结合小波变换与混沌键控的视频加密算法

朱 艳 平
(信阳农林学院信息工程学院 河南 信阳 464000)

摘 要 针对视频加密难以平衡安全性和实时性需求的问题,提出小波变换与混沌键控相结合的视频加密算法。该算法选取三维细胞神经网络系统、三维罗斯勒系统和三维陈系统作为密钥源;混沌系统的初始值、密钥的选取和密文的像素值均与明文视频有关。在置乱加密过程中采用小波变换技术,使每一帧的数据处理量减少了75%。经实验表明,该算法的密钥敏感性和明文敏感性强,密钥空间大,统计特性完全被打破,信息熵接近于理想值,具有良好的通用性、并行性、抗噪性和抗剪裁性。小波变换和混沌键控加密技术,以及“扩散”和“一次一密”加密思想的运用,有效地平衡了加密算法安全性和实时性的关系,具有一定的实用价值。

关键词 小波变换 混沌键控 视频加密 安全性 实时性

中图分类号 TP309.7 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2019.04.049

VIDEO ENCRYPTION ALGORITHM COMBINING WAVELET TRANSFORM WITH CHAOS KEYING

Zhu Yanping
(*Information Engineering College, Xinyang Agriculture and Forestry University, Xinyang 464000, Henan, China*)

Abstract In order to solve the problem that video encryption is difficult to balance the security and real-time requirements, we proposed a video encryption algorithm combining wavelet transform with chaos keying. We selected three-dimensional CNN system, three-dimensional Rosler system and three-dimensional Chen system as the key source. The initial value of the chaotic system, the selection of key and the pixel value of the ciphertext were all related to the plaintext video. The wavelet transform technology was used in scrambling encryption to reduce the data processing capacity of each frame by 75%. Experiments show that the algorithm has strong key sensitivity and plaintext sensitivity, and has large key space. It completely breaks statistical characteristics, and is close to the ideal value of information entropy. It has good versatility, parallelism, noise resistance and anti-clipping. Wavelet transform and chaos keying encryption technology, as well as "diffusion" and "one-time and one-secret" encryption ideas, effectively balance the relationship between the security and real time, which have certain practical value.

Keywords Wavelet transform Chaos keying Video encryption Safety Real time

0 引 言

互联网大数据时代的到来,视频已成为学习、工作、交流和娱乐的重要方式之一。由于其应用范围和领域不断扩大,对其安全性的要求也越来越高,因此视频信息的加密算法就成为了研究的热点问题[1]。

文献[2]采用3DES,文献[3-4]采用AES对视频信息进行加密,但此类加密方法主要适用于文本信息,如果应用在视频加密上,需要对视频进行预处理操作,达不到它的实时性要求[5]。文献[6-8]采用低维混沌系统作为密钥源,密钥空间小,安全性差;由于基于特定的视频编码标准,其应用范围具有局限性。文献[9-10]均采用四维超混沌系统作为密钥源,密钥空

收稿日期:2018-10-09。河南省科技厅科技攻关计划项目(172102210451);河南省科技厅科技攻关计划项目(172102210450)。
朱艳平,讲师,主研领域:细胞神经网络,混沌加密。

间得到了提升,但并未考虑明文对加密算法的影响,明文敏感性不强。文献[11]提出的视频加密算法具有通用性,但为了提高加密速度,舍弃了置乱加密过程,仅保留了像素替代加密过程,安全性能有所下降。

针对以上问题,本文提出小波变换与混沌键控相结合的视频加密算法。根据文献[13]对各混沌系统动力学行为特性的分析结果,选取三维 CNN 系统、三维 Rossler 系统和三维 Chen 系统作为密钥源;因为低频部分集中了视频帧的大部分信息,只需对此进行置乱就能达到加密的目的[14],所以在置乱加密过程中使用小波变换技术,仅对原视频帧四分之一的数据进行处理,大大提高了加密的效率;混沌键控技术既能扩大密钥空间,又能提升算法的并行性;密钥源的初始值、密钥的选取以及像素的加密值都与明文信息有关,提高了算法的明文敏感性;"扩散"和"一次一密"加密思想的运用,也使加密算法的安全性得到了较大程度的提高。

1 混沌系统

1.1 数学模型

细胞神经网络 CNN(Cellular Neural Network)的数学模型如下[15]:

$$\dot{x}_j = -x_j + a_j f(x_j) + \sum_{\substack{k=1 \\ k\neq j}}^{n} A_{jk} f(x_k) + \sum_{k=1}^{n} S_{jk} x_k + \tilde{I}_j \quad j = 1,2,\cdots,n \tag{1}$$

式中:j 为细胞记号;a_j、A_{jk}、S_{jk} 和 $\tilde{I}_j$ 为细胞参数;$f(x_j) = 1/2(|x_j+1| - |x_j-1|)$ 为细胞输出。当 $n=3$,$S_{33}=S_{21}=S_{23}=1$,$a_1=3.875$,$S_{11}=-1.57$,$S_{12}=9$,$S_{32}=-14.286$,其余参数均取值为 0,则式(2)为三维 CNN 系统。

$$\begin{cases} \dot{x}_1 = -2.57x_1 + 9x_2 + 3.875f(x_1) \\ \dot{x}_2 = x_1 - x_2 + x_3 \quad \dot{x}_3 = -14.286x_2 \end{cases} \tag{2}$$

三维 Rossler 系统的数据模型如下[16]:

$$\begin{cases} \dot{x}_1 = -x_2 - x_3 \quad \dot{x}_2 = x_1 + ax_2 \\ \dot{x}_3 = b + x_3(x_1 - c) \end{cases} \tag{3}$$

当 $a=b=0.2$,c 的取值在 4.2 与 9 之间时,该系统处于混沌状态,此处 $c=5.7$。

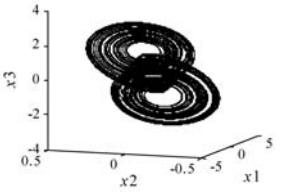
三维 Chen 系统的数学模型如下[17]:

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) \quad \dot{x}_2 = (c-a)x_1 + cx_2 - x_1x_3 \\ \dot{x}_3 = -bx_3 + x_1x_2 \end{cases} \tag{4}$$

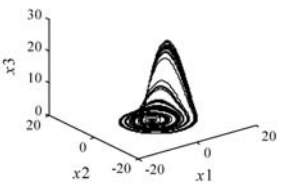
当 $a=35$,$b=3$,$c=28$ 时,该系统进入混沌状态。

1.2 混沌特性分析

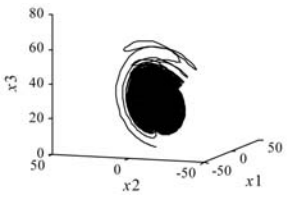
(1) 混沌吸引子 当初始值 $x_1(0)=0.1$,$x_2(0)=x_3(0)=0.2$ 时,图 1(a)为三维 CNN 系统所产生的混沌吸引子,(b)为三维 Rossler 系统产生的混沌吸引子,(c)为三维 Chen 系统产生的混沌吸引子。



(a) CNN 系统混沌吸引子



(b) Rossler 系统混沌吸引子



(c) Chen 系统混沌吸引子

图 1 三种混沌系统所产生的部分混沌吸引子

(2) 初始值敏感性 对初始条件极为敏感是混沌系统的显著特征,使用密钥变化率 KCR(Key Change Rate)对三种混沌系统的初始值敏感性进行分析。初始值 $x_1(0)=0.1$,$x_2(0)=x_3(0)=0.2$。当 $x_1(0)=0.1+1e-16$,而 $x_2(0)$ 和 $x_3(0)$ 的值不变,则三维 CNN 系统、三维 Rossler 系统和三维 Chen 系统的 KCR 值分别为 0.998 8、0.983 4 和 0.999 6;当 $x_2(0)=0.2+1e-16$,而 $x_1(0)$ 和 $x_3(0)$ 的值不变,则上述三个混沌系统的 KCR 值分别为 0.999 9、0.986 8 和 0.999 8;当 $x_3(0)=0.2+1e-15$,而 $x_1(0)$ 和 $x_2(0)$ 的值不变,则它们的 KCR 值分别为 0.999 8、0.990 3 和 0.999 9。KCR 的值越大,表示该混沌系统的初始值敏感性越强,反之越弱。

从上述实验数据可以看出,这三个混沌系统对初始条件是极为敏感的,混沌特性显著,适合将其应用于视频加密系统中。

2 视频加密算法

该视频加密算法如下:

步骤 1 选择混沌系统作为密钥源。采用 3 通道同时对视频信息进行加解密。1 通道对应 CNN 系统,2 通道对应 Rossler 系统,3 通道对应 Chen 系统。且在每个通道设置 1 个开关,分别记作 t_1、t_2 和 t_3。当其取值为 1 时,表示该通道处于忙状态,否则处于空闲状态。依次扫描 t_1、t_2 和 t_3,选择处于空闲状态的通道作为传输通道,并选择该通道对应的混沌系统作为密

钥源。

步骤 2　混沌系统初始值的选取。采用式(5)来选取混沌系统的初始值。

$$\begin{cases} Xor = R \oplus G \oplus B \quad x_1(0) = (Xor - k_1)/255 \\ x_2(0) = (Xor - k_2)/255 \quad x_3(0) = (Xor - k_3)/255 \end{cases} \tag{5}$$

式中:R、G 和 B 分别表示明文视频帧所有像素的红色分量、绿色分量和蓝色分量的异或值,⊕为异或操作。k_1、k_2和 k_3为初始值调节参数,可以取 0 到 255 之间的任意实数。

步骤 3　密钥的选取。每一个混沌系统均可生成 3 路混沌序列,每 1 路混沌序列产生 Q 个混沌值即可满足"一次一密"的密钥要求。其中 $Q = M \times N$,M 为视频帧的高,N 为视频帧的宽。使用式(6)对混沌序列进行映射处理,使其取值均在[0 ~ 255]的值域内。$x(i,j)$为最初生成的混沌值,$Y(i,j)$为经过映射处理后的混沌序列,fix 为向 0 靠近取整,mod 为取余操作。

$$\begin{cases} Y(i,j) = ((fix(x(i,j)) - fix(x(i,j))) \times 10^6) \bmod 10^3) \\ \bmod 256 \quad i = 1,2,\cdots Q; j = 1,2,3 \end{cases} \tag{6}$$

步骤 4　小波置乱加密。将视频帧进行小波分解,取其低频部分信息,按如下公式进行置乱加密:

$$\begin{cases} fi = ((i + dk + Y(ii, roadi)) \bmod M/2) + 1 \\ \quad roadi = (Xor \bmod 3) + 1 \\ fj = ((j + dk + Y(jj, roadj)) \bmod N/2) + 1 \\ \quad roadj = (roadi \bmod 3) + 1 \end{cases} \tag{7}$$

若像素点(i,j)和像素点(fi,fj)的位置均未发生变化,则将这两个像素点互换位置。其中 $Y(ii,roadi)$表示第 $roadi$ 路混沌序列的第 ii 个混沌值,ii 的取值从 1 到$(M/2) \times (N/2)$。$dk = 0,1,2,\cdots,n-1$,n 是正整数,为置乱的循环次数。最后将置乱后的低频部分与高频部分进行小波重构,得到小波置乱后的加密视频帧。

步骤 5　像素替代加密。对于小波置乱后的加密视频帧,采用如下公式进行像素替代加密:

$$\begin{cases} FXR(k) = \begin{cases} Xor \oplus XR(k) \oplus Y(hr,lr) \oplus ((XG(M \times N) + XB(M \times N)) \bmod 255) & k = 1 \\ XR(k) \oplus Y(hr,lr) \oplus ((FXG(k-1) + FXB(k-1)) mod 255) & k \neq 1 \\ hr = ((i \times j) \bmod Q) + 1 \quad lr = ((Xor + i \times j) \bmod 3) + 1 \end{cases} \\ FXG(k) = \begin{cases} Xor \oplus XG(k) \oplus Y(hg,lg) \oplus ((XR(M \times N) + XB(M \times N)) \bmod 255) & k = 1 \\ XG(k) \oplus Y(hg,lg) \oplus ((FXR(k-1) + FXB(k-1)) \bmod 255) & k \neq 1 \\ hg = (hr \bmod Q) + 1 \quad lg = (lr \bmod 3) + 1 \end{cases} \\ FXB(k) = \begin{cases} Xor \oplus XB(k) \oplus Y(hb,lb) \oplus ((XR(M \times N) + XG(M \times N)) \bmod 255) & k = 1 \\ XB(k) \oplus Y(hb,lb) \oplus ((FXR(k-1) + FXG(k-1)) \bmod 255) & k \neq 1 \\ hb = (hg \bmod Q) + 1 \quad lb = (lg \bmod 3) + 1 \end{cases} \end{cases} \tag{8}$$

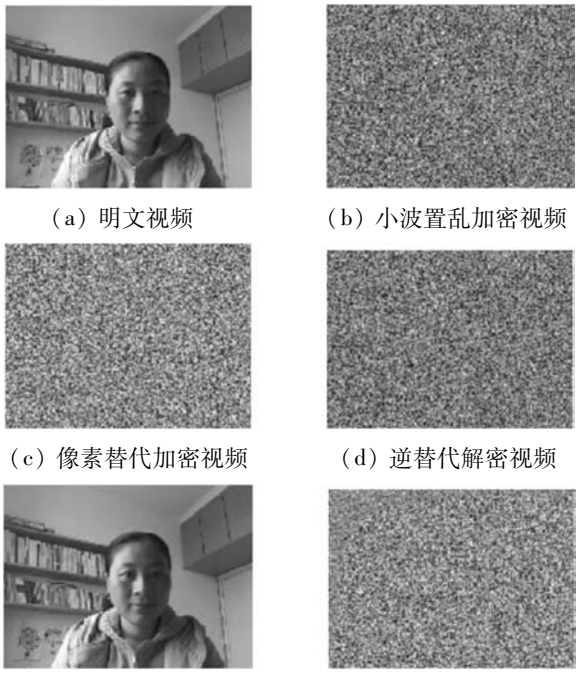
式中:$FXR(k)$、$FXG(k)$和 $FXB(k)$分别表示经像素替代加密后第 k 个像素的红色、绿色和蓝色分量的值;$XR(k)$、$XG(k)$和 $XB(k)$分别表示经小波置乱后的第个像素的红色、绿色和蓝色分量的值;Y 为加密密钥,i 和 j 分别为视频帧像素的行号和列号。

步骤 6　解密。解密过程是加密过程的逆过程。

3　实验结果分析

3.1　加密效果分析

对摄像头采集的视频信息使用上述算法进行加密和解密处理,此处 $k_1 = 0.1$,$k_2 = 0.2$,$k_3 = 0.3$,则图 2(a)为明文视频,(b)为经由小波置乱加密后的视频,(c)为像素替代加密后的视频,(d)为逆替代解密后的视频,(e)为逆置乱解密后的视频。



(a) 明文视频　(b) 小波置乱加密视频　(c) 像素替代加密视频　(d) 逆替代解密视频　(e) 逆置乱解密视频　(f) 初始值密钥敏感性

图 2　视频的加密和解密效果

从图 2 可知,无论是小波置乱后的加密视频,还是像素替代后的加密视频,都已看不出任何影像,而解密后的视频与明文视频在视觉感观上毫无差异,说明该视频加密算法取得了良好的加密和解密效果。

3.2　密钥敏感性分析

以第 1 帧视频为例,对该算法的密钥敏感性进行分析。根据上述算法,该视频帧应该选择三维 CNN 混沌系统作为密钥源。当解密的初始值密钥 $x'_1(0) = x_1(0) + 10^{-16}$,其他解密的初始值密钥和模板参数密钥不变时,得到的解密结果如图 2(f)所示。从图 2(f)可知,即使解密密钥与加密密钥相差无几,也会导致解密结果的完全错误。对混沌系统的其他初始值密钥进行测试,得到的实验结果类似,3 个初始值密钥的敏感

性均达到 10^{-16}。使用像素变化率 CPCR(Cipherimage Pixel Change Rate)对初始值的密钥敏感性进行分析。CPCR 的值越大,表示解密的效果越不好。令该混沌系统的初始值密钥分别作 10^{-16}的微小变化,则表 1 为该加密算法的 CPCR 测试结果。

表 1 初始值密钥敏感性 CPCR 测试结果

算法/初始值	红色分量	绿色分量	蓝色分量
本文算法/$x_1(0)$	0.995 2	0.995 6	0.995 3
本文算法/$x_2(0)$	0.995 6	0.995 2	0.995 8
本文算法/$x_3(0)$	0.995 4	0.995 5	0.995 3
文献[9]/初始值	0	0	0
文献[10]/初始值	0	0	0
文献[11]/$x_1(0)$	1	0.997 2	1
文献[11]/$x_2(0)$	0.992 2	0.990 6	0.992 2
文献[11]/$x_3(0)$	0.997 5	0.989 7	0.991 9
文献[11]/$x_4(0)$	0.993 4	0.996 2	0.997 5
文献[11]/$x_5(0)$	0.997 5	0.993 8	0.994 7
文献[12]/$x_1(0)$	0	0	0

从表 1 的实验数据可知,当解密的初始值密钥与加密的初始值密钥相差 10^{-16}时,文献[9]、文献[10]和文献[12]的 CPCR 值均为 0,说明上述文献的初始值密钥敏感性达不到 10^{-16},经实验验证,文献[9]和文献[12]的初始值密钥敏感性为 10^{-15},文献[10]的初始值密钥敏感性为 10^{-12}。本算法的密钥敏感性为 10^{-16},CPCR 值均达到 99.5% 以上,平均值为 0.995 43。文献[11]的密钥敏感性也达到了 10^{-16},CPCR 的平均值为 0.994 96。本文算法的初始值密钥敏感性优于文献[9-12],初始值密钥敏感性良好。对模板参数密钥和调节参数密钥的敏感性分析与此相似。

3.3 明文敏感性分析

使用 NPCR(Number of Pixels Change Rate)和 UACI(Unified Average Changing Intensity)来衡量算法的明文敏感性。NPCR 的理想值约为 0.996,UACI 的理想值约为 0.333。表 2 为该视频加密算法的明文敏感性测试结果。

表 2 明文敏感性 NPCR 和 UACI 测试结果

名称	红色分量	绿色分量	蓝色分量
该算法 NPCR	0.995 9	0.996 2	0.996 3
文献[9]NPCR	1.3021e-05	1.3021e-05	1.3021e-05
文献[10]NPCR	1.3021e-05	1.3021e-05	1.3021e-05
文献[11]NPCR	0.991 8	0.990 8	0.991 0

续表 2

名称	红色分量	绿色分量	蓝色分量
文献[12]NPCR	2.604 2e-05	2.604 2e-05	1.302 1e-05
该算法 UACI	0.336 1	0.333 7	0.335 0
文献[9]UACI	6.350 7e-06	5.235 1e-06	5.235 1e-06
文献[10]UACI	5.358 5e-06	6.344 5e-06	5.358 5e-06
文献[11]UACI	0.334 0	0.333 2	0.331 6
文献[12]UACI	6.893 4e-06	5.974 3e-06	5.004 1e-06

从表 2 的实验数据可知,文献[9]、文献[10]和文献[12]的 NPCR 和 UACI 值较理想值相去甚远,明文敏感性不强。而本算法 NPCR 和 UACI 的平均值分别为 0.996 1 和 0.334 9,比文献[11]更接近于理想值,说明该算法的明文敏感性较强。

3.4 密钥空间

三维 CNN 系统有 24 个密钥,三维 Rossler 系统有 6 个密钥,三维 Chen 系统有 6 个密钥,共计 36 个密钥。采用 16 位有效数字作为计算机浮点数的计算精度,则该算法的密钥空间为 10^{576}。另外还有 3 个初始值调节参数密钥,它们分别可以取 0 至 255 之间的任意实数,使其密钥空间变得更大。文献[9]、文献[10]和文献[12]的密钥空间分别为 10^{144}、10^{144}和 10^{32},该算法在密钥空间方面,要优于文献[9]、文献[10]和文献[12]。

3.5 相关性分析

随机选取各个颜色分量上的$(M/2)\times(N/2)$对像素值,分别计算其在水平、垂直和对角三个方向的相关性,则表 3 为实验所得的测试结果。

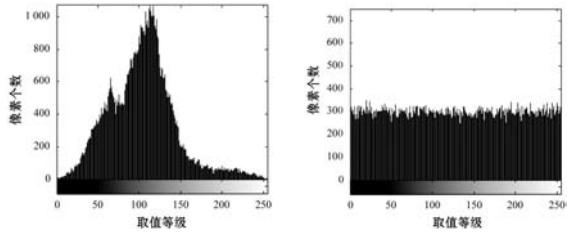
表 3 明文和密文相邻像素的相关系数

方向	红色,绿色,蓝色分量
水平(明文)	0.933 0,0.952 6,0.959 7
水平(该算法密文)	0.013 5,0.001 7,-9.1534e-04
水平(文献[9]密文)	0.005 7,0.005 2,0.008 3
水平(文献[12]密文)	-0.091 2,-0.087 7,-0.0895
垂直(明文)	0.967 2,0.976 3,0.979 4
垂直(该算法密文)	0.004 5,-0.008 5,-0.002 0
垂直(文献[9]密文)	0.008 3,0.001 1,0.003 4
垂直(文献[12]密文)	-0.052 1,-0.045 2,-0.035 4
对角(明文)	0.908 0,0.934 5,0.943 8
对角(该算法密文)	-0.005 2,6.2132e-04,0.016 4
对角(文献[9]密文)	0.004 4,0.094,0.004 6
对角(文献[12]密文)	-0.046 0,-0.065 7,-0.054 5

从表 3 的实验数据可知,明文的相关性接近于 1,相邻像素之间为极强相关;而该加密算法得到的密文相关性接近于 0,相邻像素之间为极弱相关或无相关。在 9 个相关系数中,该算法有 5 个值比文献[9]小,有 9 个值比文献[12]小。说明该算法在相关性方面要优于文献[9]和文献[12]。

3.6　直方图

图 3(a)为明文红色分量的直方图,(b)为密文红色分量的直方图。



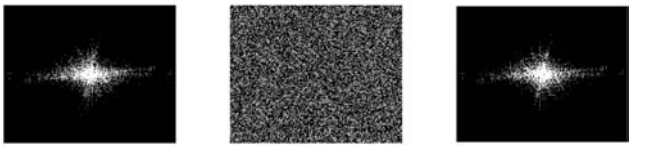
(a) 明文直方图　　(b) 密文直方图

图 3　红色分量直方图分析结果

从图 3 可知,明文视频帧的直方图呈现高低错落的山峰状,其中取值在[0 ~ 30]和[150 ~ 255]的像素个数较少,均在 100 个左右;取值在 110 左右的像素个数最多,达到 1 000 个以上。而密文视频帧的直方图呈现等概率的均匀分布,每个取值等级上的像素个数均在 300 个左右,明文的统计特性被完全打破。

3.7　视频帧的幅值频谱图分析

使用幅值频谱图来分析视频帧的频率分布情况。图 4(a)为明文的二维幅值频谱图,(b)为密文的二维幅值频谱图,(c)为解密视频帧的二维幅值频谱图。



(a) 明文频谱图　　(b) 密文频谱图　　(c) 解密视频频谱图

图 4　二维幅值频谱分析

从图 4 可知,明文的幅值频谱大多集中在中心区域,中心的亮点反映的是视频帧的低频信息。密文视频帧的幅值频谱在二维空间内分布较为均匀,呈离散化状态,在频域内的相关性较小,且明显不同于明文视频帧的幅值频谱图,可有效抵抗密文信息攻击,安全性较好。

3.8　信息熵分析

信息熵反映了视频帧分布的聚集特征,密文视频帧信息熵的理想值为 8。该算法密文在红色、绿色和蓝色分量上的信息熵分别为 7.989 5、7.989 3、7.989 3,接近于理想值 8,而文献[12]的信息熵接近于 7,说明该算法在信息熵方面要优于文献[12]。

3.9　抗噪性、抗剪裁性能分析

使用峰值信噪比 PSNR 进行抗噪性能分析。PSNR 的值越大,抗噪性能越好。若密文视频帧受到均值为 0、方差为 0.01 的高斯白噪声干扰,则解密视频帧如图 5(a)所示,其 PSNR 值为 17.169 1。若受到噪声密度为 0.01 的椒盐噪声干扰,则解密视频帧如图 5(b)所示,PSNR 值为 29.446 1。若受到均值为 0、方差为 0.01 的乘性噪声干扰,则解密视频帧如图 5(c)所示,PSNR 值为 19.150 2。

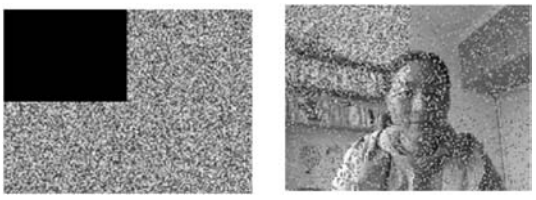
(a) 受白噪声干扰　　(b) 受椒盐噪声干扰

(c) 受乘性噪声干扰

图 5　加密算法的抗噪性能分析

从图 5 和计算得出的 PSNR 值可知,该加密算法的抗噪性能较好。虽然受到了噪声干扰,但仍可有效地解密视频帧信息。其中对椒盐噪声的抵抗性优于对乘性噪声的抵抗性,而对乘性噪声的抵抗性又优于对高斯白噪声的抵抗性。

若密文视频帧受到了左上角 1/4 的剪裁攻击,则图 6(a)为受剪裁攻击的密文视频帧,(b)为解密视频帧。



(a) 受剪裁攻击的密文　　(b) 解密视频帧

图 6　加密算法的抗剪裁性分析

从图 6 可知,即使密文视频帧遭受了 1/4 的剪裁攻击,仍能有效地解密出视频帧信息,该加密算法具有较好的抗剪裁性能。

4　结　语

本文提出了小波变换和混沌键控相结合的视频加密算法,并从加密效果、密钥敏感性、明文敏感性、密钥

空间、直方图、相关性、幅值频谱图、信息熵、抗噪性能和抗剪裁性能十个方面进行了性能分析。实验结果表明,该加密算法有效地解决了安全性和实时性难以平衡的问题,加密效率和安全性均得到了提高,具有较高的应用价值。

参 考 文 献

[1] Zeng H, Ji L. An encryption method for mobile video surveillance system based on ZUC algorithm[J]. Procedia Computer Science, 2018, 131: 282-288.

[2] 宠湃. 基于 ARM 的视频加密系统设计[D]. 北京: 北方工业大学, 2016.

[3] 杨明宣. 基于 HEVC 码流的压缩域视频加密技术研究[D]. 北京: 北京工业大学, 2016.

[4] 杨立娟, 谢淑翠, 张建中. 基于组合混沌系统的彩色视频流加密算法[J]. 电视技术, 2016(12): 7-11,16.

[5] 朱艳平. 七维 CNN 超混沌图像加密系统研究[J]. 哈尔滨师范大学自然科学学报, 2016,32(3):24-28.

[6] Sallam A I, El-Rabaie E S M, Faragallah O S. Efficient HEVC selective stream encryption using chaotic logistic map[J]. Multimedia Systems, 2018, 24(4): 419-437.

[7] 马毅超. 基于 H_264 的多混沌视频加密研究[D]. 唐山: 华北理工大学, 2016.

[8] 陈谢. 基于 H_265 的视频加密算法研究与实现[D]. 杭州: 杭州电子科技大学, 2016.

[9] 王洪伟, 史国炜, 秦军. 基于混沌密钥的视频单通道光学加密技术研究[J]. 光电子·激光, 2017,28(9): 1008-1015.

[10] 陈秋琼. 基于超混沌系统的视频压缩与加密新算法[J]. 信息技术与信息化, 2017(4): 89-92.

[11] 朱艳平. 基于 CNN 超混沌的视频加密新算法[J]. 西南师范大学学报(自然科学版), 2016,41(9):113-119.

[12] 赖益强. 多媒体视频图像信息传输安全性能研究[J]. 计算机仿真, 2017,34(11):168-171, 219.

[13] 朱艳平. 各种混沌系统性能比较研究[J]. 微型机与应用, 2016,35(12):4-6,9.

[14] 曹光辉, 李春强. 联合空域和小波域的图像加密[J]. 计算机应用, 2017,37(2):499-504.

[15] Starkov S O, Lavrenkov Y N. Prediction of the Moderator Temperature Field in a Heavy Water Reactor based on a Cellular Neural Network[J]. Nuclear Energy and Technology, 2017,3(2): 133-140.

[16] Singh L D, Singh K M. Cryptanalysis of Symmetric Key Image Encryption Using Chaotic Rossler System[J]. Optik—International Journal for Light and Electron Optics, 2017, 135: 200-209.

[17] Liang X Y, Qi G Y. Mechanical Analysis of Chen Chaotic System[J]. Chaos, Solitons and Fractals, 2017,98: 173-177.

(上接第 250 页)

[13] Lewis H G, Brown M. A generalized confusion matrix for assessing area estimates from remotely sensed data[J]. International Journal of Remote Sensing, 2001, 22(16): 3223-3235.

[14] 曹惠玲,贾超. 基于 QAR 的民航发动机燃油流量控制规律研究[J]. 科学技术与工程,2013,13(13):3814-3817.

[15] 谷润平,黄磊,赵向领. 基于 QAR 数据的飞机发动机性能异常检测[J]. 航空计算技术,2015(4):1-3.

(上接第 261 页)

[3] 黄衍,查伟雄. 随机森林与支持向量机分类性能比较[J]. 软件,2012,33(6):107-110.

[4] 吴琼,李运田,郑献文. 面向非平衡训练集分类的随机森林算法优化[J]. 工业控制计算机,2013,26(7):89-90.

[5] Chawla N V, Bowyer K W, Hall L O, et al. SMOTE: synthetic minority over-sampling technique[J]. Journal of artificial intelligence research, 2002,16(1):321-357.

[6] Sáez J A, Krawczyk B, Wozniak M. Analyzing the oversampling of different classes and types of examples in multi-class imbalanced datasets[J]. Pattern Recognition, 2016, 57: 164-178.

[7] Han H, Wang W Y, Mao B H. Borderline-SMOTE: A New Over-Sampling Method in Imbalanced Data Sets Learning[C]// Proceedings of the 2005 international conference on Advances in Intelligent Computing-Volume Part I. Springer-Verlag, 2005:878-887.

[8] 李雄飞,李军,董元方,等. 一种新的非平衡数据学习算法 PCBoost[J]. 计算机学报,2012,35(2):202-209.

[9] Gu Y X, Ding S F. Advances of support vector machines (SVM)[J]. Computer Science, 2011, 38(2):14-17.

[10] Naganjaneyulu S, Kuppa M R. A novel frame work for class imbalance learning using intelligent under sampling[J]. Progress in artificial intelligence, 2013, 2(1):73-84.

[11] Zhan X, Song Q, Wang G, et al. A dissimilarity based imbalance data classification algorithm[J]. Applied Intelligence, 2015,42(3):544-565.

[12] Jiang K, Lu J, Xia K. A novel algorithm for imbalance data classification based on genetic algorithm improved SMOTE[J]. Arabian journal for science and engineering, 2016,41(8):3255-3266.

[13] Xu Y, Yang Z, Zhang Y, et al. A maximum margin and minimum volume hyper-spheres machine with pinball loss for imbalanced data classification[J]. Knowledge Based Systems, 2016,95:75-85.

[14] Anwar N, And G J, Ganesh S. Measurement of data complexity for classification problems with unbalanced data[J]. Statistical Analysis & Data Mining the Asa Data Science Journal, 2014, 7(3):194-211.