文章编号:1671-4598(2024)03-0017-07 DOI:10.16526/j.cnki.11-4762/tp.2024.03.003 中图分类号:TP309 文献标识码:A

基于 AES 的改进视频加密测试

杜宸罡，李 博，画芊昊
(中北大学 仪器科学与动态测试教育部重点实验室，太原 030051)

摘要：为了使得视频加密技术具有更加良好的加密效果，在原本 AES 加密算法基础上进行了创新，通过加密元素的选取、运动矢量的加密方案设计、DCT 变化系数的加密方案设计三部分进行了展开分析与实验；经过后续仿真验证，密钥敏感性得到了很好的提升；视频质量方面，改进后的 AES 算法的 RGB 直方图可知其加密效果和解密还原效果良好，经过对比分析，改进后的 AES 算法加密的 SSIM 值最小、PSNR 值更低，即加密效果相对更好；经过计算可知，编码时间百分比增加了 0.23%，解码时间百分比增加了 8.56%，对 NPCR、UACI 以及加密前后视频帧像素对的相关系数等参数分别测试可知，相比前人的几种加密方式，改进后视频加密安全性能最好；综上分析可知，改进后视频加密效果最好。

关键词：AES 加密；运动矢量；DCT 变化系数；密钥敏感性；运算效率

Improved Video Encryption Test Based on AES

DU Chen'gang，LI Bo，HUA Qianhao
(Key Laboratory of Instrumental Science and Dynamic Testing，Ministry of Education，
North University of China，Taiyuan 030051，China)

Abstract：In order to improve the encryption effect of video encryption technology，based on the original advanced encryption standard (AES) encryption algorithm，the analysis and experiment are implemented through three parts of encryption element selection，motion vector encryption scheme design，DCT change coefficient encryption scheme design. After the subsequent simulation verification，the key sensitivity has a great improvement；The RGB histogram of the improved AES algorithm shows that its encryption effect and decryption and restoration effect are good video quality. Through the comparative analysis，the improved AES algorithm has the smallest SSIM and lower PSNR value，that is，the encryption effect is relatively better. After the calculation，the results show that the percentage of encoding time increases by 0.23%，and the percentage of decoding time by 8.56%. The parameters such as NPCR，UACI and correlation coefficient of video frame pixel pairs before and after encryption are tested，respectively，and the improved video encryption method has the best security performance compared with previous encryption methods. From the above analysis，the improved video encryption has the best effect.

Keywords：AES encryption；motion vector；DCT variation coefficient；key sensitivity；operational efficiency

0 引言

随着互联网技术的发展，视频加密技术[1]如同一把锁，保护好自己的贵重物品显得格外重要，广泛应用于军工、航天、生物医疗、互联网、体育比赛等诸多领域。AES 加密是目前 H5 时代广泛使用的技术，该加密是建立在 HTTP 之上，设计简单，只需要很少的存储器，因此使用简单，接入代价小，可以抵抗所有一致的攻击，在多个平台上速度快，编码紧凑，有利于 CDN 加速技术[2]的实施，其最大的优点便是几乎主流的软件都支持，包括微信、qq 等，打开就能播放，兼容性很好，但 AES 加密算法本身最大的缺点便是由于算法是公开的，如果不能保护好密钥的文件，ffmpeg 等命令行，很多工具软件均可拿到密钥对视频基本还原。对于该问题，Ajish 等人[3]提出了一种基于小波的 AES 算法，加快了加密过程，降低了移动设备的 CPU 利用率，从而增加了加密的安全性能；Yiding 等人[4]提出了一种内存处理架构 AESPIM 将 AES 加密计算卸载到内存端，通过显著减少数据移动和增加内存带宽，从而提高了加密的安全性能；Ke L 等人[5]提出了一种新的 32 位可重构、紧凑的 AES 加解密结构，并在非 bramFPG 中实现，还提出了一种新的复合域 GF ((24) 2) 上的子流水线动态密钥调度方法，可以同时生成圆密钥，进而提高了安全性能。然而，本实验在原有 AES 算法的基础上，先是利用 RANSAC 算法将误匹配消除，然后引入 2DLogistic 映射与 2D-DCT 的数字图像隐藏技术[6]，经实验对比分析，密钥敏感性、视频质量、运行效率均得到了明显更加良好的数据体现，从而使得本文改进后的 AES 算法更具有安全性，从而使得实验更有意义。

收稿日期:2023-08-11； **修回日期**:2023-09-04。

作者简介:杜宸罡(1996-)，男，硕士生。

引用格式:杜宸罡，李 博，画芊昊.基于 AES 的改进视频加密测[J].计算机测量与控制，2024，32(3):17-23，43.

1 AES 的视频加密技术基本理论

AES 是一种 SPN 结构[7]的高级加密标准的视频加密技术，其过程是由多个轮次进行，每个轮次均经过 SubByles、ShiftRows、MixColumns、AddRound Key 这 4 个步骤，即字节代替、行移位、列混淆和轮密钥加。

2 AES 加密算法的分析与改进

2.1 加密元素的选取

轮密钥加可以看成 S0 S1 S2 S3 组成的 32 位字与 W［4i］的异或运算，由于是异或运算进行语法元素加密，但方法简单，容易被破解，安全性不高，所以二值化是处理比较好的一种方法。二值化的方法有很多，比如：定长二进制（FL）、截断莱斯二元化（TR）、截断一元二元化（TU）、K 阶指数哥伦布二元化（EGK）、一元二元化（U）等等，一元码只有在非负整数时才可以使用，截断莱斯二元化加密时必须知道 CMax 和 R 的值，K 阶哥伦布指数对语法元素具有可塑性，但过程相对复杂，需要完成前缀码和后缀码的加密，定长二进制只需要满足选取的语法元素分布均匀即可，因此，此处选取定长二进制方法将轮密钥加步奏进行二值化较为合适。

字节代替是字节求一次乘法逆再完成一次仿射变换[8]而完成，使得共同点变为共线点的双射，平行直线变为平行直线，保持共线三点的简单化，从而保持俩平行线段的比值不变。在求乘法逆方法中，欧拉定理求逆元需要任意互质的 q，p 恒成立，且该方法需要多算一个欧拉函数；费马小定理具有局限性，需要 p 为质数；扩展欧几里得该方法需要先求出 xx、yy 方程的一组整数解，计算量较大。根据平时计算经验，线性求逆方法（递推法）最好，适用范围较广。线性求逆元方法如下：

$$设\ p = k * i + r,(r < i,1 < i < p) \tag{1}$$

$$则\ K * i + r = 0(mod\ p) \tag{2}$$

两边同乘 $r^{-1} + i^{-1}$，得

$$K * r^{-1} + i^{-1} = 0(mod\ p) \tag{3}$$

移项，得

$$i^{-1} = -k * r^{-1}(mod\ p) \tag{4}$$

即

$$i^{-1} = -\left|\frac{p}{i}\right| * (p \mod i)^{-1}(mod\ p) \tag{5}$$

我们可以利用该公式进行递推，边界条件为 1^{-1} 恒等于 1（$mod\ p$），时间复杂度为 $O(n)$。

行移位是一个简单的左循环移位操作。当密钥长度为 128 比特时状态矩阵的第 0 行左移 0 个字节，第一行左移 1 字节，第二行左移 2 字节，第 3 行左移 3 字节，如图 1 所示。

$$\begin{pmatrix} S0 & S1 & S2 & S3 \\ S1 & S2 & S3 & S0 \\ S2 & S3 & S0 & S1 \\ S3 & S0 & S1 & S2 \end{pmatrix} \Rightarrow \begin{pmatrix} S0 & S1 & S2 & S3 \\ S1 & S2 & S3 & S0 \\ S2 & S3 & S0 & S1 \\ S3 & S0 & S1 & S2 \end{pmatrix}$$

图 1 12 行移位操作图

列混淆是在有限域下将状态的每列 $(a0\quad a1\quad a2\quad a3)^T$ 的转置乘以一个固定多项式 $C(x)$ 模乘 4 加 1，多项式

$$C(x) = 03 * 3 + 01 * 2 + 01 * 02 \tag{6}$$

该变换以矩阵形式表示为：

$$\begin{pmatrix} b0 \\ b1 \\ b2 \\ b3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 02 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \times \begin{pmatrix} a0 \\ a1 \\ a2 \\ a3 \end{pmatrix} \tag{7}$$

明显可知，列混淆中矩阵乘法较多，计算量较大，这里我们可以利用数学中矩阵乘法次数进行优化：对于矩阵的乘法运算是相乘再相加，所以执行的乘法次数就是 $Ai * Ak * Aj$，第 i 个到第 j 个矩阵的乘法次数为：

$$\begin{aligned} matrix[i][j] = {} & matrix[k+1][j] + \\ & d[i-1] * d[k] * d[j] \end{aligned} \tag{8}$$

根据运动矢量特性可以选取语法元素 abs-mvd-minus2 和 mvd-sign-flag 进行二值化，这两种元素分别是运动矢量残差幅值和运动矢量残差符号，残差数据可以体现相邻像素的相关性，对这两种元素采用不同的二值化方法。语法元素前者 abs-mvd-minus2 采用 OTSU 方法，该方法较大的一个优点便是不用考虑分块后的图像直方图是否具有明显的双峰；语法元素后者 mvd-sign-flag 采用截断莱斯二元化方法 TR，其前缀是一元码，后缀是定长码，后缀长度为 cRiceParam，但是注意最后有截断的情况输入参数为 cRiceParm cMax 以及要二值化的 val。通过对 AES 编码标准[9]的语法元素进行筛选，可以得到如图 2 所示的适合本文加密的语法元素。

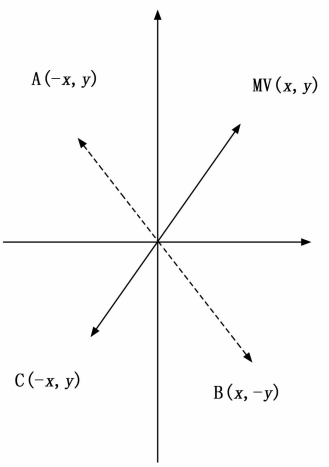

图 2 运动矢量符号位加密

表 1 适合加密的算法筛选

	二元化方案	语法元素
编码单元(CU)	TR	Intra-prediction
	TR	Inter-frame-compression
	OTSU	abs-mvd-minus2
变化单元(CU)	TR	mvd-sign-flag
	TR	coeff-abs-level-remaining
	OTSU	coeff-sign-flag

本文最大的创新即是在运动矢量加密以及 DCT[10] 变化系数加密时，在 DCT 变化系数二值化后，对运动矢量的残差数据进行二维序列处理时采用改进后的二维序列图像拼接融合技术，再结合 2DLogistic 映射与 2D-DCT 的数字图像隐藏技术，生成新的二值化编码。

二维序列图像拼接融合技术[11-13]包含数字图像拼接融合的基本流程、图像配准常用的算法、消除误匹配的算法、图像融合中常用的算法等，当然，采用 SIFT 特征初匹配算法很好地解决了畸形图像的拼接问题，通过改变校正算法和对图像进行 SIFT 特征提取、特征初匹配，利用 RANSAN 算法实现了误匹配的消除。

2DLogistic 映射与 2D-DCT 的数字图像隐藏技术即是利用二维 Logistic 映射产生的混沌序列对秘密图像的像素进行扩散和置乱[14-15]，达到了秘密图像的加密效果，然后分块对载体图像进行二维离散余弦变换，对扩散和置乱后的图像信息分存在变换后的每块右下角，最后进行二维离散余弦反变换，从而得到了隐藏图像。

2.2　基于运动矢量的加密方案设计

运动矢量加密分析主要靠运动矢量的局部最优性和相邻相关性来构造特征。前者借助运动矢量残差来提取特征，后者借助运动矢量本身的相关性提取特征。运动矢量是可以用坐标系表示的，设运动矢量坐标系为 MV（x，y），所作直角坐标系可以用肉眼进行直接分析，当改变运动矢量的横纵坐标的符号位，运动矢量的语法元素也随之发生了改变，运动矢量符号位加密如图 3 所示。

2.3　基于 DCT 变化系数的加密方案设计

Cosff-abs-level-remaining 和 Coeff-sign-flag 语法元素是 DCT 变化系数加密所需要的语法元素。对 DCT 变化系数进行的二值化[16]最好的方法是采用对角线的处理模式，下图为改进算法的 DCT 视频加密流程如图 4 所示。

3　仿真结果及实验数据分析

对于视频加密技术而言，验证该加密技术效果是否良好最重要的几个参考角度便是视频质量、运算效率、密钥敏感性。因此，本文在 Microsoft Vissual Studio 2017 上搭建实验所需的集成开发环境，硬件平台为台式电脑，型号为 i7-6700，主频为 3，40 GHZ 电脑运行内存为 4 GB，系统为 Windows7 环境，对本文改进后的 AES 算法与 AES 算法两者的密钥敏感性作对比，判断本文改进后的 AES 算法的密钥敏感性是否比 AES 算法的密钥敏感性更加良好，从视频质量角度上对本文中改进后的 AES 算法加密前后的 RGB 直方图对比分析判断本文中改进后的 AES 算法加密质量和还原性能是否良好，从而判断本文中改进后的 AES 算法加密效果是否良好，从视频质量中的 SSIM 值以及 PSNR 值、加密算法运行效率两个方面分别对比原 AES 视频加密、文献［3］中改进算法、文献［4］中改进算法、文献［5］中改进算法、本文改进后的 AES 算法进行实验分析本文中改进后的 AES 算法加密是否具有优越性。下图为 stefan、forman、gice、bus 的

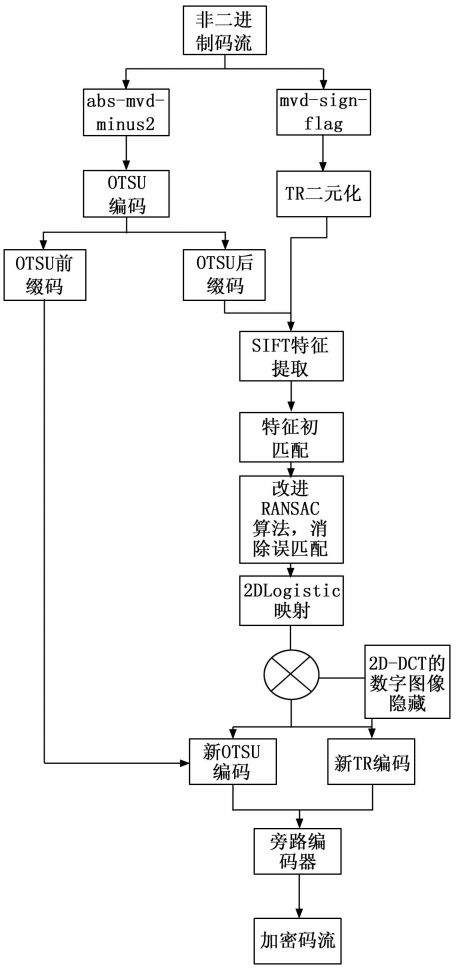

图 3　运动矢量的加密流程图

原始帧及加密帧：

图 5（a）为 stefan 原始帧，图 5（b）为 stefan 加密帧，图 5（c）为 gice 原始帧，图 5（d）为 gice 加密帧，图 5（e）为 forman 原始帧，图 5（f）为 forman 加密帧，图 5（g）为 bus 原始帧，图 5（h）为 bus 加密帧。

3.1　密钥敏感性分析

密钥敏感性是指在加解密过程中，初始密钥发生微小的变化，经密钥序列发生器或迭代函数作用后所产生的密钥发生巨大变化，从而加解密图像发生巨大变化。密钥敏感性是密码系统是否安全的主要因素，如果在加解密过程中将图像的像素值设置为控制参数并作为初始密钥，那么该算法不仅仅具有密钥敏感性，而且可以抵抗已知明文攻击。分析密钥敏感度方法为：使用两个不同的密钥加密同一语法元素序列，然后比较加密结果。

表 2　密钥敏感性对比

	AES 加密算法			改进后算法		
改变程度	改变 1e-5	改变 1e-5	改变 1 e-5	改变 1e-7	改变 1 e-8	改变 1 e-9
密钥敏感性	0.996 1	0.995 8	0.995 9	0.996	0.996 1	0.995 9

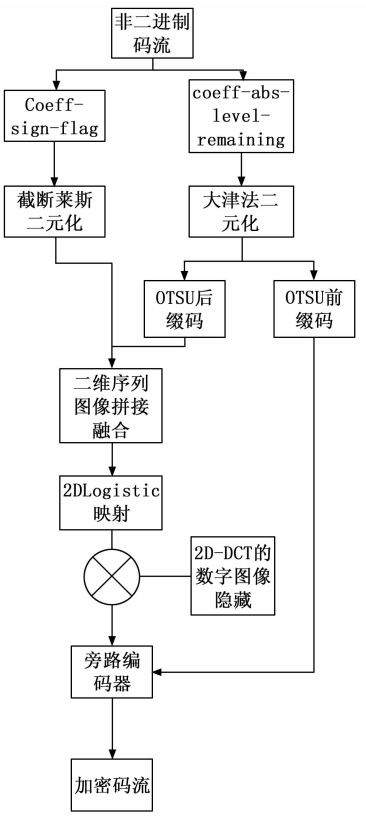

图 4 DCT 的视频加密流程图

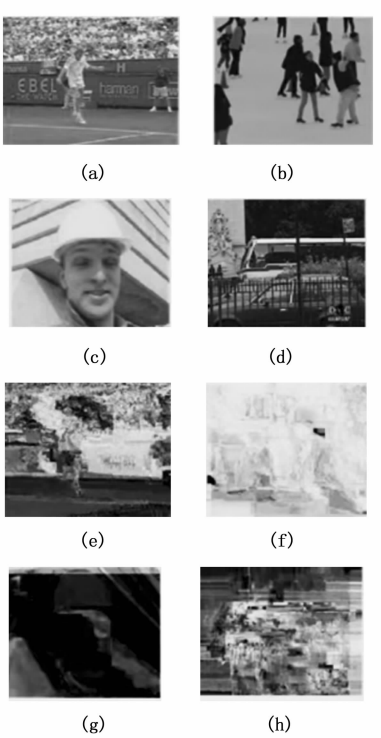

图 5 图像对比

若密钥改变一位，则解密图像中像素值的像素个数占总像素个数的比例发生了变化，将理想结果 0.996 1 的定量计算数值进行引入来衡量密钥敏感性。算法中，初始密钥为[0，0，0，1e-5]，在测试中，改变密钥的十万分之一，即 1e-5，变为 [0，0，1e-5，1e-10] 对密文进行解密。为了更具普遍性，继续改变 1e-7、1e-8、1e-9 不同的初始密码，并与 AES 加密原本算法进行对比分析，实验多次改变初始密钥的结果都在 0.996 1 附近，相比单纯 AES 加密算法密钥敏感性，本文改进后的密钥敏感性更好，从而可以抵抗已知明文攻击。

3.2 视频质量分析

RGB 直方图[17]是图像检测系统中广泛采用的颜色特征，可以通过比较 phthon 语言输出的原始帧和解密帧的 RGB 直方图是否一致以及加密帧的 RGB 直方图来判断视频加密质量，下图分别为 gice、bus、stefan、forman 的原始帧、加密帧、解密帧的 RGB 直方图：

图 6 的图（a）为 gice 原始帧的 RGB 直方图，图 6 的图（b）为 gice 加密帧的 RGB 直方图，图 6 的图（c）为 gice 解密帧的 RGB 直方图，图 6 的图（d）为 bus 原始帧的 RGB 直方图，图 6 的图（e）为 bus 加密帧的 RGB 直方图，图 6 的图（f）为 bus 解密帧的 RGB 直方图，图 6 的图（g）为 stefan 原始帧的 RGB 直方图，图 6 的图（h）为 stefan 加密帧的 RGB 直方图，图 6 的图（i）为 stefan 解密帧的 RGB 直方图，图 6 的图（j）为 forman 原始帧的 RGB 直方图，图 6 的图（k）为 forman 加密帧的 RGB 直方图，图 6 的图（l）为 forman 解密帧的 RGB 直方图。

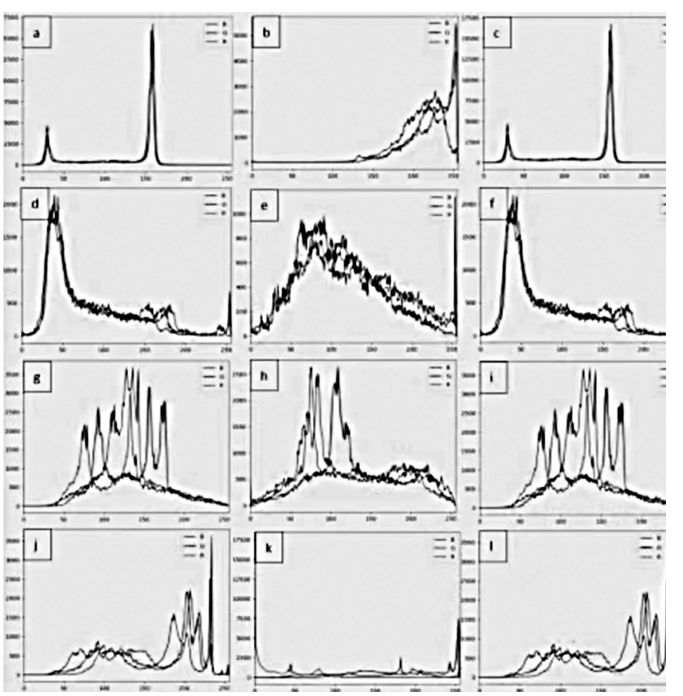

图 6 直方图

显然，改进后算法的原始帧与解密帧基本一致，说明视频加密解密性能良好，加密帧图像的像元灰度值分布不具有概率统计分布的基本特征，即视频加密质量良好。

SSIM 指数[18-20]通常用来评价视频相似度，如果 SSIM 值<0.6，则视为具有良好的保密性。计算公式如下所示：

$$SSIM(x,y=\frac{(2u_xu_{\ y}+C1)(2_{6}xy+C2)}{(u_x^2+u_y^2+C1)(6_x^2+6_y^2+C2)} \tag{9}$$

其中：x 与 y 为图像的分块，U_x 与 U_y 代表着 x，y 的平均值，6_x^2，6_y^2代表着 x、y 的方差，6_{xy}代表着 x、y 的协方差，L 是灰度级。

$$C1=(k1L)^2 \tag{10}$$

$$C2=(k2L)^2(k=0.03) \tag{11}$$

本文针对不同视频的 100 个 I 帧执行 SSIM 评估，AES 算法、文献［3］、文献［4］、文献［5］、改进后的算法进行了分析对比，结果如图 7 所示。

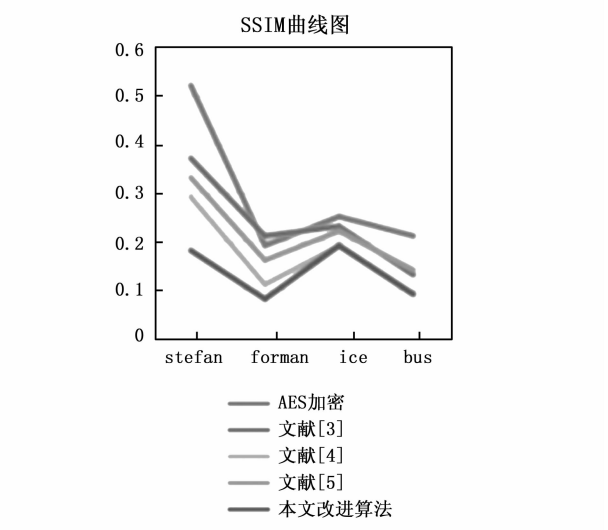

图 7　不同视频序列的 SSIM 测试结果图

图 7 中，五条曲线由上至下分别为 AES 加密序列帧、文献［3］序列特定帧、文献［4］序列特定帧、文献［5］序列特定帧、本文改进算法加密序列特定帧，经 SSIM 曲线图对比分析可知，相较而言，本文改进后的 AES 算法加密的 SSIM 值最小，其密文与明文之间的相似程度更小，即加密效果更好。

PSNR 峰值信噪比[21-23]是评价视频加密前后对比的一项重要指标，PSNR 指数越高，越不容易失真，PSNR 值≥20 为可接受范围内，如果大于 30，则视频加密前后质量非常好。计算公式如下：

$$PSNR=10*\log^{\frac{V}{MSE}} \tag{12}$$

$$MSE=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j)-C(i,j)]^2 \tag{13}$$

其中：MSE[24-25]为均方差，代表相邻像素点之间的相关性，V 是原始像素点的行个数或者列个数，C 是视频帧图像的加密图像，均方差值越小，峰值信噪比越好，则加密会有更好的效果体现。

图 8 中，五条曲线由上至下分别为 AES 加密序列帧、文献［3］序列特定帧、文献［4］序列特定帧、文献［5］序列特定帧、本文改进算法加密序列特定帧，由图明显可知，本文改进后加密序列特定帧 PSNR 值 PSNR 值相对更低，与 AES 加密序列特定帧 PSNR 值差距更大，即加密效果明显更好。

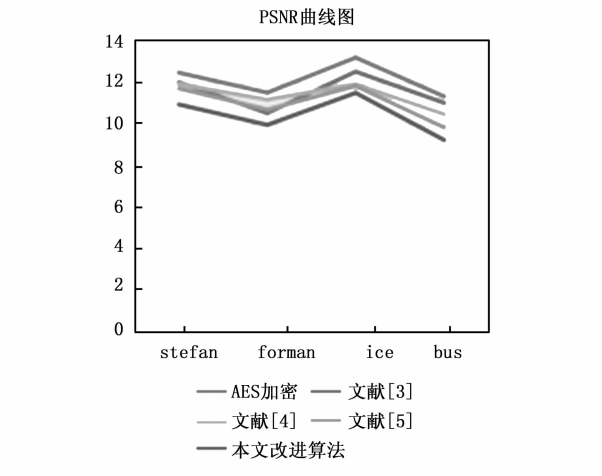

图 8　不同序列的 PSNR 测试结果图

3.3　加密算法运行效率分析

评价加密技术的一个关键特征就是处理时间[26-27]。计算机在每个测试时间所给出的执行不同，表 3 是计算了 100 个 I 帧对于 AES 加密与改进后加密由于加密过程而增加计算时间的速率对比。

表 3　加密时间运算效率

加密时间/ms	stefan	forman	ice	bus
AES 编码	1 702.81	1 716.29	1 709.97	1 708.41
文献[3]	1 697.23	1 716.05	1 705.09	1 708.37
文献[4]	1 697.13	1 715.93	1 705.07	1 708.25
文献[5]	1 697.05	1 715.24	1 704.91	1 708.12
本文编码	1 694.69	1 710.25	1 701.37	1 704.66
普通编码	1 692.49	1 706.05	1 697.57	1 699.32

表 3 中，从左到右分别为 stefan、forman、ice、bus 的 AES 加密编码、文献［3］编码、文献［4］编码、文献［5］编码、本文改进后的 AES 加密编码、普通视频编码的加密编码时间（ms）。

表 4　解密时间运算效率

解密时间(ms)	stefan	forman	ice	bus
AES 编码	123.54	135.27	135.52	140.77
文献[3]	123.29	135.12	135.44	140.59
文献[4]	123.03	134.97	135.24	140.09
文献[5]	123.01	134.75	135.11	139.84
本文编码	116.85	124.73	125.12	127.55
普通编码	108.27	112.78	114.36	119.85

表 4 中，从左到右分别为 stefan、forman、ice、bus 的 AES 加密编码、文献［3］编码、文献［4］编码、文献［5］编码、本文改进后的 AES 加密编码、普通视频编码的

解密编码时间（ms）。

表 3 中，将 AES 加密编码、文献［3］编码、文献［4］编码、文献［5］编码、本文改进后的 AES 加密编码分别与普通视频编码的作比较，经计算，AES 视频编码加密时间增幅为 0.65%，文献［3］视频编码加密时间增幅为 0.46%，文献［4］视频编码加密时间增幅为 0.456%，文献［5］视频编码加密时间增幅为 0.44%，本文改进后的 AES 视频加密编码加密时间增幅为 0.23%，从而可知本文改进后的 AES 视频加密的加密时间最少，即本文改进后的 AES 视频加密运算效率最好。

表 4 中，将 AES 加密编码、文献［3］编码、文献［4］编码、文献［5］编码、本文改进后的 AES 加密编码分别与普时间增幅为通视频编码的作比较，经计算，AES 视频编码解密 17.54%，文献［3］视频编码解密时间增幅为 17.39%，文献［4］视频编码解密时间增幅为 17.14%，文献［5］视频编码加密时间增幅为 17.01%，本文改进后的 AES 视频加密编码解密时间增幅为 8.56%，从而可知本文改进后的 AES 视频加密的解密时间最少，即本文改进后的 AES 视频加密运算效率最好。

3.4 改进加密算法安全性能分析

3.4.1 密钥空间分析

密钥空间包含了运动矢量和 DCT 变化系数在加密过程中所有加密元素的全部可能性，密钥空间的大小与加密元素的种类和语法元素可能性的多少有直接关系，并且密钥空间与它们分别均为正相关的关系。密钥空间的计算公式如下：

$$S_{frame} = (2^4 2^{l+1} 2^{k+1})^n = 2^{2WH/1024} * 2^{(l+4)m+(k+l)n} \tag{14}$$

其中：m 和 n 为加密编码的编码块个数，视频分辨率为 $W * H$，k 为加密语法元素的后缀码长度，l 为 DCT 变化系数的语法长度，预估计的密钥空间为 2^4，在改进算法运动矢量的密钥空间为 2^{k+1}，改进算法 DCT 变化系数的密钥空间为 2^{l+1}，假定视频序列分辨率为 496 * 448，则改进算法帧图像的密钥空间 $S_{\text{frame}} \geqslant 2^{256}$。一般地，密钥空间大于 2^{100} 则认为足够抵抗穷举攻击，本文改进算法的密钥空间远大于 2^{100}，因此本文改进后算法视频加密抗攻击性十分良好。

3.4.2 抗差分攻击分析

加密中，像素改变率 NPCR 和统一平均变化强度 UACI 可以充分反映原始视频帧图像和加密后视频帧图像的关系，当攻击方对加密的原始视频帧图像进行细微的改变时，若视频帧图像发生了巨大的改变，则所受到的这种明文攻击将会失效。

$$NPCR_{\text{RGB}} = \frac{\sum_{ij} D_{\text{RGB}}(i,j)}{M * N} * 100\% \tag{15}$$

$$UACI = \frac{1}{M * N}\left[\sum_{i,j} \frac{C_{R,G,B}(i,j) - C_{R,G,B}(i,j)}{255}\right] * 100\% \tag{16}$$

其中：$C_{R.G.B}$ 为所加密的图像，M、N 分别是该所加密图像像素的行数和列数。

表 5 NPCR 测试表

	期望值/%	第 18 帧/%	第 27 帧/%	第 36 帧/%
AES 加密	99.737 02	99.012 45	99.014 73	99.013 87
文献[3]	99.737 02	99.247 56	99.256 35	99.247 32
文献[4]	99.737 02	99.256 87	99.267 56	99.250 25
文献[5]	99.737 02	99.270 43	99.269 87	99.278 83
改进加密	99.737 02	99.736 98	99.737 02	99.737 03

表 6 UACI 测试表

	期望值/%	第 18 帧/%	第 27 帧/%	第 36 帧/%
AES 加密	34.528 26	34.236 73	34.236 69	34.240 25
文献[3]	34.528 26	34.367 32	34.389 13	34.357 24
文献[4]	34.528 26	34.379 12	34.384 38	34.382 57
文献[5]	34.528 26	34.381 37	34.392 57	34.390 16
改进加密	34.528 26	34.528 20	34.528 19	34.528 27

表 5 和表 6 是某像素点改变时，AES 加密、文献［3］、文献［4］、文献［5］、改进加密的视频帧分别受到的影响。经表中测试结果可知，改进加密视频帧所受影响后改变最为明显。因此，本文改进加密的抗差分攻击能力较强。

3.4.3 抗统计攻击分析

加密后，视频帧图像都具有水平和垂直的相关性。相关性越大，代表视频加密效果越差；相关性越小，代表视频加密效果越好。

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{17}$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\ \sqrt{D(y)}} \tag{18}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{19}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{20}$$

其中：x、y 为视频帧相邻像素灰度值，E（x）和 D（x）为其数学期望和方差，r_{xy} 为其相关系数。

对 AES 加密、文献［3］加密、文献［4］加密、文献［5］加密、改进后加密下在水平和垂直方向加密前后像素对的相关系数分别进行测试。

由表 7 测试结果可知，改进后加密无论是在水平方向还是垂直方向加密前后像素对相关性明显最小，抗统计攻击性最强，即改进后视频加密效果最好。

表 7 加密前后像素对的相关系数

	加密前水平方向	加密前垂直方向	加密后水平方向	加密后垂直方向
AES 加密	0.697 67	0.737 28	0.073 112	−0.023 128
文献[3]	0.697 67	0.737 28	0.072 256	−0.021 025
文献[4]	0.697 67	0.737 28	0.071 131	−0.020 762
文献[5]	0.697 67	0.737 28	0.070 328	−0.020 476
改进加密	0.697 67	0.737 28	0.055 462	−0.015 707

4　结束语

本文在加密过程实现了算法创新，在加密元素的选取板块，由于二值化是处理异或运算比较好的一种方法，文中引入了相对更为合适的定长二进制的二值化方法，使得需要进行异或运算的轮密钥加得到了方法上的进一步优化；为了计算更加简便，通过比较求乘法逆的各种方法，在拥有大量乘法逆计算的字节代替环节进行了更优乘法逆方法的找寻；为了处理大量的矩阵乘法运算，利用数学中的矩阵乘法次数的优化使得处理列混淆上更加简便。通过对 AES 编码标准的语法元素进行筛选，得到了合适的加密语法元素，在 DCT 变换的图像压缩编码方法中，采用大津法和截断莱斯二元化分别对运动矢量和 DCT 的元素进行二值化。且在 DCT 的二维序列处理上引入了二维序列图像拼接融合技术，再结合 2DLogistic 映射与 2D-DCT 的数字图像隐藏技术。在后续仿真验证中，相比原本 AES 算法，密钥敏感性得到了很好的提升；视频质量方面，相比原本 AES 算法和文献 [3－5]，本文改进后的 AES 算法的 RGB 直方图可知其加密效果和解密还原效果良好，改进后的 AES 算法加密的 SSIM 值最小、PSNR 值更低，即加密效果相对更好；运行效率经过计算可知，编码时间百分比增加了 0.23%，解码时间百分比增加了 8.56%，经过对比原本 AES 算法和文献 [3－5]，本文改进后的 AES 算法所需处理时间更短，抗统计攻击和抗差分攻击性能均最好，因此改进后视频加密效果相对更好。

在当今互联网高速发展的时代，视频加密技术有着非常大的发展潜力，非常值得进一步深入探索，尤其是对于国家网络安全、国家核心科技安全来说，视频加密技术显得极其重要，下一步将本文中改进后的 AES 算法尝试应用到工程应用中并与最新其他加密技术对比分析分别应用到工程后对工程所产生的价值。

参考文献：

[1] MACIEJ S，MARCIN N. A Sponge-Based Key Expansion Scheme for Modern Block Ciphers [J]. Energies，2022，15 (19)：124－135.

[2] M. L，S. P. R，C. R，et al. Satellite multi-beam multicast support for an efficient community-based CDN [J]. Computer Networks，2022，217 (6)：112427.

[3] AJISH S，K. S. A. Secure mobile internet voting system using biometric authentication and wavelet based AES [J]. Journal of Information Security and Applications，2021，61 (1)：109121.

[4] YIDING L，LENING W，AMER Q，et al. Enabling PIM-based AES encryption for online video streaming [J]. Journal of Systems Architecture，2022，132 (4)：110－209.

[5] KE L，HUA L，GRAEME M. A reconfigurable and compact subpipelined architecture for AES encryption and decryption [J]. EURASIP Journal on Advances in Signal Processing，2023，2023 (1)：221－293.

[6] QIYING R，ZHIPENG W. Designing a 1D extended logistic map for a secure image encryption [J]. Physica Scripta，2023，98 (8)：263－268.

[7] XU X，LIU J，WANG Y，et al. Mechanistic insights into the interactions of Ras subfamily GTPases with the SPN domain of autism-associated SHANK3 [J]. Chinese Journal of Chemistry，2020，38 (12)：101－107.

[8] BAOTAO C，ZHICHAO J，CAN L，et al. An adaptive element subdivision method based on the affine transformations and partitioning techniques for evaluating the weakly singular integrals [J]. Journal of Computational and Applied Mathematics，2024，436 (1)：120110.

[9] MARTINEZRACH MIGUEl O，MIGALLON HECTOR，LOPEZGRANADO OTONIEL，et al. Performance ovcrview of the latest vidco coding proposals：HEVC，JEM and VVC [J]. Journal of Imaging，2021. 7 (2)：227－229.

[10] KUMAR M P，THAMBIPILLAI L S，HWAN K D，et al. Area-Time efficient two-dimensional reconfigurable integer DCT architecture for HEVC [J]. Electranics，2021，10 (5)：112－113.

[11] JUN C，JIANFENG D，YANG Y，et al. THFuse：An infrared and visible image fusion network using transformer and hybrid feature extractor [J]. Neurocomputing，2023，527 (2)：101－256.

[12] XIANGHAI W，XINYING W，RUOXI S，et al. MCT-Net：Multi-hierarchical cross transformer for hyperspectral and multispectral image fusion [J]. Knowledge-Based Systems，2023，264 (3)：137－121.

[13] BIN T，LICHUN Y，JIANWU D. Fine-grained multi-focus image fusion based on edge features. [J]. Scientific Reports，2023，13 (1)：122－103.

[14] H. A，J. M. Combined image encryption and steganography technique for enhanced security using multiple chaotic maps [J]. Computers and Electrical Engineering，2023，110 (9)：134－210.

[15] WEI W，HAIPENG P，FENGHUA T，et al. A Chaotic Compressive Sensing Based Data Transmission Method for Sensors within BBNs [J]. Sensors，2022，22 (15)：227－232.

[16] HUISHAN W，GUODONG Y，WUN-SHE Y，et al. Reversible blind image hiding algorithm based on compressive sensing and fusion mechanism [J]. Optics and Laser Technology，2023，167 (4)：210－254.

[17] XIANGGEN B，ZHEXIN X，XIAOFENG X，et al. An adaptive threshold fast DBSCAN algorithm with preserved trajectory feature points for vessel trajectory clustering [J]. Ocean Engineering，2023，280 (3)：222－223.

（下转第 43 页）