

结合超混沌系统和 Logistic 映射的视频图像加密算法

韦丞婧, 李国东

(桂林电子科技大学 数学与计算科学学院, 广西 桂林 541010)

摘要: 对视频图像使用传统的单幅图像加密算法, 容易出现算法耗时长、效率低等问题。为提高视频图像加密效率, 通过使用细胞神经网络(CNN)超混沌系统和 Logistic 混沌映射, 提出一种单帧逐一加密和多帧组合加密相结合的算法。根据视频帧使用 SHA-256 生成 Logistic 初值, 经过 Logistic 映射迭代得到 Logistic 混沌序列, 利用生成的混沌序列对视频帧逐帧扩散。将视频帧以二进制的形式组合成一个矩阵, 把根据组合矩阵产生的初值代入 CNN 超混沌系统, 利用得到的混沌序列对组合矩阵进行置乱, 视频所有帧各像素点扩散、置乱一步完成, 从而缩短加密时间。在此基础上, 将组合矩阵重新分解为单帧图像, 得到最终加密的视频图像。实验结果表明, 在算法中使用高维超混沌系统安全性更高, 能够有效缩短加密视频图像的耗时, 且能抵抗统计攻击、差分攻击和暴力攻击, 具有较好的安全性。

关键词: 视频加密; 细胞神经网络; 超混沌系统; Logistic 映射; 哈希函数

开放科学(资源服务)标志码(OSID):



中文引用格式: 韦丞婧, 李国东. 结合超混沌系统和 Logistic 映射的视频图像加密算法[J]. 计算机工程, 2022, 48(5): 263-271.

英文引用格式: WEI C J, LI G D. Encryption algorithm of video images combining hyper-chaotic system and Logistic mapping[J]. Computer Engineering, 2022, 48(5): 263-271.

Encryption Algorithm of Video Images Combining Hyper-Chaotic System and Logistic Mapping

WEI Chengjing, LI Guodong

(Department of Mathematics and Computing Science, Guilin University of Electronic Technology, Guilin, Guangxi 541010, China)

[Abstract] Using the traditional single image encryption algorithm for video images is time-consuming and inefficient. To improve the efficiency of video image encryption, combined with the Cellular Neural Network(CNN) hyper-chaotic system and Logistic chaos mapping, an algorithm combining single frame encryption one by one and multi-frame combination encryption is proposed. According to the video frame, SHA-256 generates the initial value of logistic, and the logistic chaotic sequence is obtained through Logistic mapping iteration. The generated chaotic sequence diffuses the video frame by frame. The video frames are combined into a matrix in binary form, and the initial value generated by using the hash function according to the combination matrix is substituted into CNN hyper-chaotic system. The obtained chaotic sequence scrambles the combination matrix, and the diffusion and scrambling of each pixel of all video frames are completed in one step to shorten the encryption time. Simultaneously, the combination matrix is re-decomposed into a single frame image to obtain the final encrypted video image. Experiments show that using a high-dimensional hyper-chaotic system in the algorithm has higher security, effectively shortens the time spent encrypting video images, and can resist statistical attacks, differential attacks, and violent attacks.

[Key words] video encryption; Cellular Neural Network(CNN); hyper-chaotic system; Logistic mapping; Hash function
DOI: 10.19678/j.issn.1000-3428.0061608

0 概述

在互联网技术不断发展、信息传递越发频繁的

时代, 各种形式的信息在网络上的传输极大地方便了人们的生活与工作。但在图像和视频的传输过程中, 这些信息往往容易遭到非法窃取、篡改和传播,

基金项目: 国家自然科学基金“基于边缘探测细胞神经网络的电云判识模型理论研究”(11461063); 桂林电子科技大学研究生教育创新计划项目“基于高维超混沌的伪随机序列设计及在图像加密中的应用研究”(2021YCX119)。

作者简介: 韦丞婧(1996—), 女, 硕士研究生, 主研方向为图像处理、数据挖掘; 李国东, 教授、博士、博士生导师。

收稿日期: 2021-05-11 **修回日期:** 2021-07-09 **E-mail:** weijing@163.com

造成数据泄露,信息的安全得不到保障^[1],尤其是在军事、航天、医学等一些关键领域,图像和视频信息的泄露可能会造成不可估量的损失。

混沌系统因具有确定性、随机性、初值敏感性、遍历性等特点^[2],在图像加密算法设计中得到广泛运用^[3]。同时,目前对混沌系统理论的研究也不断深入^[4-7]。

在图像加密设计研究中,研究者提出了许多针对单幅图像的加密算法设计。文献[8]提出了改进的 Logistic 映射方法,运用置乱-扩散同时操作的方式对图像进行加密。文献[9]提出了一种对多图像重组加密的算法,运用 L-F 级联混沌生成混沌序列,实现了对多幅不同尺寸的图像进行加密。文献[10]提出由 Logistic 映射改进的复合混沌系统,设计了一种新的 S 盒运用于加密。一维混沌映射简单直接,能够快速生成混沌序列,提高加密的速度,但其参数少且形式简单,容易遭到穷举攻击。文献[11]在使用低维混沌映射的基础上,提出结合动态 DNA 编码加密的算法,但根据混沌序列对图像分块选取不同 DNA 编码规则增加了加密用时,效率不高。文献[12]在一维 Logistic 混沌映射的基础上进行改进,扩大了混沌序列取值的范围,但该方法参数少,密钥空间较小。文献[13]提出使用混沌系统与压缩感知的方法对图像进行加密,增加了算法的复杂度,但由于加密过程有损,尽可能降低图像质量损失的方案设计较困难。

高维混沌系统具有复杂的动力学特性,而低维混沌系统应用在加密中安全性不足,这是因为低维混沌系统虽有正的李雅普诺夫指数,但值不够大,且容易发生简并,导致混沌动力学特性退化。同时,低维混沌系统的可变参数较少,导致密钥空间不大,无法抵御穷举攻击^[14]。文献[7]提出运用细胞神经网络(Cellular Neural Network, CNN)混沌系统和 Lorenz 混沌系统进行双扩散加密的方法,增加了加密算法的复杂度和密钥空间,但高维混沌系统结构复杂,增加了计算用时^[1],难以对信息量较大的视频图像进行加密。对于多图像的加密方案设计,文献[15]将多幅图像转换成二维码的方式,根据光学加密原理进行组合加密,实现了对多幅图像的快速加密,提高了效率,但图像转换二维码过程复杂,在实际应用中难以实现。在对视频加密的研究中,部分研究者提出对视频进行选择性的加密的方法。文献[16]提出了先对视频码流进行分析选择,再对选取的部分进行加密的方法,节省了视频加密所需要的时间。然而,这一类视频加密算法在加密过程中需要对视频进行压缩,这会对原视频质量产生影响,因而所设计的加密方案不是无损的。

针对以上问题,本文提出一种视频帧逐一加密与组合加密相结合的视频图像加密算法。对视频帧逐帧

加密,采用计算速度较快的 Logistic 混沌映射,对每帧图像使用哈希函数生成哈希值,计算控制每帧加密对应的混沌序列初值,生成混沌序列,再对视频帧进行逐一异或,达到一帧一密的效果。在此基础上,将所有视频帧进行组合,采用动力学特性更为复杂的六维细胞神经网络混沌系统生成混沌序列,根据混沌序列对组合矩阵进行置乱扩散,再分解为单帧图像完成加密。

1 混沌系统

1.1 神经网络混沌系统

1988年,细胞神经网络(CNN)首次由 CHUA 等提出^[17],其以细胞为基本单位,是一种局部互联的神经网络系统。由 M 行、 N 列个细胞排列组成的细胞神经网络系统定义如下:

$$E_r(i,j) = \{c(m,n) | \max\{|m-i|, |n-j|\} \leq r, 1 \leq m \leq M, 1 \leq n \leq N\} \quad (1)$$

其中: $E_r(i,j)$ 为半径为 r 的第 i 行第 j 列的细胞的邻域; $c(m,n)$ 为邻域内的细胞。

细胞的状态方程可表示如下:

$$P\dot{x}_i = -\left(\frac{1}{R_x}\right)x_{ij} + Q + \sum_{c_{mn} \in E_r(i,j)} A(i,j; k,l)y_{kl} + \sum_{c_{mn} \in E_r(i,j)} B(i,j; k,l)W_{kl} \quad (2)$$

输出方程表示为:

$$y_{ij} = \frac{1}{2}(|x_{ij}(t)+1| - |x_{ij}(t)-1|) \quad (3)$$

其中: $|W_{kl}| \leq 1, |x_{ij}(0)| \leq 1, P > 0, R_x > 0; Q$ 为阈值常数; y_{ij} 为输出变量; P 为线性电容; R_x 为线性电阻; A 为反馈模板; B 为控制模板。

研究表明,高维超混沌系统拥有更优良的混沌特性。因此,本文选用六维细胞神经网络混沌系统,其表达式如下^[18]:

$$\begin{cases} \dot{x}_1 = -x_3 - x_4 \\ \dot{x}_2 = 2x_2 + x_3 \\ \dot{x}_3 = 14x_1 - 14x_2 \\ \dot{x}_4 = 100x_1 - 100x_4 + 200y_4 \\ \dot{x}_5 = 18x_2 + x_1 - x_5 \\ \dot{x}_6 = 4x_5 - 4x_6 + 100x_2 \end{cases} \quad (4)$$

$$y_4 = \frac{1}{2}(|x_4(t)+1| - |x_4(t)-1|)$$

计算 Lyapunov 指数,当 $t \rightarrow \infty$ 时, $\lambda_1 = 2.7481$, $\lambda_2 = -2.9844$, $\lambda_3 = 1.2411$, $\lambda_4 = -14.4549$, $\lambda_5 = -1.4123$, $\lambda_6 = -83.2282$,其中有2个正的李雅普诺夫指数,说明系统是超混沌系统。相比于仅使用一个一维混沌映射产生的6个混沌序列,使用六维 CNN 混沌系统产生的6个混沌序列动力学特性更复杂,随机性更高。因为具有

2个及以上正的李雅普诺夫指数的混沌序列表明混沌轨道能够从多个维度产生分离,从而增加了不同序列间数值的随机性。

1.2 Logistic 混沌映射

Logistic 混沌映射是最简单的一维混沌映射。1995年,PHATAK对Logistic混沌映射的混沌特性进行了研究^[19],给出其表达式为:

$$X_n = \mu X_{n-1} (1 - X_{n-1}) \quad (5)$$

其中: $X_n \in (0, 1), n = 1, 2, \dots$ 。经研究表明,当 $\mu \in [3.569\ 945\ 627, 4]$ 时,序列 X_n 处于混沌状态。该一维混沌序列计算形式简单,且有很好的伪随机序列特性,被广泛运用于图像加密中。

2 伪随机序列发生器设计

获取混沌序列首先需要确定初始值^[20]。根据混沌系统的初值敏感性,当初值仅发生微小变化时就会使得混沌序列的数值发生很大的变化。因此,在本文算法中,对视频每隔固定帧数选取一个视频帧,利用哈希函数生成该视频帧图像信息的摘要,并根据摘要信息计算更新伪随机序列的初值,以用于对视频的逐帧加密。将每次加密所用到的混沌系统的初值作为密钥,使得算法的密钥与视频明文图像相关,所需要加密的视频图像不同,产生的密钥也不同。

2.1 逐帧加密的伪随机序列发生器

将短视频按帧分成 s 张尺寸都为 $M \times N$ 的图像,间隔 f 帧更新一次混沌序列的初值,根据第 $1 + nf (n = 0, 1, \dots; 1 + nf \leq s)$ 帧图像的像素矩阵,使用 SHA-256 哈希函数生成 256 位二进制表示的哈希值 L_{1+nf} :

$$L_{1+nf} = \{l_{(1+nf)1}, l_{(1+nf)2}, \dots, l_{(1+nf)256}\} \quad (6)$$

$$l_{(1+nf)j} \in \{0, 1\}, j = 1, 2, \dots, 256$$

将 L_{1+nf} 转化成十进制数:

$$L'_{1+nf} = \{l'_{(1+nf)1}, l'_{(1+nf)2}, \dots, l'_{(1+nf)78}\} \quad (7)$$

$$l'_{(1+nf)j} \in \{0, 1, \dots, 9\}, j = 1, 2, \dots, 78$$

从 L'_{1+nf} 中从左到右,每 10 位数字组成一个数,前一个数和后一个数按位异或再乘以 10^{-10} ,得到由第 $1 + nf$ 帧图像产生的混沌序列的初值 $x_{1+nf}(0)$:

$$x_{1+nf}(0) = ((l'_{(1+nf)1} l'_{(1+nf)2} \dots l'_{(1+nf)10}) \oplus \dots \oplus (l'_{(1+nf)61} l'_{(1+nf)62} \dots l'_{(1+nf)70})) \times 10^{-10} \quad (8)$$

将初值代入到 Logistic 混沌系统中,迭代 $100 + MN - 1$ 次,去掉前 100 个值得到混沌序列 $x_{1+nf}(t), t = 101, 102, \dots, 100 + MN - 1$,再将混沌序列转换成取值范围在 $[0, 255]$ 之间的数:

$$S_{1+nf}(t) = \text{floor}(x_{1+nf}(t) \times 10^{14}) \bmod 256 \quad (9)$$

$$t = 101, 102, \dots, 100 + MN - 1$$

2.2 组合加密的伪随机序列发生器

将 s 个 $M \times N$ 的像素矩阵转成二进制,组合成一

个 $MN \times 8$ 的矩阵,根据组合矩阵使用 SHA-256 哈希函数生成 256 位哈希值 C :

$$C = \{c_1, c_2, \dots, c_{256}\} \quad (10)$$

$$c_i \in \{0, 1\}, i = 1, 2, \dots, 256$$

将 C 转化成十进制数 C' :

$$C' = \{c'_1, c'_2, \dots, c'_{78}\} \quad (11)$$

$$c'_i \in \{0, 1, \dots, 9\}, i = 1, 2, \dots, 78$$

从 C' 中从左到右取,每 10 位数字组成一个数,共取 60 位,再分别乘以 10^{-10} 得到混沌序列的初值 $x(0) = \{x_{01}(0), x_{02}(0), x_{03}(0), x_{04}(0), x_{05}(0), x_{06}(0)\}$ 。

将 $x(0)$ 代入六维 CNN 方程中,迭代 $100 + M \times N - 1$ 次,生成 6 个混沌序列,去掉前 100 个值,得到 $x(t) = \{x_1(t), x_2(t), x_3(t), x_4(t), x_5(t), x_6(t)\}, t = 101, 102, \dots, 100 + MN - 1$ 。对混沌序列做以下处理,将序列的取值范围变成 $[1, M \times N]$:

$$S(t) = \text{abs}(\text{floor}(x(t) \times 10^{14})) \bmod (M \times N) + 1 \quad (12)$$

$$t = 101, 102, \dots, 100 + MN - 1$$

3 多帧图像组合方法设计

本文对多帧图像组合的方法采用类似于计算机使用二进制储存信息的方式。例如,十进制数 11 和其二进制形式 1011 之间相互转换的规则为:

$$\begin{cases} \text{floor}(11 \div 2^3) = 1 \\ \text{floor}((11 - 1 \times 2^3) \div 2^2) = 0 \\ \text{floor}((11 - 1 \times 2^3 - 0 \times 2^2) \div 2^1) = 1 \\ \text{floor}((11 - 1 \times 2^3 - 0 \times 2^2 - 1 \times 2^1) \div 2^0) = 1 \end{cases}$$

$$1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 11 \quad (13)$$

同样地,设视频共有 s 帧,将视频帧 $I = \{I_1, I_2, \dots, I_s\}$ 转换成二进制,得到 $I' = \{I'_1, I'_2, \dots, I'_s\}$, $I'_i (i = 1, 2, \dots, s)$ 是 $M \times N$ 行 8 列、元素取值为 0 或 1 的矩阵,再做以下运算得到组合矩阵 P :

$$P = \sum_{i=1}^s 2^{i-1} \times I'_i \quad (14)$$

由于组合矩阵的每一行表示所有视频帧在相同位置的像素值,因此对组合矩阵进行置乱不仅会改变像素点的值,也会改变像素点的位置。

对组合矩阵 P 再按十进制转二进制的方式,可以重新分解成 s 个 $M \times N$ 行 8 列的二进制矩阵:

$$I'_i = \text{floor}(P \div 2^{i-1}) \quad (15)$$

$$I'_i = \text{floor}\left(\left(P - \sum_{j=1}^{i-1} I'_j \times 2^{j-1}\right) \div 2^{i-1}\right)$$

$$i = 2, 3, \dots, s$$

4 图像加密

以灰度视频图像为例,完整的加密步骤描述

如下:

- 1) 将视频按帧分成 s 个 $M \times N$ 的图像像素矩阵。
- 2) 设置更新 Logistic 混沌初值的帧间隔 f , 对第 $1+nf$ ($n=0, 1, \dots; 1+nf \leq s$) 个像素矩阵分别使用 SHA-256 哈希函数生成图像的哈希值, 经过 2.1 节所描述的算法计算得到加密第 $1+nf$ 帧到第 $(n+1)f$ 帧图像对应的 Logistic 混沌序列的初值 $x_{1+nf}(0)$, 代入 Logistic 混沌系统迭代得到 $n+1$ 个混沌序列 $x_{1+nf}(t)$, 并将序列按式(9)处理成取值范围为 $[0, 255]$ 的伪随机序列 $S_{1+nf}(t)$ 。
- 3) 将 Logistic 混沌序列 S_{1+nf} 分别与第 $1+nf$ 帧~第 $(n+1)f$ 帧图像像素矩阵 $I_{1+nf}, I_{1+nf+1}, \dots, I_{(n+1)f}$ 按位异或, 最终得到经过逐帧加密的视频帧。
- 4) 把每个经过逐帧加密后的像素矩阵 I'_i ($i=1, 2, \dots, s$) 转换成 s 个 MN 行 8 列的二进制矩阵。按照式(14)组合成一个 MN 行 8 列的组合矩阵 P 。由于计算机能达到的精度是 10^{-15} , 因此进行一次组合最多能组合 52 帧图像矩阵。若需要加密的视频帧超过 52 帧, 则需要每 52 帧做一个组合矩阵, 再对多个组合矩阵分别进行加密。
- 5) 对组合矩阵 P 按照 2.2 节所述方法, 使用 SHA-256

函数生成组合矩阵的哈希值 C , 经过计算得到 CNN 混沌系统的初值 $x(0)$, 代入 CNN 混沌系统迭代得到 6 个混沌序列 $x(t)$, 并将序列按式(12)处理成取值范围为 $[1, M \times N]$ 的伪随机序列 S 。

6) 按从左到右、从上到下的顺序将 $P(i, j)$ 的值与 $P(u, v)$ 的值互换, 其中 u, v 计算公式如下:

$$\begin{cases} u = S(i, j \bmod 6 + 1) \\ v = S(i, (j + 1) \bmod 6 + 1) \bmod 8 + 1 \end{cases} \quad (16)$$

7) 将替换后的组合矩阵按式(15)重新分解为 s 个二进制矩阵 E_i ($i=1, 2, \dots, s$), 转回十进制表示形式, 即得到 s 帧加密视频帧 E'_i ($i=1, 2, \dots, s$)。

由于本文设计的加密算法为无损加密算法, 因此解密过程即为加密过程的逆过程。将加密步骤用流程图表示, 如图 1 所示。其中: $L_{1+1 \times f}, L_{1+2 \times f}, \dots, L_{1+n \times f}$ 和 $C_1, C_2, C_{[s/52]+1}$ 分别为根据视频帧、组合矩阵使用 SHA-256 生成的哈希值; $x_{1+i \times f}(0)$ 为第 $1+i \times f$ ($i=1, \dots, n$) 帧图像对应的 Logistic 混沌序列的初值; $x_1(0), x_2(0), x_{[s/52]+1}(0)$ 为 CNN 混沌序列的初值, $S_{1+i \times f}(t)$ 为第 $1+i \times f$ ($i=1, \dots, n$) 帧图像对应的 Logistic 混沌序列; $S_1(t), S_2(t), S_{[s/52]+1}(t)$ 为对应的 CNN 混沌序列。

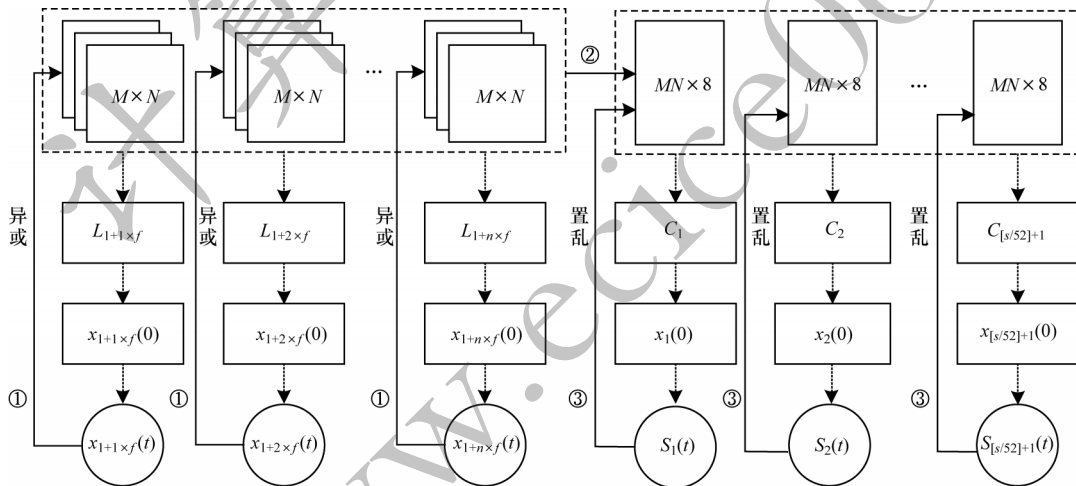


图 1 加密流程

Fig.1 Encryption process

5 实验仿真和安全性分析

选取 2 个 320×240 视频的前 12 帧图像作为仿真实验中需要加密的图像。在逐帧加密中, 对每一帧图像都更新 Logistic 混沌序列的初值, 即更新初值的帧间隔 $f=1$ 。将本文算法中六维 CNN 混沌序列改为初值不同、参数相同计算生成的 6 个 Logistic 混沌序列, 同样对视频图像进行加密, 比较两种加密方案的安全性能。经过本文算法加密, 分别得到 2 个视频图像中第 6、12 帧的明文图像、加密图像和解密图像, 如图 2、图 3 所示。

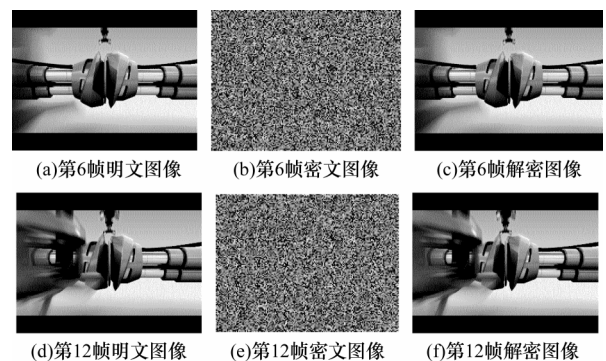


图 2 视频 A 部分帧加密和解密结果

Fig.2 Encryption and decryption results for part of frames of video A

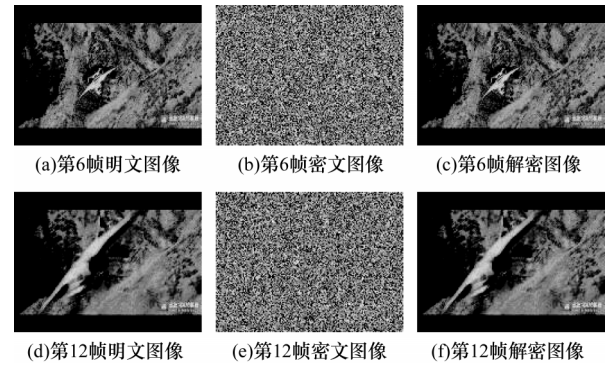


图 3 视频 B 部分帧加密和解密结果
Fig.3 Encryption and decryption results for part of frames of video B

5.1 信息熵分析

信息熵是对信息量的量化度量,信息熵越接近 8,表示图像所含信息量越小,随机性越强。本文计算了视频 A 和视频 B 每帧图像加密前后的信息熵,如表 1 所示。表 2 给出了视频 A 加密后平均每帧的信息熵,和仅使用一维 Logistic 混沌映射进行加密、其他文献提出的图像加密算法做比较。

表 1 视频帧加密前后信息熵

Table 1 Entropy of video frames before and after encryption				
帧数	视频 A		视频 B	
	明文图像	密文图像	明文图像	密文图像
1	3.873 6	7.997 8	3.566 1	7.997 5
2	3.980 3	7.997 8	3.573 1	7.997 5
3	3.971 4	7.997 6	3.573 0	7.998 1
4	4.059 5	7.998 0	3.577 1	7.998 0
5	4.062 1	7.997 6	3.589 3	7.997 9
6	4.030 9	7.997 7	3.600 2	7.997 4
7	4.026 9	7.997 8	3.628 4	7.997 5
8	4.020 1	7.997 6	3.665 2	7.997 3
9	3.978 6	7.998 0	3.705 0	7.997 6
10	3.973 8	7.997 6	3.731 1	7.997 1
11	3.952 3	7.997 5	3.745 6	7.997 7
12	3.955 8	7.998 0	3.794 2	7.997 6

表 2 不同加密算法的信息熵比较

Table 2 Entropy comparison of different encryption algorithms		
算法	明文图像	密文图像
本文算法	3.990 4	7.997 8
仅用一维混沌算法	3.990 4	7.997 7
文献[6]算法	7.453 2	7.989 7
文献[8]算法	7.453 2	7.997 8
文献[15]算法	7.569 7	7.997 5
文献[22]算法	7.453 2	7.999 2
文献[23]算法	7.692 7	7.996 9

由表 1 和表 2 可以看出:经过加密后视频帧的信息熵皆达到了 7.997,加密效果较好;本文的算法相比于其他算法加密的信息熵处于较高水平,且相比于仅用一维混沌加密得到的信息熵更高一些。

5.2 密钥空间分析

在本文设计的算法中,所用的 Logistic 混沌映射的 1 个参数和 6 阶 CNN 超混沌系统的 78 个参数可作为密钥,计算精度为计算机所能达到的精度 10^{-14} ;在逐帧加密中,将每次更新得到的 Logistic 映射的初值作为密钥,算法中精度为 10^{-10} ,可根据实际需要调整更新初值的间隔帧数,间隔越大,密钥个数越少;在组合加密中,每个组合矩阵所对应的 CNN 混沌系统的 6 个初值作为密钥,精度同样为 10^{-10} 。在本文的仿真实验中,密钥空间可以计算为 $10^{14 \times 79} \times 10^{10 \times 12} \times 10^{10 \times 6} = 10^{1286}$ 。本文算法密钥空间足够大,能够抵御穷举攻击,且能够根据实际加密需要调整密钥个数,提高加密效率。

5.3 密钥敏感性分析

在图像加密中,密钥的敏感性是评价加密算法是否安全的一个重要指标。当算法的密钥仅发生微小变化,就能导致使解密失败,从而很好地抵御攻击。在本文实验中,将生成第 1 个 Logistic 混沌的初值减小,再对密文图像进行解密,得到第 3 帧的解密图像,如图 4 所示。可以看出,本文提出的算法密钥敏感性较强。

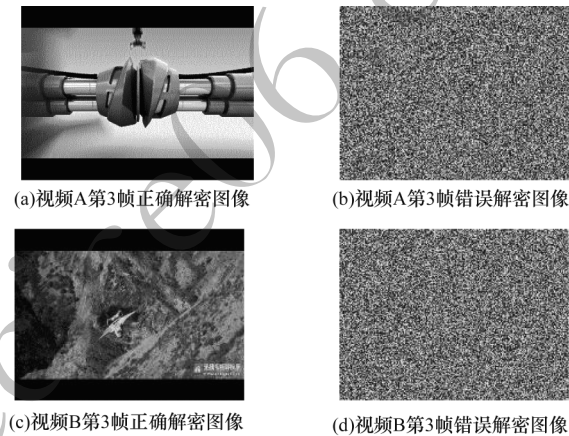


图 4 改变密钥进行解密结果图
Fig.4 Decryption results of changing key to ecrypt

5.4 抗差分攻击能力分析

破译者选用对指定像素点的值进行改变的不同明文图像,对同一加密算法进行加密,通过分析每次加密后图像之间的关联与差别总结出加密算法,能够达到破译的目的。若明文图像改变像素点的值后密文图像像素点的值随之改变,则能很好地抵抗差分攻击。NPCR 和 UACI 指标能衡量密文图像的抗差分攻击能力,计算公式如下:

$$N_{NPCR} = \frac{\sum_{i=1}^M \sum_{j=1}^N D(i,j)}{M \times N} \times 100\% \tag{17}$$

$$U_{UACI} = \frac{\sum_{i=1}^M \sum_{j=1}^N |C1(i,j) - C2(i,j)|}{255 \times M \times N} \times 100\%$$
$$D(i,j) = \begin{cases} 1, C_1(i,j) = C_2(i,j) \\ 0, C_1(i,j) \neq C_2(i,j) \end{cases} \tag{18}$$

其中: $C_1(i,j)$ 和 $C_2(i,j)$ 分别为明文图像和更改了一个像素点的值的明文图像经过同样加密算法加密后第*i*行第*j*列的像素值。

在仿真实验中,分别将视频A和视频B第3帧明文图像第80行第100列的像素值改为0,经过加密后计算图像更改像素值前后的NPCR值和UACI值,并和仅使用一维Logistic混沌映射进行加密、其他文献加密算法进行比较,结果如表3所示。可以看出,仅仅更改其中一帧图像的一个像素点的值,就能使每一帧的密文图像大部分像素值都发生变化。加入CNN高维混沌系统进行加密的UACI值有更好的表现,说明本文的加密算法较好。

表3 视频帧NPCR和UACI的值		
Table 3 NPCR and UACI of video frames		
算法	NPCR	UACI
本文算法(对视频A加密)	99.606 3	33.470 3
本文算法(对视频B加密)	99.606 6	33.443 9
仅用一维混沌算法(对视频A加密)	99.608 0	33.453 7
文献[6]算法	99.595 6	33.390 0
文献[8]算法	99.610 0	33.450 0
文献[15]算法	99.620 0	31.590 0
文献[22]算法	99.621 6	33.463 2
文献[23]算法	99.154 7	33.207 2

5.5 抗剪切攻击能力分析

视频图像在传输过程中还容易遭到剪切攻击,

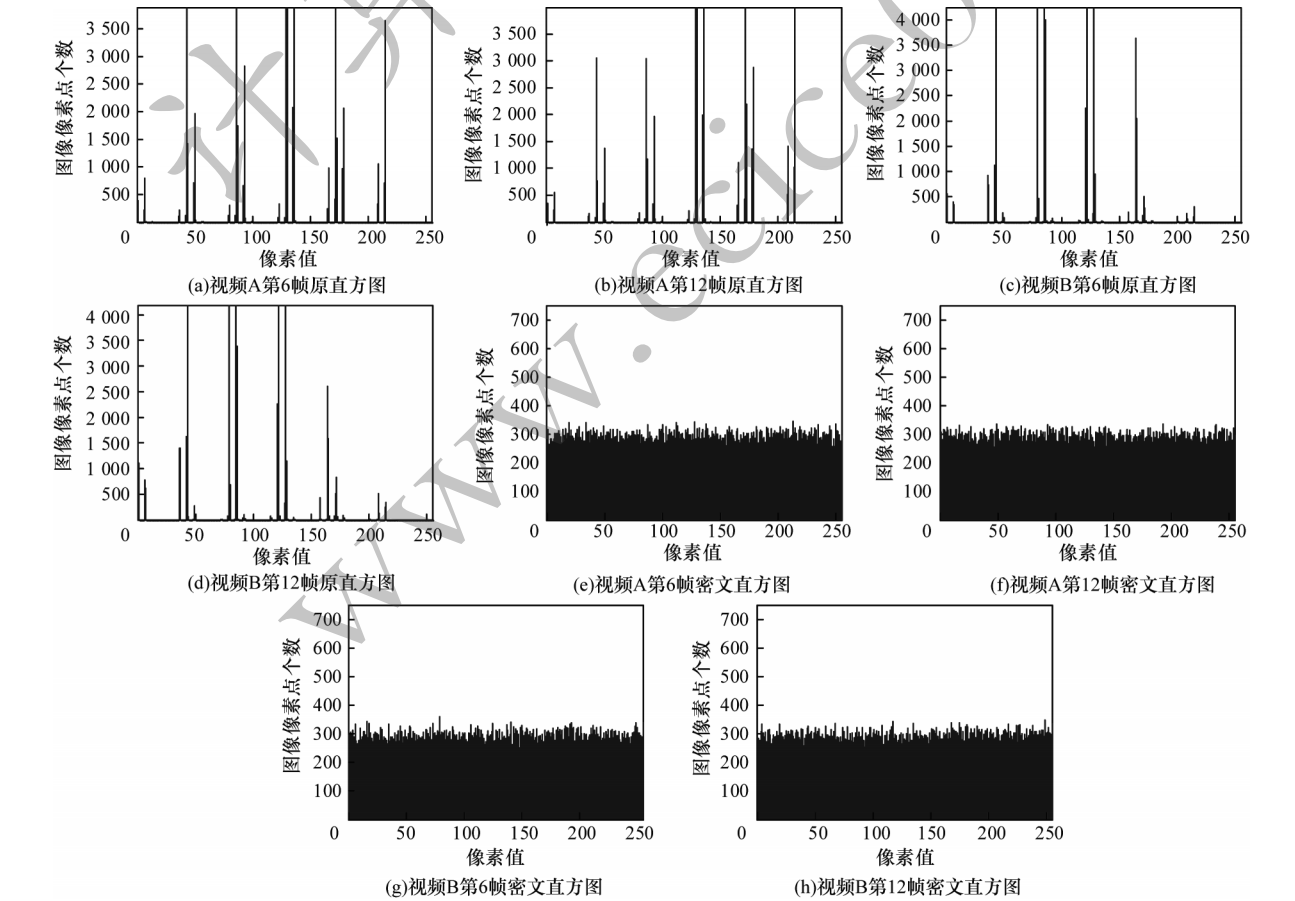


图6 视频加密前后直方图

Fig.6 Histograms of video frames before and after encryption

导致部分数据丢失的情况^[8]。本文实验测试视频A丢失1/4、1/2的数据时解密的效果。图5为解密前后第3帧的图像,可以看到,解密后的视频帧仍能基本还原图像,肉眼能够分辨得出图像内容,说明本文算法的抗剪切攻击能力较强。

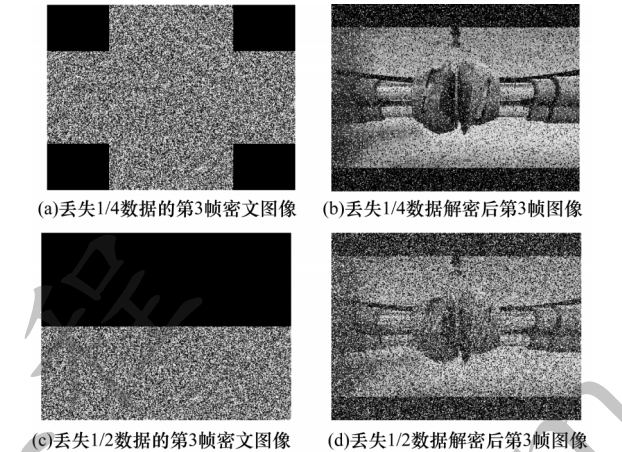


图5 视频A第3帧丢失部分数据解密效果

Fig.5 Decryption of the third frame of video A with partial data missing

5.6 直方图分析

分别绘制视频A和视频B的第6帧、第12帧明文图像、密文图像直方图,如图6所示。可以看出,视频帧原图像直方图分布及不均匀,呈现出了明显的规律,经过加密后像素点基本能在[0,255]范围内均匀取值。

5.7 相邻像素点相关性分析

明文图像的相邻像素点通常具有较高相关性,相关系数接近于1。对图像进行加密需要消除这种相邻像素点间的相关性,才能很好地抵抗统计攻击。本文对视频A和视频B每一帧都在水平、垂直、对角3个方向上计算其相关系数,结果如表4、表5所示。可以看出,经过本文加密后像素点相关系数都接近于0。

表4 视频A每帧相邻像素点相关系数

Table 4 Correlation indexes between adjacent pixels of video A						
帧数	明文图像			密文图像		
	水平	垂直	对角	水平	垂直	对角
1	0.926 8	0.949 5	0.926 3	0.008 4	0.003 3	0.001 8
2	0.926 3	0.944 5	0.923 0	0.007 6	0.002 3	0.001 8
3	0.930 0	0.947 4	0.928 1	0.010 7	0.002 6	0.005 2
4	0.925 3	0.936 5	0.921 2	0.004 6	0.007 3	0.006 8
5	0.927 6	0.942 5	0.927 3	0.000 1	0.012 7	0.003 3
6	0.935 8	0.951 0	0.932 0	0.006 6	0.004 7	0.007 8
7	0.931 0	0.950 0	0.929 7	0.003 2	0.006 0	0.002 2
8	0.934 2	0.947 2	0.931 5	0.003 6	0.002 4	0.002 1
9	0.934 7	0.945 3	0.928 1	0.007 3	0.001 6	0.002 2
10	0.940 8	0.951 7	0.941 7	0.003 4	0.004 4	0.008 0
11	0.935 5	0.946 2	0.929 1	0.004 8	0.005 4	0.000 8
12	0.932 3	0.947 9	0.926 6	0.008 5	0.004 5	0.002 9

表5 视频B每帧相邻像素点相关系数

Table 5 Correlation indexes between adjacent pixels of video B						
帧数	明文图像			密文图像		
	水平	垂直	对角	水平	垂直	对角
1	0.890 6	0.888 4	0.865 4	0.002 8	0.000 1	0.004 8
2	0.891 5	0.891 9	0.866 2	0.001 8	0.004 3	0.001 2
3	0.894 1	0.892 9	0.866 9	0.005 6	0.005 9	0.002 1
4	0.893 1	0.892 3	0.867 5	0.000 5	0.001 5	0.002 3
5	0.894 9	0.892 6	0.868 2	0.000 3	0.002 9	0.004 2
6	0.896 7	0.896 5	0.869 6	0.007 4	0.004 8	0.006 9
7	0.899 4	0.898 9	0.872 7	0.002 1	0.005 3	0.005 2
8	0.901 5	0.901 4	0.876 2	0.006 5	0.002 8	0.002 7
9	0.906 6	0.907 8	0.884 3	0.001 1	0.002 3	0.005 9
10	0.910 9	0.913 7	0.890 0	0.000 8	0.005 7	0.007 5
11	0.915 9	0.921 2	0.901 5	0.002 6	0.004 0	0.002 5
12	0.920 4	0.925 5	0.910 0	0.000 3	0.002 3	0.010 5

表6给出了仿真实验中视频A加密后平均每帧相关系数,和仅使用一维Logistic混沌映射进行加密、其他文献提出的图像加密算法进行比较。可以看出,本文算法平均每帧相关系数最低达到0.003 749,很好地消除了像素点间的相关性,且使用CNN高维超混沌系统生成序列进行加密后像素点间的相关系数更低。

表6 相邻像素点相关系数比较

Table 6 Comparison of correlation coefficients between adjacent pixels

算法	明文图像			密文图像		
	水平	垂直	对角	水平	垂直	对角
本文算法	0.931 7	0.946 6	0.928 7	0.005 7	0.004 8	0.003 7
仅用一维混沌算法	0.931 7	0.946 6	0.928 7	0.003 5	0.005 3	0.004 7
文献[6]算法	0.968 4	0.939 4	0.917 2	0.006 0	0.003 8	0.003 3
文献[8]算法	0.975 7	0.936 5	0.901 8	0.007 7	0.009 0	0.017 8
文献[15]算法	0.976 5	0.963 7	0.934 2	0.009 7	0.006 5	0.001 6
文献[22]算法	0.960 0	0.975 8	0.957 5	0.010 4	0.027 2	0.009 7
文献[23]算法	0.952 6	0.983 9	0.946 6	0.0060	0.033 0	0.047 4

选取视频A和视频B的第3帧,分别绘制加密前在水平、垂直、对角3个方向上相邻像素点的散点图,如图7、图8所示。可以看出,视频帧明文图像的相邻像素点散点图呈线性趋势,而加密后的散点图均分布均匀。

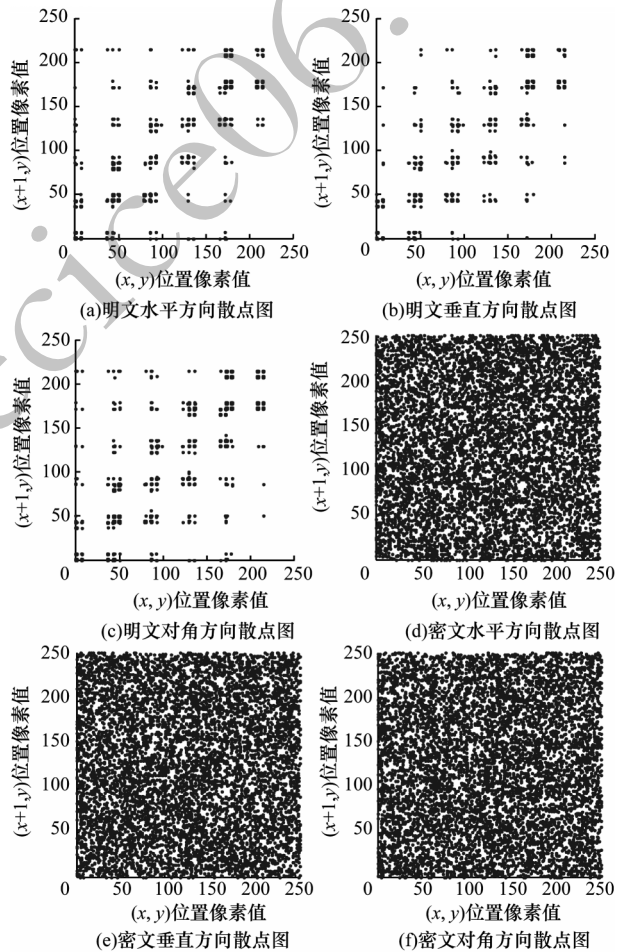


图7 视频A第3帧加密前后相邻像素点散点图

Fig.7 Adjacent pixel scatter plot of the third frame of video A before and after encryption

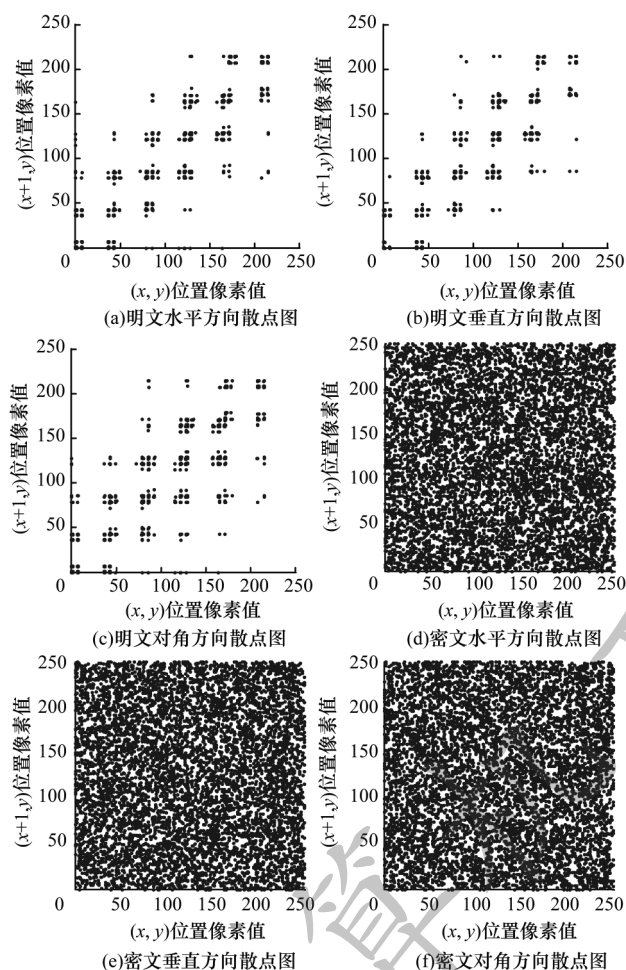


图8 视频B第3帧加密前后相邻像素点散点图

Fig.8 Adjacent pixel scatter plot of the third frame of video B before and after encryption

6 结束语

本文提出一种对视频帧图像逐一加密、组合加密相结合的视频加密算法。利用结构简单的一维 Logistic 混沌序列逐帧加密,通过随机性较强的六维 CNN 混沌序列对视频帧组合矩阵进行置乱。仿真实验结果表明,该算法引入具有复杂动力学特性的高维混沌系统,安全性能相比于仅使用一维混沌的算法要高,且具有较好的稳定性,同时算法复杂度和密钥个数可根据需要灵活改变,能适应不同的视频长度和不同的加密安全需要。此外,设计的组合加密方法能够通过一轮操作实现像素点位置和取值同时改变,提高了加密算法的效率。相比于单幅图像的加密,本文算法对视频按帧进行加密,所需要处理的数据量更大,更适用于对包含重要信息的短视频进行加密。后续将把算法推广到对时长更长、清晰度更高的视频进行加密,并进一步提高加密效率。

参考文献

- [1] 周峰,金蒙,鄂姝. 视频图像篡改鉴定技术[J]. 中国公共安全(学术版),2016(4):112-115.
ZHOU F, JIN M, E S. Identification techniques of video image tampering[J]. China Public Security, 2016(4):112-115. (in Chinese)
- [2] 武凯,李国东. 用细胞神经网络与无限折叠映射对图像加密[J]. 哈尔滨理工大学学报,2015,20(3):30-34.
WU K, LI G D. A scheme on image encryption based on dimensional chaotic system [J]. Journal of Harbin University of Science and Technology, 2015, 20(3):30-34. (in Chinese)
- [3] 沈淑涛,尼玛扎西. 基于区块链技术的双混沌可识别篡改图像加密方法[J]. 吉林大学学报(工学版),2021,51(3):1055-1059.
SHEN S T, NIMA Z X. Double chaos identifiable tampering image encryption method based on blockchain technology[J]. Journal of Jilin University (Engineering and Technology Edition), 2021, 51(3):1055-1059. (in Chinese)
- [4] 谢国波,王添. 一种新的基于比特置乱的超混沌图像加密算法[J]. 微电子学与计算机,2016,33(7):28-32,38.
XIE G B, WANG T. A novel hyperchaotic image encryption algorithm based on bit scrambling [J]. Microelectronics & Computer, 2016, 33(7):28-32, 38. (in Chinese)
- [5] 赵锋,吴成茂. 自编码和超混沌映射相结合的图像加密算法[J]. 计算机辅助设计与图形学学报,2016,28(1):119-128.
ZHAO F, WU C M. Image encryption algorithm combined self-encoded theory with super-chaotic mapping[J]. Journal of Computer-Aided Design & Computer Graphics, 2016, 28(1):119-128. (in Chinese)
- [6] 张勋才,刘奕杉,崔光照. 基于DNA编码和超混沌系统的图像加密算法[J]. 计算机应用研究,2019,36(4):1139-1143.
ZHANG X C, LIU Y S, CUI G Z. Image encryption algorithm based on DNA encoding and hyper-chaotic system [J]. Application Research of Computers, 2019, 36(4):1139-1143. (in Chinese)
- [7] 魏慧,李国东. 基于细胞神经网络超混沌特性的图像加密算法[J]. 微电子学与计算机,2020,37(5):43-48,53.
WEI H, LI G D. Image encryption algorithm based on hyperchaotic characteristics of cellular neural networks[J]. Microelectronics & Computer, 2020, 37(5):43-48, 53. (in Chinese)
- [8] 曾祥秋,叶瑞松. 基于改进Logistic映射的混沌图像加密算法[J]. 计算机工程,2021,47(11):158-165,174.
ZENG X Q, YE R S. Chaotic image encryption algorithm based on improved logistic map[J]. Computer Engineering, 2021, 47(11):158-165, 174. (in Chinese)
- [9] 郭媛,周艳艳,敬世伟. 基于图像重组和比特置乱的多图像加密[J]. 光子学报,2020,49(4):174-186.
GUO Y, ZHOU Y Y, JING S W. Multiple-image encryption based on image recombination and bit scrambling[J]. Acta Photonica Sinica, 2020, 49(4):174-186. (in Chinese)
- [10] FARAH M A B, FARAH A, FARAH T. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box[J]. Nonlinear Dynamics, 2020,

- 99(4):3041-3064.
- [11] ZHENG J Y, LIU L F. Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic sine map[J]. IET Image Processing, 2020, 14(11): 2310-2320.
- [12] CUN Q Q, TONG X J, WANG Z, et al. Selective image encryption method based on dynamic DNA coding and new chaotic map[J]. Optik, 2021, 243: 1-10.
- [13] WEI D Y, JIANG M J. A fast image encryption algorithm based on parallel compressive sensing and DNA sequence [J]. Optik, 2021, 238: 1-10.
- [14] 温贺平,禹思敏,吕金虎. 基于Hadoop大数据平台和无筒并高维离散超混沌系统的加密算法[J]. 物理学报, 2017, 66(23): 76-89.
- WEN H P, YU S M, LÜ J H. Encryption algorithm based on Hadoop and non-degenerate high-dimensional discrete hyperchaotic system[J]. Acta Physica Sinica, 2017, 66(23): 76-89. (in Chinese)
- [15] LI W, CHANG X Y, YAN A M, et al. Asymmetric multiple image elliptic curve cryptography[J]. Optics and Lasers in Engineering, 2021, 136: 1-10.
- [16] 刘博,刘建东,陈飞,钟鸣,张世博,等. 基于整数动态耦合帐篷映射的视频加密算法[J]. 计算机应用与软件, 2019, 36(12): 309-315, 328.
- LIU B, LIU J D, CHEN F, et al. A video encryption algorithm based on integer dynamic coupling tent map[J]. Computer Applications and Software, 2019, 36(12): 309-315, 328. (in Chinese)
- [17] CHUA L, YANG L. Cellular neural networks: theory[J]. IEEE Transactions on Circuits and Systems, 1988, 35(10): 1257-1272.
- [18] WANG X Y, XU B, ZHANG H G. A multi-ary number communication system based on hyperchaotic system of 6th-order cellular neural network[J]. Communications in Nonlinear Science and Numerical Simulation, 2010, 15(1): 124-133.
- [19] PHATAK S C, RAO S S. Logistic map: a possible random-number generator [J]. Physical Review E, Statistical Physics, Plasmas, Fluids, and Related Interdisciplinary Topics, 1995, 51(4): 3670-3678.
- [20] 赵凤,梁静. 一种混合级联混沌的伪随机序列生成方法[J]. 洛阳师范学院学报, 2019, 38(8): 8-11.
- ZHAO F, LIANG J. Pseudo-random sequence generation method for hybrid cascade chaos[J]. Journal of Luoyang Normal University, 2019, 38(8): 8-11. (in Chinese)
- [21] 赵晓龙,李博,贾芑,等. 改进约瑟夫遍历和分段Logistic映射的图像加密算法[J]. 电子器件, 2021, 44(1): 125-130.
- ZHAO X L, LI B, JIA P, et al. Image encryption algorithm based on improved Joseph traversal and piecewise logistic mapping[J]. Chinese Journal of Electron Devices, 2021, 44(1): 125-130. (in Chinese)
- [22] FIRDOUS A, UR REHMAN A, SAAD MISSEN M M. A highly efficient color image encryption based on linear transformation using chaos theory and SHA-2 [J]. Multimedia Tools and Applications, 2019, 78(17): 24809-24835.
- [23] KHAN J S, AHMAD J. Chaos based efficient selective image encryption[J]. Multidimensional Systems and Signal Processing, 2019, 30(2): 943-961.

编辑 金胡考