过程的逆过程,对上述过程进行相应的逆操作。其中,低频系数像素置乱恢复时要用到记录矩阵,若 $\mathrm{jl}(i,j) = 0$,则 $\mathrm{LL}_n(i,j) = \mathrm{mod}(\mathrm{LL}_n'(i,j) + \mathrm{amid} - \mathrm{ua} * D_n, \mathrm{amid})$;否则,$\mathrm{LL}_n(i,j) = \mathrm{mod}(\mathrm{LL}_n'(i,j) + \mathrm{amax} - \mathrm{ua} * D_n, \mathrm{amax})$。

3 实验结果及分析

3.1 置乱结果分析

文中以如图 1(a)所示的 Lena(512 * 512)为例验证算法的有效性,权衡多普勒波生成时间、置乱程度等因素,将其划分成大小为 128×128 的 16 块,进行三尺度的 Haar 小波变换。图 1(b)所示为用周期为 $T_1 = 0.8, T_2 = 0.7, T_3 = 0.6$ 的多普勒波对原图像进行置乱后的结果;图 1(c)为输入正确的多普勒波周期后解置乱的恢复图像;图 1(d)为输入错误的多普勒波周期 $T_1 = 0.82, T_2 = 0.71, T_3 = 0.61$ 时所得到的图像。

从中可以看出,经过置乱后完全看不到原图像的任何特征,图像的像素呈现出了多普勒波的特点,主观上达到了充分置乱的目的,使用正确的密钥能够较好地恢复出来,但使用错误的密钥恢复不出来原图像的任何特征,说明了该算法对密钥的敏感性以及置乱的有效性。



(a)原始图像 (b)置乱图像

(c)恢复图像 (d)错误恢复图像

图 1 图像进行置乱和恢复实验结果

3.2 置乱效果评价

峰值信噪比(PSNR)和均方根误差(RMSE)是客观评价置乱后恢复图像和原图像相似程度的两种常用方法。

PSNR 的公式如下(单位为 dB):

$$\mathrm{PSNR} = 10\lg\left[\frac{m \times n \times 255^2}{\sum_{i=1}^{m}\sum_{j=1}^{n}[f'(i,j) - f(i,j)]^2}\right] \quad (1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n) \tag{2}$$

RMSE 公式如下:

$$\mathrm{RMSE} = \sqrt{\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}[f'(i,j) - f(i,j)]^2}{m \times n}} \quad (1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n) \tag{3}$$

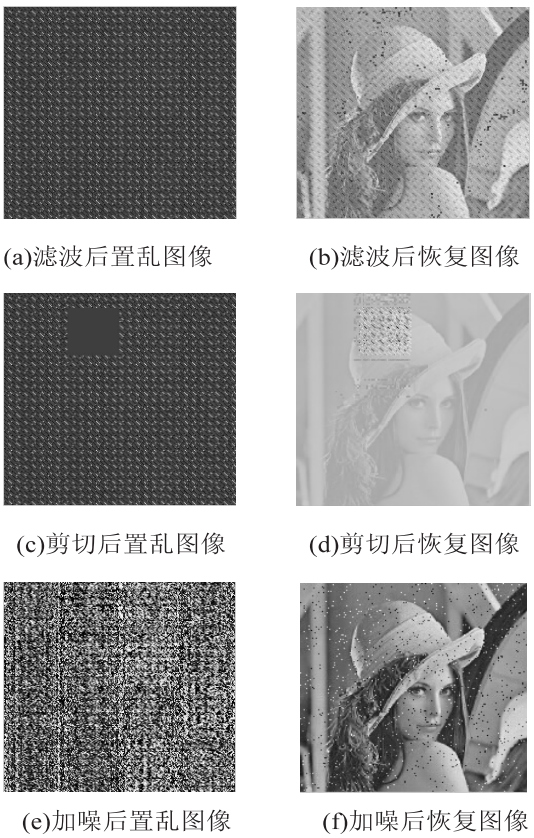
其中,$f'(i,j)$,$f(i,j)$ 分别是置乱后恢复图像和原图像在点 (i,j) 处的像素值。PSNR 值越大,图像的保真效果越好,即原图像和恢复图像越相似;RMSE 值越小,两幅图像越相似。经模拟实验验证,本算法求得 PSNR 的值为 37.53,RMSE 的值为 0.43,说明置乱后恢复效果较理想。

3.3 抗攻击分析

图 2(a)是将图 1(b)经过大小为 3×3 和标准偏差为 0.35 的高斯低通滤波器滤波后的置乱图像;图 2(b)是将图 2(a)进行正确密钥恢复后的图像;图 2(c)是将图 1(b)剪切掉(38:151,141:256)部分后的置乱图像;图 2(d)是将图 2(c)进行正确密钥恢复后的图像;图 2(e)是将图 1(b)加上 0.2 的椒盐噪声后的置乱图像;图 2(f)是将图 2(e)进行正确密钥恢复后的图像。

从中可以看到,经过本算法置乱后的图像经过滤波、剪切和加噪攻击后,虽然无法完全恢复到原图像,

但仍保留了原图像的大部分信息,具有较好的可知性,这也说明本算法具有一定的抗攻击能力。



(a)滤波后置乱图像　(b)滤波后恢复图像

(c)剪切后置乱图像　(d)剪切后恢复图像

(e)加噪后置乱图像　(f)加噪后恢复图像

图 2　置乱图像抗攻击效果图

4　结束语

文中提出了一种基于多普勒波和二维小波变换的图像置乱方法,通过分析多普勒波以及小波变换的特点,提出了具体的置乱过程,经过仿真实验取得了良好的效果。文中算法对图片的规格要求不高,能对非正方形图像进行置乱,密钥空间大,不存在周期性的安全问题,抗攻击能力好,置乱后的图像经过密钥可以得到较好的恢复。由于生成多普勒波需多次迭代,多项式的长度若选择不当,会大大降低置乱的时间效率,因此,在实际应用中必须权衡各种条件,选择合适的多项式长度,实现高效的置乱。

参考文献:

[1] 曹光辉,胡　凯. 基于混沌序列加权抽样和排序变换的图像置乱[J]. 北京航空航天大学学报,2013,39(1):67-72.

[2] 侯文滨,吴成茂. 基于 Arnold 变换的图像分存加密方法[J]. 计算机应用,2011,31(10):2682-2686.

[3] 刘　颖,刘健波. 幻方群在图像置乱中的研究与应用[J]. 计算机技术与发展,2012,22(9):119-122.

[4] 谭永杰,马　苗. 位平面与 Gray 码相结合的图像置乱方法[J]. 计算机工程与应用,2010,46(16):174-177.

[5] Beasley J D. Magic knight's tours[J]. The College Mathematics Journal,2012,43(1):72-75.

[6] Zou Jiancheng, Ward R K, Qi Dongxu. A new digital image scrambling method based on Fibonacci numbers[C]//Proceeding of the international symposium on circuits and system. Vancouver,Canada:IEEE,2004.

[7] 张　健,于晓洋,任洪娥. 基于 Arnold cat 变换的图像位置均匀置乱算法[J]. 计算机应用,2009,29(11):2960-2963.

[8] 袁　玲,康宝生. 基于 Logistic 混沌序列和位交换的图像置乱算法[J]. 计算机应用,2009,29(10):2681-2683.

[9] 尹德辉,唐　燕,李炳法. 基于置乱和灰度扩散的图象置乱算法研究[J]. 四川大学学报:自然科学版,2005,42(2):290-295.

[10] 雷仲魁,孙秋艳,宁宣熙. 马步哈密顿圈(骑士巡游)在图像置乱加密方法上的应用[J]. 小型微型计算机系统,2010,31(5):984-989.

[11] 赵　刚,李建平,唐　真,等. 基于小波变换和 Feistel 密码结构的图像置乱技术[J]. 后勤工程学院学报,2008,24(3):55-58.

[12] 邹红星,周小波,李衍达. 采用 Dopplerlet 基函数的时频信号表示[J]. 清华大学学报:自然科学版,2000,40(3):55-58.

[13] 侯启槟,杨小帆,王阳生,等. 一种基于小波变换和骑士巡游的图像置乱算法[J]. 计算机研究与发展,2004,41(2):369-375.

[14] 范铁生,张忠清,张　璞. 一种索玛立方体方块匹配的图像置乱算法[J]. 计算机科学,2013,40(6):308-310.

基于多普勒波和小波变换的图像置乱算法

作者： 卢曾新， 曲大鹏， 范铁生， LU Zeng-xin， QU Da-peng， FAN Tie-sheng
作者单位： 辽宁大学 信息学院,辽宁 沈阳,110036
刊名： 计算机技术与发展 ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2015(7)