基于单一像素值改变的图像置乱新算法*

何立明, 强赛莉
(长安大学 信息工程学院, 西安 710064)

摘　要: 针对数字图像传输的安全问题,提出一种基于单一像素值改变的图像置乱新算法,该算法将密码学中维吉尼亚加密算法进行修正,使之能够应用于数字图像的加密。实验结果表明,该算法加密的图像安全性高,与传统的基于单一像素值改变的置乱算法相比较,具有更好的抗噪声性能,该算法具有很高的灵活性,其加密图像的置乱程度与工作密钥 的选择具有密切的关系,并且适合加密任意尺寸的数字图像。以上优越性使得该算法更能适合于数字图像的网络传输过程,以及其他对数字图像安全有较高要求的领域。

关键词: 图像置乱; 维吉尼亚加密; 随机工作密钥; 交叉换位; 置乱程度; 抗噪声性
中图分类号: TP393.08　　**文献标志码**: A　　**文章编号**: 1001-3695(2012)12-4635-04
doi:10.3969/j.issn.1001-3695.2012.12.059

Novel image scrambling algorithm based on changing pixel values

HE Li-ming, QIANG Sai-li
(*College of Information Engineering, Chang'an University, Xi'an* 710064, *China*)

Abstract: Aiming at the safe problem of digital image transmission, this paper presented a new image scrambling algorithm based on changing the pixel values. The algorithm improved the Vigenere encryption algorithm, made it can be applied in the digital image encryption. Experimental result shows that, the image which is encrypted by this algorithm has a high safety, compared with the traditional image scrambling algorithm based on changing the single pixel. The method has a better ability of resist noise, it also has better flexibility, it can encrypt any size of digital images. The scrambling degree of the encrypted image has the close relationship with the choice of keyword, and it can encrypt any size of digital images. So the above superiorities of this algorithm make it suitable for digital image of the network transmission process, and other fields which have higher safety requirements for digital images.

Key words: image scrambling; Vigenere encryption; random keyword; bit exchanged across; scrambling degree; ability of resist noise

0　引言

随着网络信息技术的不断发展,大量的信息文件以数字图像形式在网上传播,并逐步成为人们获取信息的主要手段。如何解决对数字图像进行加密从而保证图像完整而安全地到达接收方的问题越来越成为人们关注的焦点。图像置乱技术作为图像加密的一种重要方法,同时也可作为进一步隐藏图像信息的预处理过程,成为一个值得深入研究的课题。

目前空域图像置乱方法从本质上可分为两类[1]:a)基于像素位置变换的置乱方法;b)基于像素灰度值变换的置乱方法。其中基于像素值位置变换的置乱方法居多,如基于幻方变换[2]、仿射变换[3]、Arnold 变换[4]、Hilbert 曲线[5]、Gray 码变换[5]、Conway 游戏[6]等,这些方法都只是对图像中像素的位置重新排列, 而其本身的像素值并未发生改变,所以置乱后图像的灰度直方图都不发生改变,而灰度直方图又是衡量一幅图像的重要特征。

本文提出基于单一像素值改变的图像置乱新算法,该算法对密码学中经典的算法——维吉尼亚加密算法进行修正,应用于数字图像的加密过程中,使得图像的像素值发生了较大的改变,置乱后图像的灰度直方图明显不同于原始图像,从而满足图像在传输过程中的安全性和可靠性要求。另外,本文的修正算法采用了 MATLAB 6.5 系统中 100 * rand(256)(随机函数)生成的图像作为工作密钥,将类似于噪声图像的工作密钥和加密后的目标图像同时发送给接收方,这样可以在一定程度上混淆非法截获者的视听,使得传输的图像更加安全。

1　维吉尼亚加密

维吉尼亚密码是一种以移位代换为基础的周期代换密码,是 1858 年由法国密码学家维吉尼亚提出的,它首次引入了密钥的概念,根据密钥来决定用哪一行的密表来进行替换,以此来对抗字频统计,在密码学中占有重要的地位。所谓密钥是一种参数,它是在明文转换为密文或将密文转换为明文的算法中输入的数据。

维吉尼亚加密原理如下。

收稿日期: 2012-05-09; **修回日期**: 2012-06-26　**基金项目**: 西部交通建设科技项目(2011318223710);中央高校基本科研业务费专项资金资助项目(CHD2011JC156)

作者简介:何立明(1978-),男,陕西西安人,副教授,博士,主要研究方向为智能交通系统信息采集及融合、无线传感器网络及其在交通中的应用、数字视频技术及其在交通中的应用(lmhe@chd.edu.cn);强赛莉(1988-),女,硕士研究生,主要研究方向为数字图像处理、无线多媒体传感器网络及其在交通中的应用.

首先构造一个维吉尼亚方阵,如表 1 所示。

表 1 维吉尼亚方阵

	a	*b*	*c*	*d*	…	*x*	*y*	*z*
a	*A*	*B*	*C*	*D*	…	*X*	*Y*	*Z*
b	*B*	*C*	*D*	*E*	…	*Y*	*Z*	*A*
c	*C*	*D*	*E*	*F*	…	*Z*	*A*	*B*
d	*D*	*E*	*F*	*G*	…	*A*	*B*	*C*
e	*E*	*F*	*G*	*H*	…	*B*	*C*	*D*
⋮	⋮	⋮	⋮	⋮		⋮	⋮	⋮
x	*X*	*Y*	*Z*	*A*	…	*U*	*V*	*W*
y	*Y*	*Z*	*A*	*B*	…	*V*	*W*	*X*
z	*Z*	*A*	*B*	*C*	…	*W*	*X*	*Y*

其基本阵列是 26 行 26 列的方阵,方阵的第一行是 *a* ~ *z* 按正常顺序排列的字母表,第二行是第一行循环左移一位得到的,第三行是第二行循环左移一位得到的,以此类推,得到其余各行,然后在基本方阵的最上方附加一行,最左侧附加一列,分别依序写上 *a* ~ *z* 共 26 个字母,表的第一行与附加列上的字母 *a* 相对应,表的第二行与附加列上的字母 *b* 相对应……最后一行与附加列上的字母 *z* 相对应,如果把上面的附加行看做是明文序列,则下面的 26 行就分别构成了左移 0 位、1 位、2 位、…、25 位的 26 个单表代换加同余密码的密文序列。加密时按照密钥字的指示决定采用哪一个单表。

维吉尼亚密码加密和解密的数学模型可以表示为[7]:

令英文字母 *a*,*b*,…,*z* 对应于 0 ~ 25 的整数,设明文是 *n* 个字母组成的字符串,即

$$m = m_1 m_2 \cdots m_n \tag{1}$$

密钥字周期性地延伸就给出了明文加密所需的工作密钥:

$$k = k_1 k_2 \cdots k_n \tag{2}$$

$$E(m) = C = c_1 c_2 \cdots c_n \tag{3}$$

加密:

$$c_i = m_i + k_i \bmod 26 \tag{4}$$

解密:

$$m_i = c_i - k_i \bmod 26 \quad i \in (1,n) \tag{5}$$

2 本文改进算法

利用维吉尼亚密码加密的思想,本文以 256 × 256 的 Lena 图像为例,进行说明。由于一般加密的数字图像的像素值为十进制的数值,所以本文算法加密中的数学模型为:设原始图像 *I* 的大小为 $M \times N$,$I(i,j)$ 表示图像 *I* 第 *i* 行第 *j* 列元素的灰度值,工作密钥为图像 *K*,大小也为 $M \times N$,$K(i,j)$ 表示图像 *K* 第 *i* 行第 *j* 列元素的灰度值。需要加密的图像像素值为 $I(i,j) = I_1 I_2 \cdots I_n$,相应工作密钥的值为 $K(i,j) = K_1 K_2 \cdots K_n$。

加密时:

a) $C_i = I_i + K_i \bmod 10, i \in (1,n)$。

b)将 C_i 转换成二进制数,然后进行交叉换位(图 1),得到 D_i。

解密时:

a)将 D_i 转换成二进制数,进行逆交叉换位(图 1),得到 E_i。

b) $I'_i = E_i - K_i \bmod 10, i \in (1,n)$。

这里可以选取同原始图像同等大小(256 × 256)的任意图像,作为给原始图像加密所用的工作密钥,由于工作密钥也是需要传输的,因此在本文的修正算法中,采用了 MATLAB 6.5 系统中 100 * rand(256)(随机函数)生成的图像作为工作密钥,将类似于噪声图像的工作密钥和加密后的目标图像同时发送给接收方,这样可以在一定程度上混淆非法截获者的视听,使得要传输的图像更加安全。

2.1 关于交叉换位

传统的交叉换位是将十进制数值转换为 8 bit 二进制数进行交叉换位。8 bit 二进制数表示的十进制数范围是 0 ~ 255,而在本文算法中各像素值在进行维吉尼亚加密运算后,大部分数值已经超出了 0 ~ 255 所表示的数值范围,显然传统的交叉换位在此处已不能适用。因而本文将十进制数值转换为 10 bit 二进制数,可以表示的十进制数范围为 0 ~ 1 023,其中最高两位用来存储因为维吉尼亚编码产生的溢出数值位,不参与交叉换位。具体操作如图 1 所示。

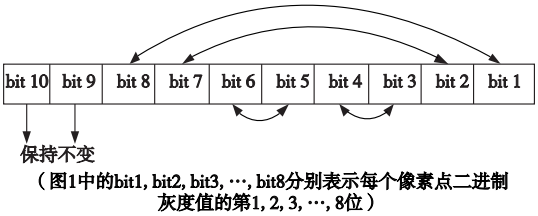


图1 交叉换位原理

2.2 本文算法框图

2.2.1 置乱算法

本文中维吉尼亚修正算法的置乱算法框图如图 2 所示。

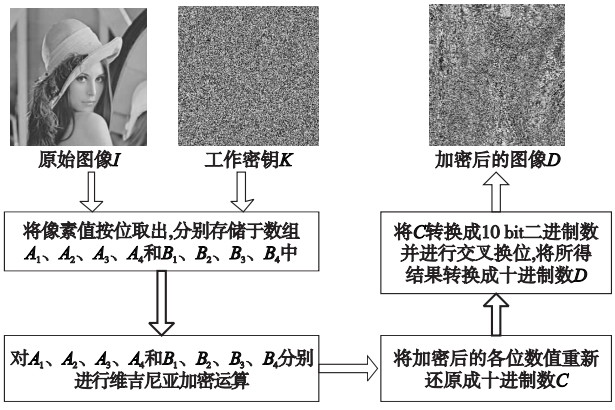


图2 本文置乱算法框图

2.2.2 还原算法

本文中维吉尼亚修正算法的还原算法框图如图 3 所示。

3 维吉尼亚修正算法实现步骤

3.1 置乱算法

a)将原始图像的第一个像素值 $I(1,1)$ 和工作密钥图像的第一个像素值 $K(1,1)$ 的值按从高位到低位的顺序取出,并分别存储放在数组 A_1、A_2、A_3、A_4 和 B_1、B_2、B_3、B_4 中,具体如下:

$$\begin{cases} A_1 = I(1,1)/1000 \\ A_2 = (I(1,1) - A_1 \times 1000)/100 \\ A_3 = (I(1,1) - A_1 \times 1000 - A_2 \times 100)/10 \\ A_4 = I(1,1) - A_1 \times 1000 - A_2 \times 100 - A_3 \times 10 \end{cases} \tag{6}$$

$$\begin{cases} B_1 = K(1,1)/1000 \\ B_2 = (K(1,1) - B_1 \times 1000)/100 \\ B_3 = (K(1,1) - B_1 \times 1000 - B_2 \times 100)/10 \\ B_4 = K(1,1) - B_1 \times 1000 - B_2 \times 100 - B_3 \times 10 \end{cases} \tag{7}$$

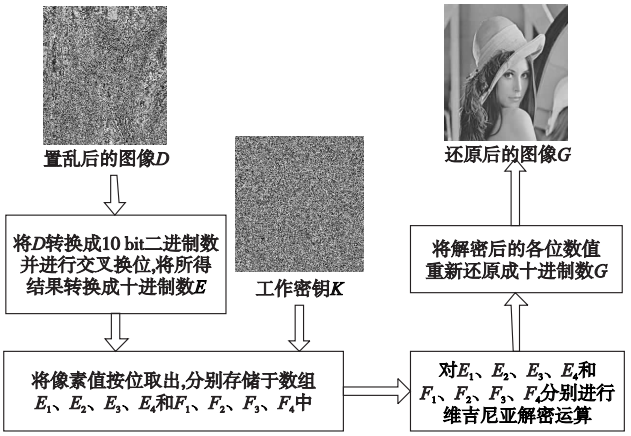


图3　还原算法框图

b)将取出的原始图像像素值的各位上的数值进行维吉尼亚加密,即

$$\begin{cases} C_1 = A_1 + B_1 \bmod 10 \\ C_2 = A_2 + B_2 \bmod 10 \\ C_3 = A_3 + B_3 \bmod 10 \\ C_4 = A_4 + B_4 \bmod 10 \end{cases} \tag{8}$$

c)将加密后的像素值的各位上的数值重新还原成十进制数值,即

$$C(1,1) = C_1 \times 1000 + C_2 \times 100 + C_3 \times 10 + C_4 \tag{9}$$

d)将 $C(1,1)$ 转换成 10 bit 的二进制数,然后进行交叉换位(图 1),即将转换后的二进制数第 9、10 bit 不变,第 8 位和第 1 位互换,第 7 位和第 2 位互换,第 6 位与第 5 位互换,而第 4 位与第 3 位互换,再将得到的新的二进制数值转换为十进制数值,记为 $D(1,1)$。

e)重复以上步骤,依次得到 $D(1,2)$,$D(1,3)$,…,$D(i,j)$。其中,$i \in (1,M)$,$j \in (1,N)$,则图像 D 就是最终的加密图像。

3.2　还原算法

a)将加密图像 D 中第一个像素值 $D(1,1)$ 转换成 10 bit 的二进制数值,然后进行逆交叉换位操作(图 1),即将转换后的二进制数第 9、10 位不变,第 8 位和第 1 位互换,第 7 位和第 2 位互换,第 6 位与第 5 位互换,而第 4 位与第 3 位互换,再将得到的新的二进制数值转换为十进制数值,记为 $E(1,1)$。

b)将 $E(1,1)$ 和工作密钥图像的第一个像素值 $K(1,1)$ 的值按从高位到低位的顺序取出,并分别存储放在数组 E_1、E_2、E_3、E_4 和 F_1、F_2、F_3、F_4 中,具体如下:

$$\begin{cases} E_1 = E(1,1)/1000 \\ E_2 = (E(1,1) - E_1 \times 1000)/100 \\ E_3 = (E(1,1) - E_1 \times 1000 - E_2 \times 100)/10 \\ E_4 = E(1,1) - E_1 \times 1000 - E_2 \times 100 - E_3 \times 10 \end{cases} \tag{10}$$

$$\begin{cases} F_1 = K(1,1)/1000 \\ F_2 = (K(1,1) - F_1 \times 1000)/100 \\ F_3 = (K(1,1) - F_1 \times 1000 - F_2 \times 100)/10 \\ F_4 = K(1,1) - F_1 \times 1000 - F_2 \times 100 - F_3 \times 10 \end{cases} \tag{11}$$

c)将取出的像素值的各位上的数值进行维吉尼亚解密,即

$$\begin{cases} G_1 = E_1 - F_1 \bmod 10 \\ G_2 = E_2 - F_2 \bmod 10 \\ G_3 = E_3 - F_3 \bmod 10 \\ G_4 = E_4 - F_4 \bmod 10 \end{cases} \tag{12}$$

d)将解密后的像素值的各位上的数值重新还原成十进制数值,即

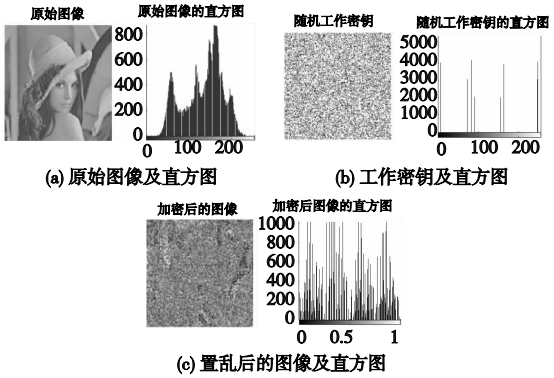
$$G(1,1) = G_1 \times 1000 + G_2 \times 100 + G_3 \times 10 + G_4 \tag{13}$$

e)重复以上步骤,依次得到 $G(1,2)$,$G(1,3)$,…,$G(i,j)$。其中,$i \in (1,M)$,$j \in (1,N)$,则图像 G 就是解密后的图像,即原始图像。

4　实验仿真与性能分析

实验 1　原始图像与置乱后的图像对比。

从图 4 中各组图片可以看出,本文的维吉尼亚修正算法置乱的图像纹理较细、颗粒均匀,从人类视觉系统(human visual system,HVS)的角度来说,看不出任何原图像的信息,置乱效果良好。从直方图看,修正算法生成的直方图与原始图像的直方图相比也发生了较大的改变,这说明将该算法生成的置乱图像应用于数字水印等秘密信息的隐藏预处理时,置乱信息能够更加均匀地嵌入到宿主信息中,得到的水印透明性更好,这说明本文算法已完全满足传输过程中的安全性的需要。



(a) 原始图像及直方图　(b) 工作密钥及直方图

(c) 置乱后的图像及直方图

图4　原始图像与置乱图像的对比

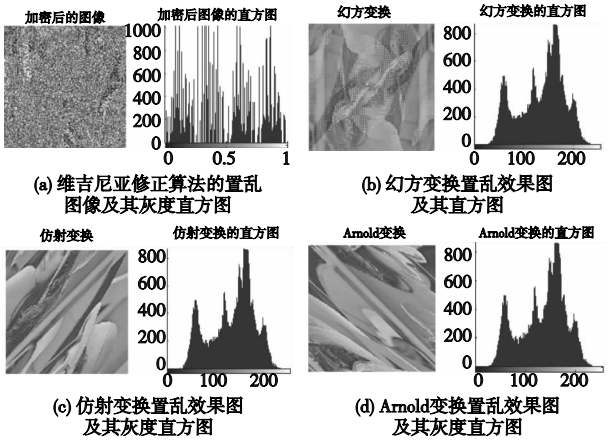
实验 2　在置乱一次的情况下与幻方变换、仿射变换以及 Arnold 变换置乱效果对比。

从图 5 中各组图片可以看出,本文的置乱算法与传统的基于像素值位置改变的置乱算法(幻方变换、仿射变换、Arnold 变换算法)相比较,同样在置乱一次的情况下,从视觉角度分析,本文算法的置乱效果明显优于其他三种算法。从置乱前后图像的直方图来看,幻方变换置乱、仿射变换置乱和 Arnold 置乱图像与原图像的直方图完全相同,截获者可容易地得到原图像的直方图信息,这也是所有基于位置变化的图像置乱方法的一个共同的缺点。

实验 3　与按位异或算法的比较。

本文提出的是一种基于单一像素值改变的置乱算法。目前在数字图像处理领域比较常见的是按位异或算法,该算法的基本思想[8]为将像素值按位异或后再进行交叉换位,从而改变像素值。以下实验将从置乱后的视觉效果(图 6)以及抗噪声性(图 7、8)两个方面将两种算法进行比较。

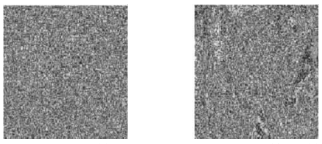
a)置乱效果对比如图 6 所示。



(a) 维吉尼亚修正算法的置乱图像及其灰度直方图　(b) 幻方变换置乱效果图及其直方图

(c) 仿射变换置乱效果图及其灰度直方图　(d) Arnold变换置乱效果图及其灰度直方图

图5　本文置乱效果与幻方变换、仿射变换以及Arnold变换置乱效果对比



(a) 按位异或算法　(b) 维吉尼亚修正算法

图6　本文置乱效果与按位异或算法置乱效果对比

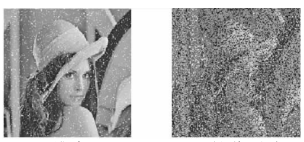
b)抗噪声性对比。数字图像在传输的过程中难免会受到噪声的干扰,因此,置乱图像是否具有良好的抗噪声性也是一个非常重要的问题。本文实验采用 MATLAB 6.5 系统产生的随机函数的倍数作为噪声函数,对本文的维吉尼亚修正算法和按位异或算法进行分析。将两种算法加密后的图像分别加上同一个噪声函数后,再分别对它们进行解密运算,将得到的解密图像进行对比,结果与原始图像越接近的,说明该算法的抗噪声性能越好。

(a)噪声 $s = 2 \times \mathrm{rand}(256)$时抗噪声效果如图 7 所示。

(b)噪声 $s = 1.5 \times \mathrm{rand}(256)$时抗噪声效果如图 8 所示。

(a) 维吉尼亚修正算法　(b) 按位异或算法

图7　抗噪声效果对比1



(a) 维吉尼亚修正算法　(b) 按位异或算法

图8　抗噪声效果对比2

通过以上实验可以看出,同样作为基于单一像素值改变的图像置乱算法,在一定的噪声范围内,维吉尼亚修正算法的抗噪声性能明显优于按位异或算法,更加适合于传输过程。

5　基于 SNR 的图像置乱程度评价

文献[9]中提到了用基于图像亮度的信噪比(SNR)来评价数字图像置乱效果的方法,该方法将原始数据与重现图像数据之差看做噪声。设 $f(x,y), x,y \in \{0,1,\cdots,N-1\}$ 表示 $N \times N$ 个原始图像数据,用 $g(x,y), x,y \in \{0,1,\cdots,N-1\}$ 表示重现的图像数据,此时噪声 $e(x,y)$ 为 $e(x,y) = f(x,y) - g(x,y)$。

重现图像的均方信噪比定义为

$$(\mathrm{SNR})_{ms} = \frac{\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} g^2(x,y)}{\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} e^2(x,y)} \tag{14}$$

图像置乱度的定义为 $\eta = 1/s$,其中 $s = \sum_{i=1}^{t} \mathrm{SNR}_i / t$,$t$ 为将原始图像和置乱图像分别分成的块数。

显然,均方信噪比越大,重现图像就越接近原始图像,其置乱度也就越小。一般来说,若置乱后的图像相对于原始图像越乱,表明该置乱变换越有效。也就是说,若置乱图像相对于原始图像的偏离程度越大,则置乱的程度就越大,置乱的效果也就越好。

根据式(14),比较几种算法的置乱度($t = 64$),如表 2 所示。

表2　不同算法生成的置乱图像与原始图像的置乱度

	仿射变换置乱	Arnold 变换置乱	幻方变换置乱	按位异或算法	本文方法置乱
置乱度	0.122 3	0.100 0	0.051 7	0.344 1	0.650 6

从表 2 可以看出,与仿射变换置乱、Arnold 变换置乱和幻方变换置乱这三种传统的基于像素值位置改变的图像置乱算法,以及按位异或算法置乱这一传统的基于像素值改变的图像置乱算法相比较而言,本文修正算法的置乱度要高出很多,这说明该算法生成的置乱图像相对于原始图像的偏离程度大,置乱的效果好。

6　工作密钥对置乱效果的影响

6.1　不同的数字图像作为工作密钥

在图 9 中,分别采用不同图像作为工作密钥对 256 × 256 的 Lena 图像进行维吉尼亚修正算法的加密,第一行为工作密钥,第二行是与第一行工作密钥相对应的置乱图像以及相应的置乱度。

6.2　同一图像置乱不同次数作为工作密钥

在图 10 中,分别将 256 × 256 的 baboon 图像采用 Arnold 变换分别置乱 1、3、5 次后再作为工作密钥对 256 × 256 的 Lena 图像进行维吉尼亚修正算法的加密,第一行为工作密钥,第二行是与第一行工作密钥相对应的置乱图像以及相应的置乱度。

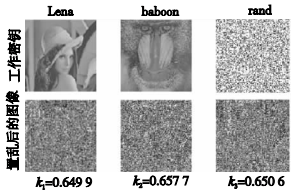


图9　不同图像作为工作密钥

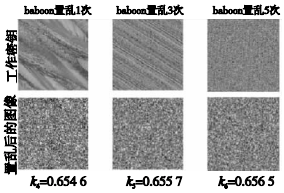


图10　同一图像置乱不同次数作为工作密钥

由以上实验结果可以看出,对于同一目标图像进行维吉尼亚修正方法置乱时,不同的工作密钥将直接影响到目标图像的置乱效果,因此选择适合目标图像加密的工作密钥也是非常重要的,这也将是下一步研究工作的一个重要方向。

7　结束语

本文提出了一种基于单一像素值改变的数字图像置乱方法,该算法在维吉尼亚加密算法的基础上进行交叉换位的操作,从而改变了数字图像的像素值,并使图像的灰度直方图产生了较大的改变。本文算法实现简单,并且适合于加密任意大小的数字图像。为了验证算法的有效性,本文分别从视觉效果方面以及置乱图像与原始图像的信噪比方面对该算法的置乱效果作了分析。结果表明,与传统的基于像素值位置改变的置乱算法相比较,维吉尼亚修正算法从视觉角度看置乱效果更好,置乱度也更高;而与传统的基于单一像素值改变的图像置乱算法——按位异或算法相比较,本文算法不但置乱度较高,而且抗噪声性更胜一筹。这充分说明该算法 (下转第 4650 页)

理算法对于 DDoS 攻击的防御能力非常有限。

4 防御 DDoS 攻击的主要策略

在低发包率的条件下,主动式队列管理算法对于 DDoS 攻击的防御能力较强。但在较高发包率的情况下,主动式和被动式队列管理算法均无法有效防范 DDoS 攻击,所以 Ad hoc 网络若要有效防范 DDoS 攻击,需要结合其他机制,综合运用各种防御策略。

由于传统 DDoS 攻击是利用底层协议的安全隐患或是系统设计问题进行攻击的,因此针对这种攻击类型的大部分研究主要是依靠分析网络数据包的分组特征、流特征、请求速率等方面的内容来检测攻击,由此提出的防御方案主要可以分为基于攻击源进行检测和基于受攻击节点进行检测两种类型[12]。

文献[13]是一种典型的基于攻击源的检测方案。该方案基于反馈机制建立了一种简单的数据过滤模型。该过滤模型采用统计概率的方法,根据当前网络数据流量、延时以及过滤节点的处理能力确定丢弃该包的概率。

而作为基于受攻击节点的检测方案,文献[12]设计了一种基于决策树机制的 DDoS 检测系统,该系统在检测到攻击后,利用数据流模型匹配机制追踪攻击者的位置及攻击路径。仿真表明,该系统能够检测出 DDoS 攻击者的漏报率为 1.2% ~ 2.4%,误报率仅为 2% ~10%,发现攻击路径的漏报率和误报率分别为 8% ~12% 和 12% ~14%。

5 结束语

本文介绍了三种传统的网络队列管理算法:Drop-Tail、RED 和 REM,并在 Ad hoc 网络环境中,利用网络仿真软件 NS2 对三种算法在 DDoS 攻击下的发包率和平均端到端延时进行了仿真比较。结果表明:在轻、中度 DDoS 攻击下,主动式队列管理算法(如 RED、REM 等)与被动式队列管理算法(Drop-Tail)相比性能较优;然而在重度 DDoS 攻击下,无论是主动式队列管理算法还是被动式队列管理算法,其性能均有明显下降。由于队列管理算法的先天不足,在实际应用中,一般都将队列管理算法与其他防范 DDoS 攻击的策略(如 DDoS 攻击检测)相结合以提高对 DDoS 攻击的防御能力。另一方面,在确保网络服务质量 QoS 的前提下,如何对原有的主动式队列管理算法作出相应修改,使其能够有效应对 DDoS 攻击,则是本文下一步的研究重点。

参考文献:

[1] 金舒原,云晓春,方滨兴. DDoS 攻击检测的挑战[J]. 信息技术快报,2008,6(5):25-35.

[2] 张长旺,殷建平,蔡志平,等. 抗 DDoS 攻击的主动队列管理算法[J]. 软件学报,2011,22(9):2182-2192.

[3] 王建新,荣亮,肖雪峰. 几种主动队列管理算法的仿真及性能评估[J]. 计算机工程,2007,33(3):128-130.

[4] 韦蓉. Ad hoc 网络关键技术研究[D]. 北京:邮电大学,2008.

[5] PENG T, LECKIE C, RAMAMOHANARAO K. Survey of network-based defense mechanisms countering the DoS and DDoS problems [J]. ACM Computing Surveys,2007,39(1):1-42.

[6] 方路平,刘世化,陈盼,等. NS-2 网络模拟基础与应用[M]. 北京:国防工业出版社,2008:156-166.

[7] ZHANG Wei, TAN Liang-sheng, PENG Gang. Dynamic queue level control of TCP/RED systems in AQM routers[J]. Computers and Electrical Engineering,2009,35(1):59-70.

[8] 刘明,张鹤颖,窦文华. 随机指数标记算法的性能分析与控制模型[J]. 计算机工程与科学,2005,27(9):66-68.

[9] ATHURALIYA S, LOW S H, LI V H, *et al*. REM : active queue management[J]. IEEE Network,2001,15(3):48-53.

[10] 吴春明,姜明,朱淼良. 几种主动式队列管理算法的比较研究[J]. 电子学报,2004,32(3):429-434.

[11] 柯志亨,程荣祥,邓德隽. NS-2 仿真实验——多媒体和无线网络通信[M]. 北京:电子工业出版社,2009:315-331.

[12] WU Y C, TSENG H R, YANG W, *et al*. DDoS detection and trace-back with decision tree and grey relational analysis[J]. Ad hoc and Ubiquitous Computing,2011,7(2):121-136.

[13] TAN H X, SEAH W K G. Framework for statistical filtering against DDoS attacks in MANETs[C]//Proc of the 2nd International Conference on Embedded Software and Systems. Berlin: Springer-Verlag, 2006:456-465.

(上接第 4638 页)的有效性及可靠性。实验结果表明本文提出的算法适合图像的加密传输,以及在数字水印等隐蔽传输中的置乱预处理,有很好的实用价值和应用前景。下一步的工作主要包括:如何选择合适的工作密钥使置乱算法达到最优,该算法在数字水印等技术中的应用以及在其他领域应用的研究。

参考文献:

[1] 谭永杰,张文娟,崔海花. 图像置乱技术综述[J]. 周口师范学院学报,2010,27(5):98-102.

[2] 练芝飞,徐荣聪. 幻方变换加密分形图[J]. 福建电脑,2009(12):111-112.

[3] 柏森,曹长修,柏林. 基于仿射变换的数字图像置乱技术[J]. 计算机工程与应用,2002,38(10):74-75,78.

[4] 李用江,葛建华,李昌利,等. 一种新的 n 维广义 Arnold 矩阵构造方法及其在图像置乱中的应用[J]. 北京科技大学学报,2010,32(12):1630-1636.

[5] 万里红,孙燮华,林旭亮. 分形 Hilbert 曲线混合 Gray 码的图像加密算法研究[J]. 计算机工程与应用,2010,46(34):184-186,194.

[6] 丁玮,闫伟齐,齐东旭. 基于生命游戏的数字图像置乱与数字水印技术[J]. 北方工业大学学报,2000,12(1):1-5.

[7] 关可,王建新,亓淑敏. 信息论与编码技术[M]. 北京:清华大学出版社,2009:210-211.

[8] 马苗,谭永杰. 基于相邻像素间位异或的图像置乱算法[J]. 计算机工程与应用,2008,44(9):187-189.

[9] 李志伟,陈燕梅,张胜元. 基于 SNR 的数字图像置乱程度评价方法[J]. 厦门大学学报:自然科学版,2006,45(4):484-487.

[10] 赵红,温文雅. 数字图像置乱技术综述[J]. 福建电脑,2007(12):10-12.

[11] QI Dong-xu, ZOU Jian-cheng, HAN Xiao-you. A new class of scrambling transformation and its application in the image information covering[J]. Science in China:Series E,2000,43(3):304-312.

[12] 熊玮. 一种基于位置变换和灰度变换相结合的数字图像置乱方法[J]. 软件导航,2011,10(11):159-161.

[13] 林雪辉,蔡利栋. 基于 Hilbert 曲线的数字图像置乱方法研究[J]. 中国体视学与图像分析,2004,9(4):224-227.