基于离散型 Hopfield 神经网络的图像加密算法

徐子同,高 涛,于正同,时培燕
(长安大学 信息工程学院,陕西 西安 710054)

摘 要:为了提高加密算法的安全性能,该文提出了明文相关的通道关联的同时置乱扩散加密方案,算法中置乱扩散矩阵是与明文图像以及外部密钥相关的。由于明文图像中相邻像素之间的相关性很高,因此,图像加密方案一般采用置乱的方式对图像进行“洗牌”操作,再进行扩散操作改变像素值,即 Fridrich 提出的经典置乱-扩散结构。然而随着图像破解技术的进步,分开攻击技术对这种经典的加密方案造成了很大的影响。该文采用同时置乱扩散的方案提高加密算法的安全性,首先使用三阶神经网络产生密钥流对彩色图像的三通道进行同时置乱扩散操作,然后再对得到的三个通道矩阵进行二次扩散操作,使得加密算法更加安全。对比现有的图像加密方案,该加密算法能够避免分开攻击对加密安全性的影响,提高了算法的安全性。实验结果表明,该算法有良好的加密性能,可以抵抗各种攻击。

关键词:Hopfield 神经网络;图像加密;置乱-扩散结构;同时置乱扩散;信息安全
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2021)06-0106-06
doi:10.3969/j.issn.1673-629X.2021.06.019

Image Encryption Algorithm Based on Discrete Hopfield Neural Network

XU Zi-tong,GAO Tao,YU Zheng-tong,SHI Pei-yan
(School of Information Engineering,Chang'an University,Xi'an 710054,China)

Abstract:In order to improve the security performance of the encryption algorithm,we propose a simultaneous scrambling and diffusion encryption scheme that is plaintext related and channel associated. The scrambling diffusion matrix in the algorithm is related to plaintext image and external key. Since the high correlation between adjacent pixels in plaintext image,image encryption schemes generally use scrambling to permutate the image,and then diffusion operation can change the pixel value,which is the classical permutation-diffusion structure proposed by Fridrich. However,with the progress of image cracking technology,the separate attack technology has a great impact on this classic encryption scheme. We adopt the scheme of simultaneous permutation and diffusion to improve the security of encryption algorithm. First of all,we use the third-order Hopfield neural network to generate the key stream to permutate and diffuse simultaneously for the three channels of the color image,and then carry out the secondary diffusion operation on the three matrices,which makes the encryption algorithm more secure. Compared with the existing image encryption schemes,the proposed algorithm can avoid the impact of separate attacks on the encryption security and improve the security of the algorithm. Experimental results and security analyses verify that the proposed scheme can achieve ideal encryption result and resist various attacks.

Key words:Hopfield neural network;image encryption;permutation-diffusion structure;simultaneous permutation-diffusion operation;information security

1 概 述

随着网络媒体的快速发展,越来越多的图像数据通过公共网络进行传输,保证信息传输的安全性至关重要。一种可以保证图像完整性的加密方式是将明文图像转为类噪声图像再传输,这种信息隐藏方式提高了传输的安全性,目前,越来越多的图像加密算法被提出。由于图像的特殊性,例如数据容量大、像素间的相关性高以及数据冗余等,传统的数据加密算法如 DES、AES 以及 IDEA[1-2] 等不适用于图像加密。近些年,各种类型的加密算法被大量提出[3-14],例如,基于混沌的图像加密[3-6]、基于压缩感知的图像加密[7-8]、基于遗传算法的图像加密等等。离散型 Hopfield 神经

收稿日期:2020-07-15 **修回日期**:2020-11-18
基金项目:国家自然科学基金项目(61302150)
作者简介:徐子同(1996-),男,硕士研究生,研究方向为数字图像处理、深度学习;高 涛,博士,教授,研究方向为图像处理、深度学习与人工智能。

网络是一种稳定的反馈型的神经网络,文中使用三阶神经网络系统,使得图像加密的安全性得到了显著提升。

图像加密的主要思想是改变图像像素值的大小以及改变像素值的位置,即对图像进行扩散和置乱。在传统的加密方案中,置乱过程和扩散过程是分开进行的,攻击者可以通过分开攻击来破解加密方案,这种加密方法很可能会被选择明文攻击。其次,根据密钥是否明文相关,加密算法可以分为两类:第一,加密过程中密钥与明文图像没有关联,是非一次一密的加密方案。此方案中,由于明文图像与密钥相互独立,不同的明文图像加密用到的密钥流是唯一确定的,因此,这种类型的加密方案容易被选择明文攻击。例如文献[15]已经被攻击[16],攻击者选取一幅像素值全为零的特殊图像作为明文图像,加密后得到密文图像,通过对比明文图像和密文图像可以得到加密过程中的两个密钥流,再通过三次异或操作得到密钥图像,完成对加密方案的攻击。第二,加密过程中密钥与明文图像相关联,是一次一密的加密方案。此方案中,由于密钥与明文相关联,并且是一次一密的加密方案,因此,每一幅不同的明文图像加密后都将产生与之对应的一个密钥,并且该密钥需要与方案中其他的固定密钥一起传送给解密方才能完成解密。

为了克服以上加密方案的缺点,该文提出了一种与明文相关的通道关联的同时置乱扩散加密方案。在该加密方案中,密钥流的产生与明文图像相关,不同像素和的明文图像将产生不同的密钥流,但是加密方案中用到的初始密钥是固定的,解密方只需要得到固定的密钥就可以解密图像。这种方案解决了与明文无关的加密方案容易被选择明文攻击的缺点,并且采用同时置乱扩散的方式提高算法的安全性,使得加密算法能够更好地抵抗选择明文攻击。

2　离散型 Hopfield 神经网络

Hopfield 神经网络最早是由美国物理学家 Hopfield 于 1982 年提出的[17]。它主要用于模拟生物神经网络的记忆机制。Hopfield 神经网络是一种全连通的神经网络。三阶神经网络具体形式如下:

$$y = -y_i + \sum_{(i=1)}^{3} w_{ij}\tanh(x_i) \tag{1}$$

$$\boldsymbol{w} = \begin{bmatrix} 2 & -1 & 0 \\ 1.7 & 1.71 & 1.1 \\ -2.5 & -2.9 & 0.56 \end{bmatrix} \tag{2}$$

为了确认其伪随机性,对 Hopfield 神经网络进行了 NIST 随机性测试[18],当 p 值大于 0.01 时,认为它通过了测试。结果见表 1。随机性测试结果表明,基于权值矩阵的 Hopfield 混沌神经网络具有伪随机性。

表 1　NIST 随机性测试

测试标准	p 值	结果
频率检验	0.887 213	通过
块内频数检验	0.416 539	通过
二元矩阵秩检验	0.257 959	通过
离散傅里叶变换	0.768 992	通过
非重叠模块匹配	0.895 326	通过
重叠模块匹配	0.365 744	通过
线性复杂度检验	0.665 482	通过
序列检验	0.965 425	通过
近似熵检验	0.654 783	通过

3　提出的加密算法

该文所提出的图像加密算法包括彩色图像 R、G、B 三通道关联的同时置乱和扩散算法以及二次扩散算法,加密过程中输入明文图像 P,输出密文图像 C;解密过程与之相反。假设图像大小为 $M \times N$,加密过程具体步骤如下所述,加密流程框图如图 1 所示。

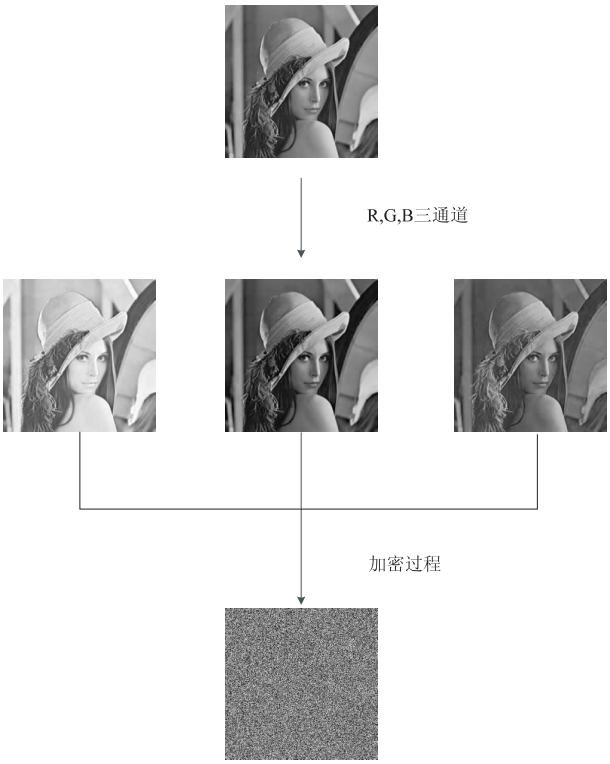


图 1　算法流程

3.1　通道关联的同时置乱扩散

为了更好地抵抗攻击,该文提出了彩色图像通道关联的同时置乱扩散算法,并且在加密过程中用到了明文图像的有效信息,即使明文图像只有 1 bit 的差别,加密后图像也会大不相同。具体的加密过程如下:

(1)分别计算 R、G、B 三通道像素值的和,分别标

记为 sum(R)、sum(G)、sum(B)。通过如下公式计算神经网络系统的初始值,其中 c_1、c_2 以及 c_3 是外部密钥:

$$\begin{cases} x_1(0) = \mathrm{mod}(\mathrm{sum}(R) \times 10^{14}, 256)/255 + c_1 \\ x_2(0) = \mathrm{mod}(\mathrm{sum}(G) \times 10^{14}, 256)/255 + c_2 \\ x_3(0) = \mathrm{mod}(\mathrm{sum}(B) \times 10^{14}, 256)/255 + c_3 \end{cases} \tag{3}$$

其中,mod 是取模运算。

(2)将神经网络系统迭代 1 000 + $M \times N$ 次,为了避免瞬态效应,将前 1 000 次的数值舍弃,得到序列:

$$\begin{cases} X_1 = \{x_1(1\,000+1), x_1(1\,000+2), \cdots, \\ \qquad x_1(1\,000 + M \times N)\} \\ X_2 = \{x_2(1\,000+1), x_2(1\,000+2), \cdots, \\ \qquad x_2(1\,000 + M \times N)\} \\ X_3 = \{x_3(1\,000+1), x_3(1\,000+2), \cdots, \\ \qquad x_3(1\,000 + M \times N)\} \end{cases} \tag{4}$$

明文图像中每个通道的每一个像素值都有可能置换到本通道或另外两个通道中新的位置上,并改变此像素本身的值。通过公式(4)产生的序列首先得到三个决定通道置乱位置的矩阵 $X1\_1$, $X2\_1$ 以及 $X3\_1$:

$$\begin{cases} X1\_1 = \mathrm{mod}(\mathrm{abs}(X_1) \times 10^{14}, 3) + 1 \\ X2\_1 = \mathrm{mod}(\mathrm{abs}(X_2) \times 10^{14}, 3) + 1 \\ X3\_1 = \mathrm{mod}(\mathrm{abs}(X_3) \times 10^{14}, 3) + 1 \end{cases} \tag{5}$$

其中,abs 为取绝对值的操作。

进而分别产生三个通道新的像素位置,具体过程如下:当 $X1\_1(i,j) = 1$ 时,矩阵 $\boldsymbol{R}$ 中像素值 $R(i,j)$ 和 $R(m,n)$ 交换位置,再根据如下公式执行扩散操作改变像素 $R(i,j)$ 的值:

$$R(i,j) = \mathrm{bitxor}(R(i,j), R(m,n)) \tag{6}$$

当 $X1\_1(i,j) = 2$ 时,矩阵 $\boldsymbol{R}$ 中像素值 $R(i,j)$ 和 $G(m,n)$ 交换位置,根据如下公式执行扩散操作改变像素 $R(i,j)$ 的值:

$$R(i,j) = \mathrm{bitxor}(R(i,j), G(m,n)) \tag{7}$$

当 $X1\_1(i,j) = 3$ 时,矩阵 $\boldsymbol{R}$ 中像素值 $R(i,j)$ 和 $B(m,n)$ 交换位置,根据如下公式执行扩散操作改变像素 $R(i,j)$ 的值:

$$R(i,j) = \mathrm{bitxor}(R(i,j), B(m,n)) \tag{8}$$

其中,像素值行位置 m 和列位置 n 计算如下:

$$m = 1 + \mathrm{mod}((\mathrm{abs}(X_1(i,j))) \times 10^{14}, M) \tag{9}$$

$$n = 1 + \mathrm{mod}((\mathrm{abs}(X_1(i,j)) + \mathrm{abs}(X_2(i,j))) \times 10^{14}, N) \tag{10}$$

当 $\boldsymbol{R}$ 通道置乱扩散结束后得到三个新的矩阵 $\boldsymbol{R}\_1$, $\boldsymbol{G}\_1$, $\boldsymbol{B}\_1$。

当 $X2\_1(i,j) = 1$ 时,矩阵 $\boldsymbol{G}\_1$ 中像素值 $G\_1(i,j)$ 和 $G\_1(m,n)$ 交换位置,用如下公式执行扩散操作改变像素 $G\_1(m,n)$ 的值:

$$G\_1(i,j) = \mathrm{bitxor}(G\_1(i,j), G\_1(m,n)) \tag{11}$$

当 $X2\_1(i,j) = 2$ 时,矩阵 $\boldsymbol{G}\_1$ 中像素值 $G\_1(i,j)$ 和 $R\_1(m,n)$ 交换位置,再根据如下公式执行扩散操作改变像素 $G\_1(i,j)$ 的值:

$$G\_1(i,j) = \mathrm{bitxor}(G\_1(i,j), R\_1(m,n)) \tag{12}$$

当 $X2\_1(i,j) = 3$ 时,矩阵 $\boldsymbol{G}\_1$ 中像素值 $G\_1(i,j)$ 和 $B\_1(m,n)$ 交换位置,再根据如下公式执行扩散操作改变像素 $B\_1(i,j)$ 的值:

$$G\_1(i,j) = \mathrm{bitxor}(G\_1(i,j), B\_1(m,n)) \tag{13}$$

其中,像素值行位置 m 和列位置 n 计算如下:

$$m = 1 + \mathrm{mod}((\mathrm{abs}(X_2(i,j))) \times 10^{14}, M) \tag{14}$$

$$n = 1 + \mathrm{mod}((\mathrm{abs}(X_2(i,j)) + \mathrm{abs}(X_3(i,j))) \times 10^{14}, N) \tag{15}$$

当 G 通道置乱扩散结束后得到三个新的矩阵 $\boldsymbol{R}\_2$, $\boldsymbol{G}\_2$, $\boldsymbol{B}\_2$。

当 $X3\_1(i,j) = 1$ 时,矩阵 $\boldsymbol{B}\_2$ 中像素值 $B\_2(i,j)$ 和 $B\_2(m,n)$ 交换位置,再根据如下公式执行扩散操作改变像素 $B\_2(i,j)$ 的值:

$$B\_2(i,j) = \mathrm{bitxor}(B\_2(i,j), B\_2(m,n)) \tag{16}$$

当 $X3\_1(i,j) = 2$ 时,矩阵 $\boldsymbol{B}\_2$ 中像素值 $B\_2(i,j)$ 和 $R\_2(m,n)$ 交换位置,再根据如下公式执行扩散操作改变像素 $B\_2(i,j)$ 的值:

$$B\_2(i,j) = \mathrm{bitxor}(B\_2(i,j), R\_2(m,n)) \tag{17}$$

当 $X3\_1(i,j) = 3$ 时,矩阵 $\boldsymbol{B}\_2$ 中像素值 $B\_2(i,j)$ 和 $G\_2(m,n)$ 交换位置,再根据如下公式执行扩散操作改变像素 $B\_2(i,j)$ 的值:

$$B\_2(i,j) = \mathrm{bitxor}(B\_2(i,j), G\_2(m,n)) \tag{18}$$

$$m = 1 + \mathrm{mod}((\mathrm{abs}(X_1(i,j)) + \mathrm{abs}(X_3(i,j))) \times 10^{14}, N) \tag{19}$$

$$n = 1 + \mathrm{mod}((\mathrm{abs}(X_1(i,j)) + \mathrm{abs}(X_2(i,j)) + \mathrm{abs}(X_3(i,j))) \times 10^{14}, N) \tag{20}$$

当 B 通道置乱扩散结束后得到三个新的矩阵 $\boldsymbol{R}\_3$, $\boldsymbol{G}\_3$, $\boldsymbol{B}\_3$。

3.2 二次扩散算法

为了提高加密算法的安全级别,对矩阵 $\boldsymbol{R}\_3$, $\boldsymbol{G}\_3$, $\boldsymbol{B}\_3$ 进行二次扩散,过程如下:

(1)通过序列 X_1, X_2 以及 X_3 得到三个中间图像矩阵 $\boldsymbol{X}1\_2$, $\boldsymbol{X}2\_2$ 以及 $\boldsymbol{X}3\_2$。

$$\begin{cases} X1\_2 = \lfloor \mathrm{mod}((\mathrm{abs}(X_1 + X_2) - \lfloor X_1 + X_2 \rfloor) \times 10^{14}, 256) \rfloor \\ X2\_2 = \lfloor \mathrm{mod}((\mathrm{abs}(X_1 + X_3) - \lfloor X_1 + X_3 \rfloor) \times 10^{14}, 256) \rfloor \\ X3\_2 = \lfloor \mathrm{mod}((\mathrm{abs}(X_1 + X_2 + X_3) - \lfloor X_1 + X_2 + X_3 \rfloor) \times 10^{14}, 256) \rfloor \end{cases} \tag{21}$$

(2)执行扩散操作。

$$R\_4 = \text{bitxor}(R\_3, X1\_1) \tag{22}$$

$$G\_4 = \text{bitxor}(G\_3, X2\_2) \tag{23}$$

$$B\_4 = \text{bitxor}(B\_3, X3\_3) \tag{24}$$

R_4, G_4, B_4 即加密图像 C 的三个通道。

提出的加密算法是对称的,解密过程是加密过程的逆过程。

4　仿真结果

整个加密算法是基于 MATLAB 实现的,使用的测试图像分别为 Lena(256 × 256)。实现加密方案的密钥以及仿真时的取值如表 2 所示。

表 2　密钥及其仿真时的取值

密钥	取值
sum(R)	11 781 328
sum(G)	6 460 231
sum(B)	6 886 587
c_1	0.1
c_2	0.2
c_3	0.3

仿真结果如图 2 所示。在图 2 中,第一列的图像为明文图像,第二列为加密后的图像,最后一列为解密后的图像。由结果可以看出,这个加密方案是可行的。

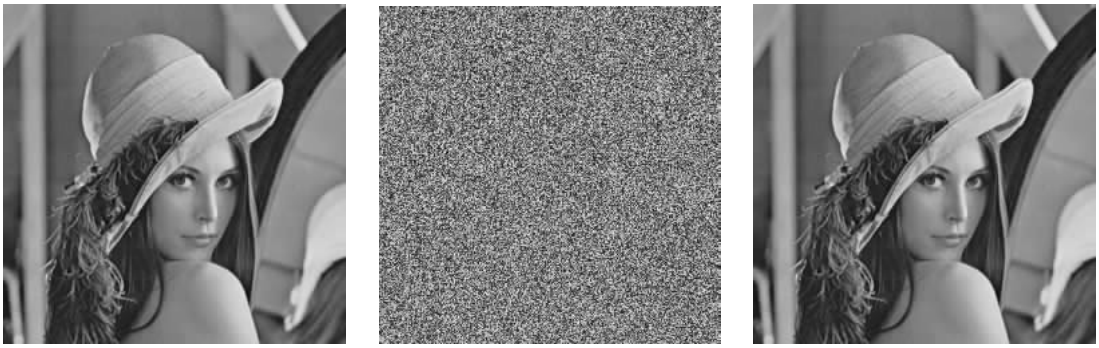


图 2　仿真结果

5　安全性分析

5.1　密钥空间

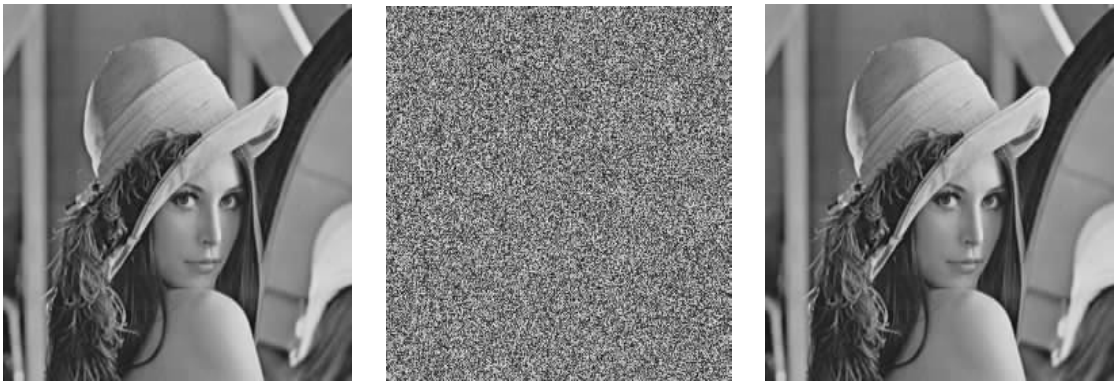
当一个加密方案中密钥空间大于 2^{100} 时,可以认为该加密方案是安全的,可以抵抗暴力攻击。加密算法的密钥包括明文图像 R,G,B 三个通道的像素和以及外部密钥 c_1, c_2, c_3,如果计算机的计算精度为 10^{-14},则提出的算法的密钥空间为 $(10^{14})^6 \approx 2^{289}$,所以认为加密方案是安全的。

5.2　密钥敏感性分析

一个安全有效的加密方案应该保证在加密和解密过程中都是对密钥敏感的,即当密钥取值发生微小的变化时,解密结果将会完全不同。为了测量加密方案的敏感性,选择测试图像 Lena(256 × 256),它的加密后的图像以及解密后的图像分别如图 3 所示。当分别改变 R 通道的像素和以及外部密钥 c_1 的值,改变后的数值如表 3 所示。

表 3　密钥改变值分析

密钥值	改变后的值
sum(R)	sum(R) + 1
sum(G)	sum(G) + 1
sum(B)	sum(B) + 1
c_1	$c_1 + 10^{-14}$
c_2	$c_2 + 10^{-14}$
c_3	$c_3 + 10^{-14}$



明文图像　　密文图像　　正确解密后图像

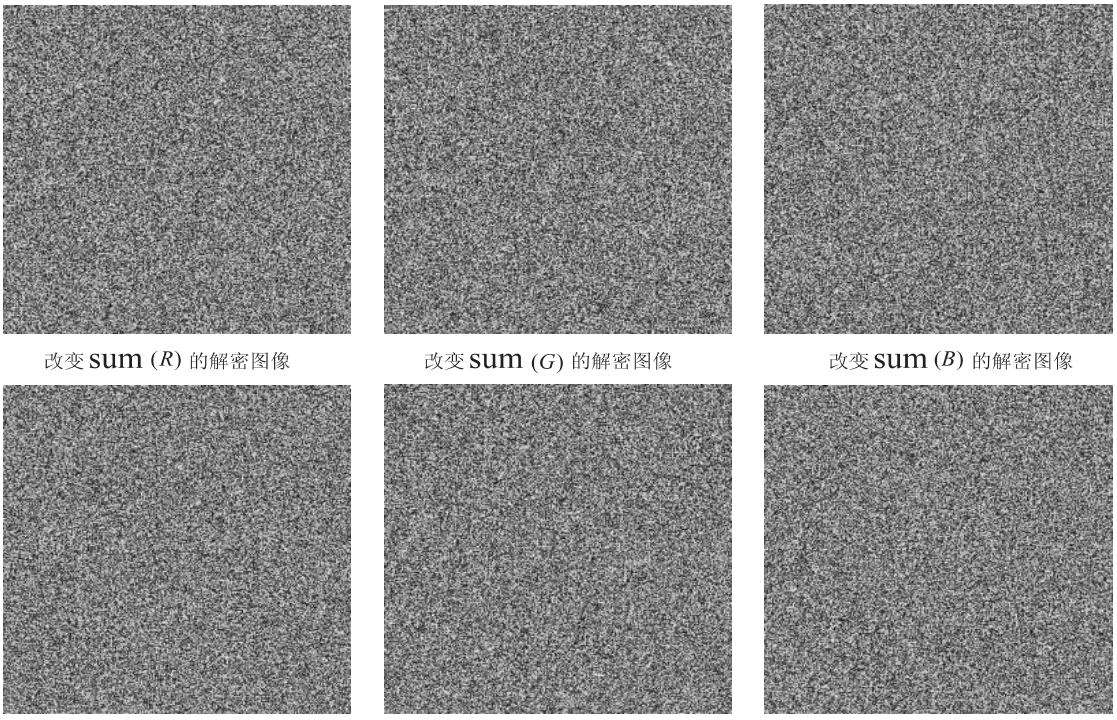


图 3 密钥敏感性分析结果

5.3 直方图分析

图像加密算法抵抗统计攻击的能力可以通过加密后图像的直方图来直观地体现出来。直方图反映了各个不同灰度级的像素个数,直方图越均匀平坦,加密算法抵抗统计攻击的能力越好。选择的测试图像为 Lena。

通常,直方图方差用如下公式计算:

$$\mathrm{var}(V) = 1/n^2 \sum_{(i=1)}^{n} \sum_{(j=1)}^{n} (v_i - v_j)^2$$

其中, $\boldsymbol{V} = \{v_0, v_{1,\cdots,} v_{255}\}$,向量中的每一个值 $v_i(i = 0, 1, \cdots, 255)$ 代表图像中灰度值为 i 的数量。$\mathrm{var}(V)$ 是向量 V 的方差。方差的值越小,直方图越均匀。

由以上分析可知,提出的加密算法加密后图像的直方图更加平坦,能够有效地抵抗统计攻击。

5.4 相关性分析

通常一幅明文图像信息量很大,每一个像素与其相邻像素之间的相关性很高。然而,为了抵抗各种统计攻击,要求加密后图像的像素之间的相关性近似为零。明文图像 Lena 及其加密后图像的相关分布显示,提出的图像加密算法足够抵抗统计攻击。

5.5 抵抗一些典型攻击

通常情况下,对加密系统分析时有四种典型的攻击形式:唯密文攻击、选择密文攻击、已知明文攻击和选择明文攻击。其中,选择明文攻击是对密码系统最有威胁的一种,一般来说,如果一个加密方案能够抵抗选择明文攻击,那么它也有足够的能力去抵抗其他类型的攻击。在提出的方案中,有一些步骤是为了抵抗选择明文攻击而设计的。

加密方案主要的两个步骤:神经网络系统初始值的产生是与明文图像像素和以及外部密钥有关的,即使在外部密钥相同的条件下,不同的明文图像也会产生不同的序列。

6 结束语

该文使用三阶神经网络对彩色图像进行通道间的同时置乱扩散,可以有效地避免置乱和扩散分开攻击对加密算法的影响,实验结果表明,该算法有良好的加密性能,可以抵抗各种攻击。

参考文献:

[1] FIPS PUB 46, data encryption standard (DES), ANSI X3.92-1981, American National Standards Institute[S]. 1999.

[2] FIPS PUB 197, advanced encryption standard (AES), ANSI X3.92-1981, American National Standards Institute[S]. 2001.

[3] 廖晓峰,肖 迪,陈 勇,等. 混沌密码学原理及其应用[M]. 北京:科学出版社,2009:1-40.

[4] 郑继明,高文正. 彩色图像的混沌加密算法[J]. 计算机工程与设计,2011,32(9):2934-2937.

[5] WANG X Y, TENG L, QIN X. A novel colour image encryption algorithm based on chaos[J]. Signal Processing, 2012,92(4):1101-1108.

[6] PAK C, HUANG L L. A new color image encryption using combination of the 1D chaotic map[J]. Signal Processing, 2017,138:129-137.

[7] ZHOU Nanrun, PAN Shumin, CHENG Shan, et al. Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing[J]. Optics & Laser Technology, 2016, 82: 121-133.

[8] GONG L, QIU K, DENG C, et al. An image compression and encryption algorithm based on chaotic system and compressive sensing[J]. Optics & Laser Technology, 2019, 115: 257-267.

[9] 肖成龙,孙　颖,林邦姜,等. 基于神经网络与复合离散混沌系统的双重加密方法[J]. 电子与信息学报, 2020, 42(3): 687-694.

[10] WANG X, SUO G. Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory[J]. Information Sciences, 2020, 507: 16-36.

[11] WANG M, WANG X, ZHANG Y. A novel chaotic system and its application in a color image cryptosystem[J]. Optics and Lasers in Engineering, 2019, 121: 479-494.

[12] CHEN L P, YIN H, YUAN L G, et al. A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and DNA sequence operations[J]. Frontiers of Information Technology & Electronic Engineering, 2020, 21(6): 866-879.

[13] GAO Y, JIAO S M, FANG J C, et al. Multiple-image encryption and hiding with an optical diffractive neural network[J]. Optics Communications, 2020, 463: 125476.

[14] YANG F F, MOU J, CAO Y H, et al. An image encryption algorithm based on BP neural network and hyperchaotic system[J]. China Communications, 2020, 17(5): 21-28.

[15] ZHANG Q, GUO L, WEI X P. A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system[J]. Optik, 2013, 124(18): 3596-3600.

[16] ZHANG Y S, WEN W Y, SU M T. Cryptanalyzing a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system[J]. Optik, 2014, 125(4): 1562-1564.

[17] HOPFIELD J J. Neural networks and physical systems with emergent collective computational abilities[J]. Proc. Nat. Acad. Sci. USA, 1982, 79(8): 2554-2558.

[18] RUKHIN A L, SOTO J, NECHVATAL J R, et al. A statistical test suite for random and pseudo-random number generators for cryptographic applications[M]. [s. l.]: Special Publication (NIST SP), 2001.

(上接第 105 页)

the vehicle cloud[C]//MILCOM 2012 - 2012 IEEE military communications conference. Orlando, FL: IEEE, 2012: 1-6.

[9] YI C, AFANASYEV A, MOISEENKO I, et al. A case for stateful forwarding plane[J]. Computer Communications, 2013, 36(7): 779-791.

[10] AMADEO M, MOLINARO A. CHANET: a content-centric architecture for IEEE 802.11 MANETs[C]//2011 international conference on the network of the future. Paris: IEEE, 2011: 122-127.

[11] AMADEO M, CAMPOLO C, MOLINARO A, et al. Content-centric wireless networking: a survey[J]. Computer Networks, 2014, 72(7): 1-13.

[12] HAN H, WU M, QIAN H, et al. Best route, error broadcast: a content-centric forwarding protocol for MANETs[C]//Vehicular technology conference. Vancouver: IEEE, 2014.

[13] NGUYEN A D, SÉNAC P, DIAZ M. STIgmergy routing (STIR) for content-centric delay-tolerant networks[C]//LAWDN-Latin-American workshop on dynamic networks. Buenos Aires, Argentina: HAL, 2010.

[14] KATEVENIS M, SIDIROPOULOS S, COURCOUBETIS C. Weighted round-robin cell multiplexing in a general-purpose ATM switch chip[J]. IEEE Journal on Selected Areas in Communications, 1991, 9(8): 1265-1279.

[15] 陈秋瑶. NDN 网络区分服务研究[D]. 合肥:中国科学技术大学, 2019.

[16] AMADEO M, CAMPOLO C, MOLINARO A. Named data networking for priority-based content dissemination in VANETs[C]//2016 IEEE 27th annual international symposium on personal, indoor, and mobile radio communications (PIMRC). Valencia: IEEE, 2016: 1-6.

[17] 苏　涛. 基于梯度提升树的行为式验证码人机识别的研究[D]. 武汉:华中师范大学, 2016.